COMMENTS

CRITICALLY UNDERREGULATED: AN ANALYSIS OF THE FEDERAL GOVERNMENT'S SHORTCOMINGS ON CYBERSECURITY AND HOW PRESIDENT BIDEN'S EXECUTIVE ORDER DOESN'T GO FAR ENOUGH

NAOMI HUGHES*

* J.D. Candidate, 2023, American University Washington College of Law; B.S. Public Health & B.S. Microbiology, Brigham Young University, 2018. Thank you to CJ Blaney, Leah Hamilton, Cannon Jurrens, and the entire staff of the *Administrative Law Review*.

INTRODUCTION

The United States faces a rising number of cyber threats to private organizations and state and federal governments.[1] As technology rapidly expands and more people and organizations rely on computers and the Internet to do their work, the need for adequate cybersecurity protections increases. Specifically, the nation's critical infrastructure sectors are at risk due to the current cybersecurity requirements.[2] Two recent major events made headlines for weeks: the SolarWinds and Colonial Pipeline incidents.[3] Both events threatened the nation's critical infrastructure by impacting transportation systems and information technology.[4]

The attack on SolarWinds posed a major threat to the federal sector. SolarWinds is a firm that provides information technology (IT) security and network and systems management software products.[5] At the time of SolarWinds cyberattack,[6] it worked with Fortune 500 businesses, accounting

---

1. *See* Connor Perrett, *Major Cyberattacks Have Rocked the US, and There are 'a lot of Different Ways that Ransomware Actors can Disrupt Everyone's Lives,' Experts Say*, INSIDER (June 12, 2021, 7:49 AM), https://www.businessinsider.com/cyberattacks-are-on-the-rise-in-the-us-experts-say-2021-6 (discussing an increase of attacks on U.S. television stations, public transportations, and local city computer systems).

2. *See Critical Infrastructure Sectors*, CISA (Oct. 21, 2020), https://www.cisa.gov/critical-infrastructure-sectors (defining the sixteen critical infrastructure sectors, which includes the "critical manufacturing"; "defense industrial base"; "emergency services"; "energy"; "financial services"; "government facilities"; "healthcare and public health"; and "information technology" sectors); H.R. REP. NO. 117-87, at 65 (2021) ("The Committee is increasingly concerned with the ability of adversaries to circumvent and use existing cybersecurity solutions to gain access to critical systems and data.").

3. *See* Perrett, *supra* note 1 (explaining that infrastructure incidents, like the SolarWinds and Colonial Pipeline events, make headlines for weeks because of their "spillover" effects on the supply chain, such as gas shortages creating long lines at the gas station).

4. *See id.* (showing that Colonial Pipeline controls the largest fuel pipeline in the United States and SolarWinds is an information technology firm that contracted with public and private actors alike, including the U.S. Military and the Pentagon).

5. Chris Ciaccia, *What is SolarWinds? A Look at the Hacked Software Company in Crosshairs*, FOX BUS. (Dec. 17, 2020), https://www.foxbusiness.com/technology/what-is-solarwinds-hacked-software-company.

6. *See Cyberattack*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary

firms, and "all branches of the US Military, the Pentagon, and the State Department."[7] The breach, which remained undiscovered until late December 2020, focused on a particular software package users installed on their personal network, rather than accessed from the cloud.[8] SolarWinds regularly notified its users of recommended routine updates to its software; on one such update, hackers included malicious code that users unknowingly downloaded with the update.[9] Because SolarWinds provided IT and network management services, the malicious code allowed hackers to steal legitimate credentials, such as usernames and passwords, that the hackers used to gain further access into its network and cloud system.[10] The hackers went undetected for well over a year; in April 2021, the United States formally named the Russian Foreign Intelligence Service (SVR) as the hackers behind the attack, stating that SVR had "the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide."[11] With the federal sector relying on private sector companies to provide technology services, the private sector's cybersecurity is of the utmost importance.

Likewise, the Colonial Pipeline incident showcases the impact of weak cybersecurity standards on critical infrastructure sectors. In late April 2021, Colonial Pipeline, the largest fuel pipeline in the United States, was hacked

---

/cyberattack (last visited May 10, 2022) ("[A]n attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm.").

7. Lucian Constantin, *SolarWinds Attack Explained: And Why it was so Hard to Detect*, CSO (Dec. 15, 2020, 3:44 AM), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

8. *See* Robert Chesney, *SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom*, LAWFARE (Aug. 25, 2021, 8:01 AM), https://www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom (explaining that the SolarWinds "Orion" software package required users to routinely accept software updates, leading those users to trust that SolarWinds had taken the "necessary safety precautions" to prevent the inclusion of malicious code in the updates).

9. *See id.*

10. *See* Constantin, *supra* note 7.

11. *See* Chesney, *supra* note 8 (discussing that the Russian Foreign Intelligence Service gained access to SolarWinds' code in between January and September of 2019); *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government*, WHITE HOUSE (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/ (cautioning companies against buying information technology that relies on Russia for software development).

through a virtual private network (VPN)[12] used by one of its employees.[13] The hackers gained access to Colonial Pipeline's network through the VPN with a compromised password.[14] The hackers left a ransom note on Colonial Pipeline's computers threatening to release almost 100 gigabytes of data unless Colonial Pipeline paid the hackers a $4.4 million ransom using cryptocurrency.[15] Colonial Pipeline paid the ransom to the Russia-associated group known as DarkSide; however, the fuel pipelines were down for nearly a week, causing long lines and higher prices at gas stations.[16] After paying the ransom, Colonial Pipeline stated that the hackers never accessed the computer networks that controlled the flow of its fuel.[17] While the attack on the Colonial Pipeline ultimately caused relatively minimal harm, it shows just how quickly a major disaster can occur when companies do not implement adequate cybersecurity practices.

Major cyber incidents like SolarWinds and Colonial Pipeline will likely always make national headlines while hundreds of thousands of attacks go underreported every year. The FBI's Internet Crime Complaint Center received over 791,000 complaints from the American public in 2020, with reported losses of over $4.1 billion.[18] Ransomware attacks alone cost local, state, and federal governments and agencies an estimated $915 million, with cybercrimes expected to have caused around $6 trillion in damages globally in 2021.[19]

---

12. *What is a VPN? – Virtual Private Network*, CISCO, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (last visited May 10, 2022) ("[A] VPN[] is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.").

13. William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 3:58 PM), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

14. *See id.* (exposing how the password was later "discovered inside a batch of leaked passwords on the dark web").

15. *Id.*

16. *Id.*

17. *Id.*

18. U.S. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2020 3 (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (reporting a "69% increase in total complaints from 2019").

19. *See* The State of Ransomware in the US: Report and Statistics 2020, EMSISOFT BLOG (Jan. 18, 2021), https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/ (estimating $915 million in damages from 113 reported attacks on

With hundreds of thousands of victims, billions of dollars lost, and threats Do to national security, it is surprising to learn that only a fraction of cybercriminals are ever charged and convicted of a crime.[20] For every cybercrime reported to agencies like the FBI's Internet Crime Complaint Center, many more go unreported.[21] The lack of reporting may come from the fact that victims are often reimbursed by their banks, "[s]o it may never occur to most victims even to report the crime."[22] But the lack of reporting is also likely due to the fact that criminal enforcement of cybercrimes is extremely difficult, so victims are less likely to report the crime if they know that a criminal conviction is unlikely.

Part of the difficulty in enforcing laws against cybercriminals is because of their location.[23] One police officer explained that "[o]ur closure rates are below 10 percent, because I can't call a police department or prosecutor 800 miles away and ask them to invest all these resources to bring a criminal to our jurisdiction to be charged with a crime."[24] Additionally, local law enforcement agencies tend to lack the training and technological capabilities to handle cybercrimes.[25] Both state and federal law enforcement agencies face jurisdictional and resource-related issues in prosecuting cybercrimes because the perpetrators have the advantage of being located across state or international borders.[26] While cybercriminals continue to evade charges more people, businesses, and organizations are harmed by cyberattacks.

---

local, state, and federal governments and agencies); Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

20. *See* MIKE EOYANG, ALLISON PETERS, ISHAN MEHTA & BRANDON GASKEW, THIRD WAY, TO CATCH A HACKER: TOWARD A COMPREHENSIVE STRATEGY TO IDENTIFY, PURSUE, AND PUNISH MALICIOUS CYBER ACTORS 2 (2018), https://thirdway.imgix.net/pdfs/override/To_Catch_A_Hacker_Report.pdf (stating that an estimated less than 1% of cybercriminals of "malicious cyber incidents" are ever arrested, with likely even fewer being convicted).

21. *See* POLICE EXEC. RSCH. F., THE ROLE OF LOCAL LAW ENFORCEMENT AGENCIES IN PREVENTING AND INVESTIGATING CYBERCRIME 1 (2014), https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf ("[T]he head of the FBI's Cyber Division . . . estimates that only about [ten] percent of all incidents are reported to IC3.").

22. *Id.*

23. *See id.* (noting that perpetrators of cybercrimes often live far away from the victims).

24. *Id.*

25. *See* Maggie Brunner, *Challenges and Opportunities in State and Local Cybercrime Enforcement,* 10 J. NAT'L SEC. L. POL'Y 563, 565 (2020) (explaining that federal agencies can typically only assist in prosecution and investigations of major cybercrimes).

26. *See id.*

Charging and convicting cybercriminals plays an important role in mitigating threats to both the private sector and the federal government. However, preventing these cyber incidents from occurring in the first place would be preferable. One of the setbacks the United States faces in preventing cyberattacks is the current patchwork of regulations and laws that create the United States' cybersecurity requirements, which leaves much of the private sector unregulated.[27] Because the private sector owns the majority of the critical infrastructure across the country,[28] there is a need for the federal government to impose comprehensive and multi-disciplinary cybersecurity regulations that will defend against future cybersecurity threats.

Following the SolarWinds and Colonial Pipeline attacks, President Biden released an Executive Order on actions federal agencies and the private sector can take to strengthen the nation's cybersecurity.[29] The Executive Order includes mandatory changes for federal agencies and private sector partners and voluntary measures for the private sector in general.[30] While President Biden's Executive Order will create beneficial changes for federal agencies and their partners, there is still a lack of mandatory regulations on the private sector, which will create a greater national security threat to the critical infrastructure as time goes on.

This Comment discusses how the current cybersecurity rules are too limited and how President Biden's Executive Order, created in part to address these limitations, does not go far enough. Part I of this Comment evaluates the effectiveness of current cybersecurity laws and regulations under the authorities of the Department of Health and Human Services (HHS), the Federal Trade Commission (FTC), the Federal Acquisition Regulation (FAR) Council, and the Cybersecurity and Infrastructure Security Agency (CISA). Part II looks at President Biden's Executive Order

27. *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1506 (2013) ("Companies are essentially on their own when it comes to protecting their computer systems, with the government neither imposing security requirements nor bearing a share of the resulting costs.").

28. *See Critical Infrastructure Sector Partnerships*, CISA, https://www.cisa.gov/critical-infrastructure-sector-partnerships (last visited May 10, 2022) ("The private sector owns and operates a vast majority of the nation's critical infrastructure . . . ."). *But see* Paul Rosenzweig, *Is it Really 85 Percent?*, LAWFARE (May 11, 2021, 11:21 AM), https://www.lawfareblog.com/it-really-85-percent (discussing how the often-cited statistic of "85[%] of the nation's critical infrastructure is owned by the private sector" has no known factual basis, and the percentage of what the private sector owns is unknown).

29. *See* Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,633 (May 12, 2021) (describing that the United States faces persistent cyber threats, and the federal government and private sector will have to partner to adequately protect the nation).

30. *See* discussion *infra* Part II.

and how it will improve cybersecurity for federal agencies but falls short for the private sector's critical infrastructure. Part III recommends actions to adequately protect the critical infrastructures' cybersecurity.

I. EXISTING FEDERAL CYBERSECURITY STATUTES AND REGULATIONS

Most federal cybersecurity statutes and regulations apply to specific industries. Currently, these industries include the healthcare, financial, and federal sectors.[31] Within the federal sector, there are additional regulations and statutes that cover industries and people not included in other rules.

A. Healthcare Sector

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorizes HHS to create cybersecurity regulations for the healthcare sector.[32] While HIPAA is best known to patients for its requirement that healthcare providers do not disclose patients' protected health information (PHI), it also authorizes HHS to regulate the security of that information.[33] HHS developed the HIPAA Security Rule to require "covered entities" to protect electronic PHI (e-PHI) when it is "create[d], receive[d], maintain[ed], or transmit[ted]."[34] Each covered entity must conduct risk analyses and management evaluations, use unique user identifications, and ensure e-PHI is properly protected when transmitted.[35] However, covered entities are not required to encrypt e-PHI; change their passwords; have a periodic update for their security; or set "procedures for guarding against, detecting, and reporting malicious

31. *See* Leonard Wills, *A Very Brief Introduction on Cybersecurity Regulations/Standards: Part 1*, A.B.A. (Jan. 30, 2020), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/a-very-brief-introduction-on-cybersecurity-regulations-standards-1/.

32. Health Insurance Portability and Accountability Act (HIPAA) of 1996 § 261, 42 U.S.C. § 1320d note.

33. 42 U.S.C. § 1177(a)(1)–(3) (describing how patients' information can be wrongfully disclosed); *id.* § 264(c)(1) (explaining that the Department of Health and Human Services could only create the regulations if Congress did not pass legislation that adequately protected patients' information within three years).

34. *See* Security and Privacy, 45 C.F.R. § 164.104(a) (defining a covered entity as "(1) A health plan. (2) A health care clearinghouse. (3) A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter" and particular business associates).

35. *See* 45 C.F.R. §§ 164.306, 164.312 (listing additional security standards that are both required and voluntary).

software."[36] Although each covered entity must follow the standards and requirements set forth in the regulations, the individual entity chooses which software and programs it will use to reasonably implement these requirements.[37]

As COVID-19 continues to overburden hospitals, rising numbers of malware attacks increase concern over hospitals' cybersecurity abilities.[38] In September 2020, Universal Health Services, a hospital network of over 400 hospitals, shut down computer systems for 250 hospitals after Russian hackers placed ransomware on their networks in what is thought to be the largest healthcare cyber incident.[39] While the cyberattack did not directly harm patients, the hospital was forced to postpone surgeries and divert ambulances away.[40] Although there has been no credible report of a patient dying from a cyberattack on a hospital, it seems to be only a matter of time as hospital cyberattacks increase.[41] Though protection of PHI remains a concern when hospitals are the victims of a cyberattack, the physical safety of patients is increasingly threatened.[42] With hospitals increasing their reliance on computers for both patient records and care, HHS's standards and requirements for hospitals' cybersecurity fall short.[43]

---

36. *See id.* §§ 164.306, 164.308, 164.312 (recognizing that these security standards should be implemented if it is considered "reasonable and appropriate" for the covered entity).

37. *See id.* § 164.306(b) (allowing covered entities to consider their size, cybersecurity capabilities, and cost in choosing how they will implement the requirements).

38. *See* Melanie Evans & Robert McMillan, *Cyberattacks Cost Hospitals Millions During Covid-19*, WALL ST. J. (Feb. 26, 2021, 12:18 PM), https://www.wsj.com/articles/cyberattacks-cost-hospitals-millions-during-covid-19-11614346713 (detailing various cyberattacks and noting that many more publicly traded companies choose not to report the incidents).

39. *See id.* (noting that the malware attack cost Universal Health $67 million before taxes); Nicole Perlroth, *Officials Warn of Cyberattacks on Hospitals as Virus Cases Spike*, N.Y. TIMES (Oct. 28, 2020), https://www.nytimes.com/2020/10/28/us/hospitals-cyberattacks-coronavirus.html (explaining that it was the same hackers responsible for the "TrickBot" ransomware attacks).

40. Aaron Holmes, *More Than 250 Hospitals Across the US have been Debilitated by a Cyberattack that Forced Staff to Cancel Surgeries and Work with Pen and Paper*, INSIDER (Sept. 29, 2020, 4:09 PM), https://www.businessinsider.com/uhs-cyberattack-hack-derails-surgeries-at-hospitals-across-us-2020-9.

41. *See* Kevin Collier, *Baby Died Because of Ransomware Attack on Hospital, Suit Says*, NBC NEWS (Sept. 30, 2021, 7:16 PM), https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465 (reporting on a lawsuit that alleges that a baby died after receiving "severely diminished care" because the hospital's computers were down from a cyberattack).

42. *See* Kevin Poulsen & Melanie Evans, *The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: 'They Do Not Care'*, WALL ST. J. (June 10, 2021, 11:50 AM), https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215 (noting that cyberattacks at hospitals have caused patient monitor alerts to go down, stopped elective surgeries, and delayed patients' access to care).

43. *See id.*

All regulations under the Security and Privacy Rules apply to e-PHI.[44] Though a patient's e-PHI contains sensitive information that may be of interest to hackers, using ransomware to freeze all the computers in a hospital until the hospital pays the ransom seems to be the current preferred method of hackers.[45] The cybersecurity requirements for e-PHI likely benefit a hospital's overall cybersecurity, but hospitals and the greater healthcare sector have to address their cybersecurity systems as a whole, not just patient information security, to prevent future cyberattacks.

B. Financial Sector

Within the financial sector, the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect customers' "nonpublic personal information."[46] Pursuant to its GLBA authority, the FTC created the Safeguards Rule, which supplies industry-specific regulations for financial institutions.[47] After relying on the same standard for nearly twenty years, the FTC amended the Safeguards Rule at the end of 2021, which will become effective on December 9, 2022.[48]

The current Safeguards Rule requires companies to create an "information security program" to assess the risks of their operations, including evaluating the network and software used, how they prevent and respond to attacks, and how they train their employees.[49] The level of security required of each financial institution varies based on the risks and size of the institution.[50]

Financial institutions have been at the center of countless news stories reporting that millions of customers' personal information, such as Social

44. Security and Privacy, 45 C.F.R. § 164.302 (2020) ("A covered entity . . . must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.").

45. *See* Perlroth, *supra* note 39 (listing several hospitals that went offline as hackers held their information hostage).

46. Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–09 (defining nonpublic information as information "provided by a consumer to a financial institution; resulting from any transaction with the consumer . . . or otherwise obtained by the financial institution" and discussing permitted and prohibited uses and disclosures of it).

47. *See* 15 U.S.C. §§ 6801(b), 6804(a)(1)(C) (authorizing the Federal Trade Commission (FTC) to promulgate rules to protect nonpublic personal information); Safeguards Rule, 16 C.F.R. § 314 (2020) (mandating the elements of a GLBA-compliant information security program, which includes annual penetration and vulnerability tests on information systems).

48. *See* Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,272 (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314); Wills, *supra* note 31.

49. Safeguards Rule, 16 C.F.R. §§ 314.3–4.4 (2020).

50. *See id.* § 314.3(a).

Security numbers, birthdates, and addresses, had been stolen in a cyber incident.[51] Hackers can use personal information to apply for credit cards, steal identities, or sell to other criminals.[52] These types of attacks can be very damaging to an individual, and the financial institution may be liable for damages.[53] Individuals will be better protected when all financial institutions meet the same sector-specific cybersecurity requirements.

Although personal information hacks are more common, an attack that affects a major financial institution's computer system or data could cause a threat to national security and create economic instability.[54] The likelihood of a successful cyberattack against a major financial institution is unlikely because those institutions invest heavily in cybersecurity and often have additional cybersecurity regulations compared to smaller financial institutions.[55] Many major financial institutions are members of the National Securities Clearing Corporation (NSCC) under the Securities and Exchange Commission, which provides risk management, settlement, and "a guarantee of completion for virtually all broker-to-broker trades."[56] However, to be a member of the NSCC, financial institutions must confirm that their cybersecurity programs "meet standard industry best practices and guidelines."[57] This requirement provides the larger financial institutions with

51. *See* Jordan Valinsky, *7 of the Biggest Hacks in History*, CNN BUS. (July 30, 2019, 12:08 PM), https://www.cnn.com/2019/07/30/tech/biggest-hacks-in-history/index.html (discussing the hacks of Equifax and Capital One that potentially compromised 243 million accounts).

52. *See* Ravi Sen, *Here's How Much Your Personal Information is Worth to Cybercriminals – and What They do With It*, PBS NEWS HOUR (May 14, 2021, 12:04 PM), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it (identifying that 86% of cyberattacks are motivated by money).

53. *See* THOMAS M. EISENBACH, ANNA KOVNER & MICHAEL JUNHO LEE, FED. RSRV. BANK OF N.Y., CYBER RISK AND THE U.S. FINANCIAL SYSTEM: A PRE-MORTEM ANALYSIS 6–8 (2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf (describing the potential consequences of various types of cyberattacks for the financial institution and its customers).

54. *See id.* at 2–3, 5 (discussing that the top five most active banks account for nearly 50% of all payments, and if one of those banks faced a major cyberattack that lasted for five days, nearly 40% of the banking sector would be impaired, with an "average liquidity shortfall . . . of $1 trillion by the fifth day").

55. *See id.* at 33–34 (observing that top financial institutions dedicate large amounts of money and resources to defend against cyberattacks).

56. Self-Regulatory Organizations; National Securities Clearing Corporation; Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program, 84 Fed. Reg. 68,243, 68,244 (Dec. 13, 2019).

57. *Id.* at 68,246.

greater protection against cyber threats compared to the requirements found in the GLBA.[58] Therefore, smaller banks or clearinghouses are likely an easier target because they have fewer resources to invest in cybersecurity and only have to comply with the GLBA's minimum cybersecurity requirements.[59] Major financial institutions stand a better chance against cyberattacks, largely because of their heightened cybersecurity protocols, but even those heightened protocols have proven inadequate.[60] The FTC recognized the current regulations' ineffectiveness and strengthened the requirements accordingly to further protect American consumers and institutions.[61]

The 2021 Amendments significantly strengthen the Safeguards Rule. The most impactful changes include requiring multi-factor authentication; a written risk assessment and incident response; annual penetration testing; and encrypting data in transit and at rest.[62] These new requirements "represent proven elements of effective data security programs" and will reduce the number of successful cyberattacks for all financial institutions.[63] Additionally, the 2021 Amendments bridge the cybersecurity gap between large and small sized institutions created by the current Safeguards Rule, which threatens the whole financial sector.[64] The FTC should enact its

58. *Id.*

59. *See* EISENBACH, KOVNER & LEE, *supra* note 53, at 34 (emphasizing that smaller financial institutions likely do not have the resources to defend against a significant cyberattack).

60. *See id.* at 33–34; Press Release, Lina M. Khan, Chair, & Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter Regarding Regulatory Review of the Safeguards Rule Commission File No. P145407, at 2–3 (Oct. 27, 2021), https://www.ftc.gov/system/files/documents/public_statements/1598006/statement_of_chair_lina_m_khan_joined_by_commr_slaughter_regarding_regulatory_review_of_safeguards_0.pdf (noting Equifax's massive breach, "which the FTC alleged was caused by inadequate data security that could have been easily corrected by the company").

61. *See* Khan & Slaughter, *supra* note 60, at 1.

62. Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,272, 70,307 (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314).

63. *See* Khan & Slaughter, *supra* note 60, at 3, 5. *But see* Standards for Safeguarding Customer Information, 86 Fed. Reg. at 70,301 (providing an exception to the regulations for financial institutions that maintain information on fewer than 5,000 consumers).

64. *See* EISENBACH, KOVNER & LEE, *supra* note 53, at 34–36 (stating that a cyberattack against a small or medium sized financial institution could cause a top five financial institution to fall below its liquidity threshold 72% to 100% of days respectively). *Compare* 16 C.F.R. §§ 314.3–4.4 (2020) (describing the FTC's minimum cybersecurity requirements for all financial institutions from the GLBA), *with* Self-Regulatory Organizations; National Securities Clearing Corporation; Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program, 84 Fed. Reg. 68,243, 68,243 (Dec. 13, 2019) (approving the National Securities Clearing Corporation's cybersecurity requirements for mainly large financial institutions).

recently-proposed security event reporting requirement to prevent another twenty-year delay in modernizing financial sector cybersecurity regulations.[65] It should then use the collected data to evaluate the effectiveness of the amended regulations and shape future amendments.[66]

C. Federal Sector

Despite the numerous statutes and regulations governing the federal sector, many federal agencies have failed to fulfill their cybersecurity obligations.[67] Some of these statutes and regulations also apply to the private sector, which must meet specific cybersecurity standards when contracting with the federal government.[68] Additionally, federal criminal laws, such as the Computer Fraud and Abuse Act (CFAA), are available to prosecute cybercriminals but have left prosecutors, judges, and defendants confused as to when they apply.[69]

1. Federal Agencies

The Federal Information Security Modernization Act of 2014 (FISMA) largely governs federal sector cybersecurity.[70] FISMA requires federal agencies to report information security incidents annually to Congress, allows CISA to issue "binding operational directives" to other agencies, and mandates that each agency develop and implement information security programs based on its unique risks to safeguard federal information.[71] Should an agency fail to comply with FISMA requirements, the Office of Management and Budget (OMB) may consequently recommend a reduction

---

65. Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,062, 70,063–64 (proposed Dec. 9, 2021) (to be codified at 16 C.F.R. pt. 314) (mandating notification of the FTC of a breach impacting more than 1,000 consumers).

66. *See id.* at 70,063.

67. This Comment only focuses on the federal civilian Executive Branch. An analysis including the military and intelligence community is beyond the scope of this Comment.

68. *See, e.g.*, Basic Safeguarding of Covered Contractor Information, FAR 52.204-21 (2021) (requiring federal contractors to employ certain information system safeguards).

69. *See* Computer Fraud and Abuse Act of 1986 (CFAA), 18 U.S.C. § 1030; Joseph Marks, *Breyer's Supreme Court Replacement Will Face a Hefty Cyber Docket*, WASH. POST (Jan. 28, 2022, 7:24 AM), https://www.washingtonpost.com/politics/2022/01/28/breyers-supreme-court-replacement-will-face-hefty-cyber-docket/ (noting that questions about the CFAA remain even after the Court's recent ruling in *Van Buren v. United States*).

70. Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551–59.

71. *Id.* §§ 3552–54.

in appropriations.[72] Per FISMA, an agency's information security program should include periodic risk assessments, consistent implementation of policies and procedures across the agency, and an evaluation of how its policies and procedures work.[73] However, by 2019, very few agencies had created and implemented an effective information security program.[74]

Agencies continually fail to adequately protect federal information, opening themselves up to thousands of attacks on sensitive information.[75] In implementing their information security programs, many agencies have struggled to design effective policies and procedures for detecting and protecting against threats to their cybersecurity framework.[76] In the 2018 fiscal year, federal agencies reported over 31,000 incidents to the United States Computer Emergency Readiness Team.[77] Attacks through email, phishing, or "website or web-based application[s]" accounted for most attacks by unauthorized users in these incidents.[78] Although many agencies are better at consistently implementing and managing their policies and procedures for responding to and recovering from cybersecurity incidents,

---

72. 40 U.S.C. § 11303 (enumerating the Office of Management and Budget's (OMB's) enforcement authority).

73. *See* 44 U.S.C. § 3554(b) (listing the different factors an agency can include in its information security program).

74. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-288, HIGH-RISK SERIES: FEDERAL GOVERNMENT NEEDS TO URGENTLY PURSUE CRITICAL ACTIONS TO ADDRESS MAJOR CYBERSECURITY CHALLENGES 44 (2021) [hereinafter HIGH-RISK SERIES] (pointing out that only five out of twenty-three inspectors general reported that their agency had an effective information security program).

75. *See generally* Michael Adams, *Why the OPM Hack is far Worse than You Imagine*, LAWFARE (Mar. 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine (reporting how a breach of the Office of Personnel Management led to hackers accessing information included in SF-86 forms, which includes highly sensitive data used to grant security clearances).

76. *See* HIGH-RISK SERIES, *supra* note 74, at 44–45 (reporting that eleven out of twenty-three agencies had only formalized and documented their policies and procedures, and no agencies had optimized their procedures).

77. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-545, FEDERAL INFORMATION SECURITY: AGENCIES AND OMB NEED TO STRENGTHEN POLICIES AND PRACTICES 6–7 (2019) (explaining that federal agencies are required to report these incidents to the U.S. Computer Emergency Readiness Team).

78. *Id.* at 8. While "improper usage" by persons with authorization comprised the largest single category of information security incidents, the Supreme Court has recently made a point to distinguish these from hacking. *See generally* Van Buren v. United States, 141 S. Ct. 1648 (2021) (finding that the CFAA only prohibits the access of information beyond one's authorization, not misuse of information one may access).

the majority of agencies evaluated still did not meet the qualifications needed to be considered effective.[79] The Government Accountability Office (GAO) has given thousands of recommendations to federal agencies over the years to strengthen cybersecurity; however, hundreds of those recommendations have gone unimplemented.[80] If federal agencies continue to ignore FISMA's requirements, guidance from the GAO, and the binding operational directives from CISA, cyber incidents against federal agencies will continue to occur, and individual federal agencies will not be trusted to create and implement their own cybersecurity programs.

2. *Private Sector Partners*

Attempting to further prevent cyber incidents, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA 2015 Act).[81] Under the CISA 2015 Act, the Department of Homeland Security (DHS) can share "classified cyber threat indicators and defensive measures" with the private sector.[82] Additionally, private sector companies can voluntarily share cyber threat indicators with the federal government without being concerned with violating antitrust laws, losing proprietary information, or losing any applicable privileges provided by the law, as long as it is for a "cybersecurity purpose."[83] Cyber threat indicators include information that describes or identifies "malicious reconnaissance," ways to exploit security vulnerabilities, or the potential future harm caused by a cyber incident.[84] The DHS tasked CISA, an agency within the DHS, with managing the requirements under the CISA 2015 Act.[85]

---

79. *See* HIGH-RISK SERIES, *supra* note 74, at 45 fig.9 (showing that only a total of ten agencies had an effective program for either the respond or recover function).

80. *See id.* at ii (noting that about 3,300 recommendations have been given since 2010 but more than 750 have not been implemented).

81. Cybersecurity Information Sharing Act (CISA) of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015) (codified at 6 U.S.C. §§ 1501–10).

82. *See* 6 U.S.C. § 1502.

83. *See id.* §§ 1501, 1503–04 ("The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."). This protection follows from joint Department of Justice-FTC statements made a year before Congress passed the CISA 2015 Act. *Justice Department, Federal Trade Commission Issue Antitrust Policy Statement on Sharing Cybersecurity Information*, U.S. DEP'T OF JUST. (Apr. 10, 2014), https://www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing.

84. *See, e.g.*, 6 U.S.C. § 1501(6)(A) ("malicious reconnaissance"); *id.* § 1501(6)(B) ("exploitation of a security vulnerability"); *id.* § 1501(6)(F) ("actual or potential harm").

85. OFF. INSPECTOR GEN., OIG-20-74, DHS MADE LIMITED PROGRESS TO IMPROVE

However, there has been criticism over the effectiveness of the CISA 2015 Act. First, the private sector states that the cyber threat indicators shared did not provide enough details to properly manage or prevent any of the potential threats indicated.[86] Second, as of 2018, only 219 private sector organizations participated in the Automated Indicator Sharing (AIS) program.[87] CISA created the AIS to fulfill its information sharing requirements, enabling "[a]ll federal and non-federal entities, as well as foreign governmental and foreign private sector entities" to participate in sharing cyber threat indicators to CISA and participating members.[88] Third, almost none of the AIS participants have shared cyber threat indicators with CISA in return.[89] For private sector organizations, "only 2 of 188 AIS participants (1 percent) shared cyber indicators with CISA in 2017, and only 9 of 252 participants (3 percent) shared indicators in 2018."[90] Although cyber threat indicators can also be shared through a web form and email, CISA claims that the cyber threat indicators are not as detailed as participants want because CISA is understaffed and does not receive an adequate number of indicators from the private sector.[91]

Additionally, while increasing the federal government and private sectors' access to cyber threat information is generally beneficial, it is less so when those in the private sector are incapable of implementing the recommended changes. In a 2020 survey, nearly 75% of corporate legal departments had not established ways to use the information sharing policies from the CISA 2015 Act.[92] The majority of these companies said that their "organization does not have the resources or knowledge base to engage in these types of

---

INFORMATION SHARING UNDER THE CYBERSECURITY ACT IN CALENDAR YEARS 2017 AND 2018 (2020) [hereinafter DHS LIMITED PROGRESS].

86. *See id.* at 10 (explaining that the cyber threat indicators had to be supplemented from third-party sources to be effective at preventing an attack).

87. *See id.* at 8; U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF JUST., GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 14 (2020) (highlighting that the Automated Indicator Sharing (AIS) program shares cyber threat indicators through a secure manner to CISA, who then sanitizes the information and shares with all other AIS participants).

88. DHS LIMITED PROGRESS, *supra* note 85, at 2–3.

89. *See id.* at 12.

90. *Id.*

91. *See id.* at 11.

92. Daniel Sutherland, *What is a Cybersecurity Legal Practice?*, LAWFARE (Apr. 2, 2021, 11:10 AM), https://www.lawfareblog.com/what-cybersecurity-legal-practice.

programs."[93] It is clear from Congress passing the CISA 2015 Act that the federal government wants to enhance the nation's cybersecurity and prevent cyberattacks; however, the current method of voluntary information sharing has not been as beneficial as Congress might have envisioned because of the lack of participation and criticism from the private sector participants.

Aside from the mainly voluntary measures the CISA 2015 Act places on the private sector, the federal government can also control the private sector's cybersecurity standards when the two parties enter a contract. When the federal government contracts with the private sector, the FAR Council requires the private sector to implement cybersecurity standards to protect the government's information.[94] Any federal contractor that "processes, stores, or transmits" information not available for public release, such as "facts, data, or opinions," must follow the FAR Council's regulations.[95] Some of the required regulations include limiting an authorized user's access to only the functions the user needs, updating software to protect against malicious code when it is released, limiting the number of connections to outside systems, creating subnetworks that separate internal networks and publicly accessible system components, and escorting facility visitors who could have physical access to devices.[96] These safeguards are only considered a minimum standard, with each contract having additional requirements depending on the agency and contract.[97] Unlike the information sharing in the CISA 2015 Act, these cybersecurity measures are mandatory for any private sector organization that partners with the federal government to help defend against any national security threats that could stem from a hack of a private sector partner.[98]

While requiring cybersecurity standards for private sector partners is valuable, the partners must implement these standards. Recently, the Department of Justice (DOJ) announced that it would launch a new Civil Cyber-Fraud Initiative that would focus on prosecuting cases against government contractors who do not comply with the stated cybersecurity requirements.[99] The DOJ said that

93. *Id.*

94. *See* Basic Safeguarding of Covered Contractor Information, FAR 52.204-21 (2021) (expanding upon the standards and measures that the private sector must implement to contract with the federal government).

95. *See id.*

96. *See id.* (elaborating that the safeguarding requirements listed in this subsection are only a baseline level requirement and additional cybersecurity measures are expected of private sector partners).

97. *See id.*

98. *See id.*

99. *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, U.S. DEP'T

government contractors have failed to report cybersecurity breaches, fraudulently represented their cybersecurity systems, and provided deficient cybersecurity products.[100] While the DOJ's initiative will primarily focus on civil remedies to address the actions of government contractors, prosecutors can also use federal criminal laws to charge cybercriminals.[101] Establishing clear enforcement guidelines against private sector partners will ensure the cybersecurity standards are well-executed and federal information is properly protected.

3. Federal Criminal Laws

The CFAA is the primary federal law that criminalizes cybercrimes.[102] The CFAA criminalizes accessing a "protected computer without authorization" or when "exceed[ing] authorized access"[103] for seven categories of criminal activities.[104] Specific acts in these categories could include obtaining information from financial institutions, threatening to impair the availability of data in return for money, delivering information about protected foreign relations material, and transmitting a program or code that intentionally damages a computer.[105] The CFAA is broadly applicable and can be used to charge defendants in nearly any situation.

OF JUST. (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (describing that the initiative will help create a more resilient cybersecurity and will reimburse taxpayers for damages caused by contractors).

100. *See id.*

101. *See id.* ("The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.").

102. *See* CFAA, 18 U.S.C. § 1030; Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010) (describing that the CFAA has become so broad that it potentially regulates "every computer in the United States").

103. *See* 18 U.S.C. § 1030(a)(4), (e)(6) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]"); Timothy Edgar, *Why* Van Buren *is Good News for Cybersecurity*, LAWFARE (Aug. 4, 2021, 10:18 AM), https://www.lawfareblog.com/why-van-buren-good-news-cybersecurity ("These separate crimes are designed to cover distinct types of malicious cyber activity: outside intrusions into a computer or computer network (accessing without authorization), and insider threats (exceeding authorized access).").

104. OFF. OF LEGAL EDUC. EXEC. OFF. FOR U.S. ATT'YS, PROSECUTING COMPUT. CRIMES 3 (2010) (listing the categories as "Obtaining National Security Information, Accessing a Computer and Obtaining Information, Trespassing in a Government Computer, Accessing a Computer to Defraud & Obtain Value, Intentionally Damaging by Knowing Transmission, Recklessly Damaging by Intentional Access, Negligently Causing Damage & Loss by Intentional Access, Trafficking in Passwords, [and] Extortion Involving Computers").

105. *See* 18 U.S.C. § 1030.

Prosecutors have used the CFAA to charge some of the most well-known cyberhackers that threatened the United States' national security and critical infrastructure.[106] For example, the indictment of Paige Thompson included seven counts of violating the CFAA for allegedly accessing Capital One's servers without authorization.[107] Thompson accessed Capital One's servers by exploiting a weakness in misconfigured firewalls to gain access to over 100 million customers' information.[108] Likewise, Julian Assange's federal indictment included a count of violating the CFAA for allegedly conspiring with Chelsea Manning to access a government computer without authorization and in excess of Manning's authorized access to obtain classified information on documents relating to national defense.[109] While Thompson's and Assange's cases may be clear examples of violating the CFAA's "without authorization" and "exceeding authorized access" terms, courts have struggled in deciding where and how the CFAA applies because of the broad language used in the statute.[110]

Recently, the Supreme Court attempted to narrow the CFAA's scope by further defining "exceeding authorized access."[111] The Supreme Court held that a person exceeds authorized access when they "obtain information from particular areas in the computer—such as files, folders, or databases—to which

106. *See* Timothy H. Gray, Ethan Kisch & Michael F. Buchanan, *Capital One Hack Prosecution Raises New and Old Questions About Adequacy of CFAA*, PATTERSON BELKNAP (Sept. 9, 2019), https://www.pbwt.com/data-security-law-blog/capital-one-hack-prosecution-raises-new-and-old-questions-about-adequacy-of-cfaa (discussing how the CFAA was used to charge Paige Thompson and Julian Assange).

107. Superseding Indictment at 5–7, 16–17, United States v. Thompson, No. CR19-0159RSL (W.D. Wash. June 17, 2021).

108. *See id.* at 2–4, 8 (explaining that Capital One's customer information included personal identifying information, such as Social Security numbers and bank account numbers).

109. Superseding Indictment at 35–36, United States v. Assange, No. 1:18-cr-00111 (CMH) (E.D. Va. May 23, 2019).

110. *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1077 (9th Cir. 2016) (holding that Power Ventures continued to access Facebook via Facebook-owned computers "without authorization" after receiving a cease and desist letter because Facebook's user information was not publicly available); HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 992, 1000 (9th Cir. 2019) (holding that HiQ did not access LinkedIn "without authorization" after receiving a cease and desist letter because LinkedIn's information is publicly available); United States v. Rodriguez, 628 F.3d 1258, 1260, 1263 (11th Cir. 2010) (holding that Rodriguez "exceeded authorized access" by obtaining personal identifying information of people for nonbusiness related reasons, which went against the workplace's policy); United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (holding that Nosal did not access his workplace's database "without authorization" when obtaining confidential information, even though it went against the workplace's policy).

111. Van Buren v. United States, 141 S. Ct. 1648 (2021).

their computer access does not extend."[112] This interpretation is considered a "gates-up-or-gates-down" approach, which means that a user does not exceed their authorized access, regardless of their motive for accessing the information, if there is no password or technological restriction preventing their access to the computer, network, or files.[113] This would protect employees who violate their workplace's computer-use policies, perhaps by checking personal email or the news, or people who continue to visit a website in violation of its terms and conditions from being charged with federal crimes for these infractions.[114]

The suggested gates-up-or-gates-down approach would provide prosecutors and judges with a clear understanding of when the CFAA applies. However, in a footnote, the Supreme Court noted on the gates-up-or-gates-down approach that it "need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[115] This footnote muddles the definition of "exceeding authorized access" that would have resulted from a purely technological approach.[116] Now, technological limits appear to be the main, but not the only, factor in considering whether someone has exceeded their authorized access.[117] Ambiguity still exists as to when, how, and to what degree courts can consider contract- or policy-based limits in determining whether someone has exceeded their authorized access. These ambiguities hinder a company's cybersecurity when it is unsure of how extensive its cybersecurity protections must be before the protection of the law begins.

Under the CFAA's broad language, journalists, activists, and social media users have become convicted criminals.[118] The CFAA creates harsh penalties where violators with no criminal history may face decades in federal prison.[119] When first enacted, the CFAA's protections only

112. *Id.* at 1652.

113. *See id.* at 1652, 1658 (reasoning that "improper motives" do not contribute to whether someone has "exceed[ed] authorized access").

114. *See id.* at 1661 (describing that "millions of otherwise law-abiding citizens" would be considered criminals if the government's definition was used).

115. *Id.* at 1659 n.8.

116. 18 U.S.C. § 1030(a)(1), (a)(7)(B), (e)(10).

117. *See* Orin Kerr (@OrinKerr), TWITTER (June 3, 2021, 1:10 PM), https://twitter.com/OrinKerr/status/1400500114569916422.

118. *See* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015, 7:00 AM), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/ (discussing charges brought against Aaron Swartz, Matthew Keys, Lori Drew, and others under the CFAA).

119. *See* Noam Cohen, *A Data Crusader, a Defendant and Now, a Cause*, N.Y. TIMES (Jan. 13,

covered government computers, financial records, and national security information.[120] However, over the course of several amendments, the CFAA has become the broad, overarching statute it is today, even with the new judicially drawn limits.[121] Because of this broadness, prosecutors may be overzealous or overly cautious in their approach of using the statute for charging defendants, neither of which is beneficial to an equitable administration of the law.[122] The CFAA seemingly tries to cover all computers and crimes in a single statute, which is unworkable in today's digitally powered world.[123] Rather than depending on criminal laws to protect companies, government computers, national security information, or individual users, Congress should prioritize measures that improve cybersecurity and prevent unwanted access.

II. PRESIDENT BIDEN'S EXECUTIVE ORDER ON STRENGTHENING THE NATION'S CYBERSECURITY

On May 12, 2021, President Biden released an Executive Order on "Improving the Nation's Cybersecurity."[124] President Biden discussed how the federal government needs to improve its cybersecurity to better respond to and prevent major cyber incidents from occurring.[125] He also stressed that the private sector needs to update its cybersecurity to create a safer and more secure cyber environment for the nation at large.[126] The Executive Order lays out several actions to achieve this goal.

2013), https://www.nytimes.com/2013/01/14/technology/aaron-swartz-a-data-crusader-and-now-a-cause.html (describing that Aaron Swartz was charged under the CFAA and faced over thirty years in prison and up to $1 million in fines for using M.I.T.'s computers to download scholarly papers from JSTOR before he died by suicide).

120. Kerr, *supra* note 102, at 1564.

121. *See id.* at 1564–71 (analyzing the amendments to the CFAA, such as the Economic Espionage Act of 1996 and the USA Patriot Act of 2001).

122. *See* ADRIAAN LANNI, CAROL STEIKER & ELIZABETH MORONEY, HARV. L. SCH., PROSECUTORIAL DISCRETION IN CHARING AND BARGAINING: THE AARON SWARTZ CASE (A) 8 (2014) (explaining how prosecutors continued seeking criminal punishment for Aaron Swartz using the CFAA after JSTOR indicated it had no interest in Swartz's prosecution); Gray, Kisch & Buchanan, *supra* note 106 (noting that prosecutors may pair CFAA charges with other statutes to prevent an entire case from being dismissed by a judge).

123. *See* Kerr, *supra* note 102, at 1571 ("[I]t may be no exaggeration to say that a 'protected computer' now just means a 'computer.'").

124. Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

125. *Id.* at 26,633.

126. *Id.*

A. Changes to Federal Agencies

The bulk of the Executive Order focuses on changes to the "Federal Civilian Executive Branch [(FCEB)] Agencies."[127] Three of the major changes for federal agencies include moving toward zero trust architecture (ZTA), standardizing the federal government's playbook, and creating the Cyber Safety Review Board.[128] Each of these changes will have varying levels of impact on President Biden's goal of strengthening the nation's cybersecurity.

1. Zero Trust Architecture

ZTA system design implements several factors to help limit access to compromised networks.[129] Typically, under the ZTA system, authorized users are limited to only accessing the resources necessary to complete their job functions.[130] "The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."[131] Agencies can implement ZTA systems by securing communications regardless of network location and limiting access to resources based on observable characteristics, such as the "software versions installed, network location, time/date of request," and current network credentials.[132] Under President Biden's Executive Order, federal agencies must implement a ZTA system based on the guidelines given by the National Institute of Standards and Technology (NIST).[133]

While implementing a ZTA system has the potential to greatly increase the federal government's cybersecurity, the logistics of implementation raise significant concerns. Developing a ZTA system across all federal agencies will

---

127. *See id.* at 26,645 ("[T]he term 'Federal Civilian Executive Branch Agencies' or 'FCEB Agencies' includes all agencies except for the Department of Defense and agencies in the Intelligence Community.").

128. *See id.* at 26,635–37, 26,641 (mandating that federal agencies take comprehensive action on increasing cybersecurity).

129. *See id.* at 26,646.

130. *See* SCOTT ROSE, OLIVER BORCHERT, STU MITCHELL & SEAN CONNELLY, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-207, ZERO TRUST ARCHITECTURE 4 (2020) [hereinafter ZERO TRUST ARCHITECTURE] (explaining a zero trust architecture (ZTA) system's goals of "prevent[ing] unauthorized access to data and services coupled with making the access control enforcement as granular as possible").

131. Exec. Order No. 14,028, 86 Fed. Reg. at 26,646 (May 12, 2021).

132. ZERO TRUST ARCHITECTURE, *supra* note 130, at 6.

133. Exec. Order No. 14,028, 86 Fed. Reg. at 26,636.

be a substantial undertaking. A federal agency has to identify all the people working with its resources; manage all of its devices, including computers, phones, user accounts, and applications; and evaluate and rank its resources to determine when access can be granted.[134] Additionally, upon initial implementation, the ZTA system may restrict a user's access to an unnecessarily narrow set of resources.[135] Implementing a ZTA system within each federal agency will be very time-intensive, so a hybrid ZTA approach, where some users or departments still have access to resources not necessary to their job functions, may alleviate this strain.[136] However, as federal agencies successfully implement ZTA systems, the systems will help prevent data breaches and limit the potential damage to the agency and its information.[137]

2. *Standardizing the Federal Government's Playbook*

Executing the ZTA system will likely be a long and complicated process; however, standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents will be an easier process. Currently, under FISMA, each federal agency determines how to respond to cybersecurity incidents and vulnerabilities based on the risk and harm that would occur from accessing, disrupting, or destroying its information.[138] Under President Biden's Executive Order, the federal government's playbook will require all FCEB agencies to "incorporate all appropriate NIST standards" with CISA approving any deviations from the playbook.[139] Such standardization will "ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses."[140]

In response to the Executive Order, CISA created two different playbooks: the Incident Response Playbook and the Vulnerability Response

---

134. *See* ZERO TRUST ARCHITECTURE, *supra* note 130, at 38–39 (evaluating access requests beyond database maintenance, configuration management, and monitoring).

135. *See id.* at 40 (noting that few policies are complete in their first iterations to make sure the policies are effective and workflow is manageable).

136. *See id.* at 36 (explaining that it is more difficult to implement a "pure zero trust architecture" in existing federal agency networks).

137. *See id.* at 1 (describing that ZTA can limit "internal lateral movement[s]," which would limit what information an attacker could access).

138. *See* Federal Information Security Modernization Act of 2014 § 2(a), 44 U.S.C. § 3554.

139. Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,642–43 (May 12, 2021) (illustrating how requiring CISA to approve any deviations will safeguard against any one federal agency having a greater threat risk than another agency).

140. *Id.* at 26,642.

Playbook.[141] The Incident Response Playbook sets out the process that agencies will follow when they confirm that a malicious cyber event has occurred, and the Vulnerability Response Playbook will standardize the process agencies follow "when responding to urgent and high priority vulnerabilities[.]"[142] When agencies implement these playbooks, they will ensure that all FCEB agencies have the proper minimum protections and will help prevent future cyber incidents.[143]

3. *Creating the Cyber Safety Review Board*

The creation of the Cyber Safety Review Board, which will review both federal agency and non-federal agency threats and vulnerabilities, will help prevent further cyber incidents.[144] The Director of CISA will appoint members to the Cyber Safety Review Board, to include federal officials from the Department of Defense, the DOJ, the National Security Agency, the FBI, and cybersecurity or software suppliers in the private sector.[145] Combining members from the federal government and the private sector means better and more practicable recommendations, which will help prevent future cyber incidents.

The Cyber Safety Review Board will likely act similarly to the National Transportation Safety Board (NTSB).[146] The NTSB investigates, determines the probable cause, and provides recommendations to prevent future accidents from occurring for every civil aviation accident and other major accidents

---

141. CISA, *Executive Order on Improving the Nation's Cybersecurity*, https://www.cisa.gov/executive-order-improving-nations-cybersecurity (last visited May 10, 2022) ("Agencies should use these playbooks to help shape overall defensive cyber operations to ensure consistent and effective response and coordinated communication of response activities.").

142. *Id.*

143. *See id.* ("A standardized response process ensures that agencies, including CISA, can understand the impact of confirmed malicious cyber activity as well as critical and dangerous vulnerabilities across the federal government.").

144. *See* Exec. Order No. 14,028, 86 Fed. Reg. at 26,641–42 (explaining that the board will give recommendations on how to improve cybersecurity after major cyber incidents).

145. *See id.* at 26,641; Notice of the Establishment of the Cyber Safety Review Board, 87 Fed. Reg. 6,195, 6,195 (Feb. 3, 2022).

146. *See* Steven M. Bellovin & Adam Shostack, *Finally! A Cybersecurity Safety Review Board*, LAWFARE (June 7, 2021, 11:23 AM), https://www.lawfareblog.com/finally-cybersecurity-safety-review-board (describing how many cybersecurity experts have called for the creation of a cybersecurity board and have identified aspects of the National Transportation Safety Board (NTSB) that experts want in the Cyber Safety Review Board, such as reports not being used in court proceedings, having a dedicated investigation staff, and looking at both technical and organizational factors for determining the cause).

involving the "highway, marine, pipeline, and railroad."[147] The NTSB reports provide detailed information that airlines and other transportation entities can use to make effective policy and procedural changes to improve safety,[148] unlike the current cyber incident threat reporting done by CISA.[149] If the Cyber Safety Review Board is as effective as the NTSB, there will be a great improvement to both federal and private sector cybersecurity.[150]

B. Changes to the Private Sector

Although most policies and requirements included in President Biden's Executive Order are mainly focused on federal agencies, President Biden's goals of enhancing the software supply chain security and reducing barriers to information sharing will directly impact the private sector.[151] Between the two changes, the consumer labeling pilot program, which is part of enhancing the software supply chain security, will likely have the greatest impact on the private sector.

1. Enhancing Software Supply Chain Security

President Biden stated that the "development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors."[152] The Executive Order lists extensive requirements, guidelines, and standards for federal contractors and the broader private sector to improve software security.[153] Though "critical software" is currently the priority, the entire software supply chain is subject to this regulation.[154]

---

147. *Who We Are and What We Do*, NTSB, https://www.ntsb.gov/Pages/home.aspx (last visited May 10, 2022) (explaining that factors for determining major accidents include mass casualties, high profile accidents, or the involvement of public transportation).

148. *See* Bellovin & Shostack, *supra* note 146 ("[A] good NTSB report will look at *all* of the myriad technical and organizational factors that contributed to what happened.").

149. *See supra* note 84 and accompanying text.

150. *See* Bellovin & Shostack, *supra* note 146 (illustrating that more information is needed to know to what extent the Board will be beneficial, but it is a step in the right direction).

151. *See* Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,633–35, 26,637–42.

152. *Id.* at 26,637.

153. *See id.* at 26,637–42.

154. *See id.* at 26,637; *Critical Software – Definition & Explanatory Material*, NIST (July 9, 2021), https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory ("EO-critical software . . . is designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing

The first action in enhancing the software supply chain security is addressing the minimum standards required for testing software source code.[155] This generally applicable guideline from the Executive Order recommends that the NIST put forth "minimum standards for vendors' testing of their software source code."[156] The NIST produced five minimum standards that vendors should use, including "threat modeling," "static (code-based) analysis," "dynamic analysis," correcting discovered bugs, and assuring that packages and services are as secure as the code.[157] While vendors should have already used these guidelines, the guidelines will "serve as a basis for mandated standards in the future."[158] However, because these standards are already broadly used, they are not likely to create a substantial change in the software supply chain.

Additionally, the NIST published standards and procedures to assist in enhancing the software supply chain for critical software.[159] The NIST has five objectives and twenty security measures that apply to all critical software, platforms, users, data, or networks.[160] The objectives include: protecting the critical software and platforms from unauthorized access and use; protecting data used by critical software; protecting critical software from exploitation; quickly responding to threats of critical software; and strengthening "the understanding and performance of humans' actions that foster the security" of critical software.[161] Comprehensive implementation of these security measures will demonstrate whether these actions can create beneficial changes for critical software.

Moreover, CISA will provide agencies with a list of software the federal government uses that already complies with the standards given by the NIST.[162] After May 2022, the FAR Council will amend the federal government's contracting language to require that all software sold to

---

resources; is designed to control access to data or operational technology; performs a function critical to trust; or, operates outside of normal trust boundaries with privileged access.").

155. *See* Exec. Order No. 14,028, 86 Fed. Reg. at 26,637.

156. *Id.* at 26,640.

157. NAT'L INST. OF STANDARDS & TECH., NISTIR 8397, GUIDELINES ON MINIMUM STANDARDS FOR DEVELOPER VERIFICATION OF SOFTWARE 4–5 (2021).

158. *Id.* at 3.

159. *See* Exec. Order No. 14,028, 86 Fed. Reg. at 26,637–38 (requiring the National Institute of Standards and Technology (NIST) to publish guidelines based on recommendations from other federal agencies, the private sector, and other appropriate members of the software supply chain field); *Security Measures for EO-Critical Software Use*, NIST (July 9, 2021), https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use [hereinafter *EO-Critical Software*].

160. *See EO-Critical Software*, *supra* note 159 (grouping security measures by objective).

161. *See id.*

162. Exec. Order No. 14,028, 86 Fed. Reg. at 26,639.

federal agencies complies with the Executive Order.[163] Requiring critical software to meet these security measures will incentivize private companies to comply with the requirements in future contracts with the federal government. This will also improve the cybersecurity of critical infrastructure controlled by the private sector as more options for adequate software that meets cybersecurity standards become available.

The last major guidance on enhancing the software supply chain that will impact the private sector is the consumer labeling program, which will provide information about the software and devices consumers purchase.[164] The consumer labeling program tells consumers whether the software or device meets minimum cybersecurity requirements, or if the software or device has certain desirable cybersecurity attributes the consumer wants.[165] The NIST's proposed labels for software include user data security, encryption, software integrity, and software design and development.[166] Device label options include device-specific cybersecurity education, data security, and limiting interface access.[167] While the consumer labeling program will begin as a pilot program, it could become a fully approved program.[168] If the labeling program is successful, users can make informed decisions about their software and be confident that they will be adequately protected based on their needs.

---

163. *See id.* at 26,639–40.

164. *See id.* at 26,640 (referring specifically to the "security capabilities of Internet-of-Things (IoT) devices and software development practices"); *see also* Andrew Meola, *A Look at Examples of IoT devices and Their Business Applications in 2022*, INSIDER INTELLIGENCE (Jan. 10, 2022, 4:17 PM), https://www.insiderintelligence.com/insights/internet-of-things-devices-examples/ (defining IoT as the "network of connected objects that are able to collect and exchange data in real time using embedded sensors[, such as t]hermostats, cars, lights, [and] refrigerators").

165. *See* NAT'L INST. OF STANDARDS & TECH., DRAFT BASELINE SECURITY CRITERIA FOR CONSUMER IOT DEVICES 1 (2021), https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf (explaining that not all consumers are looking for, or need, the same levels of security, so the labels will help customers choose the software that best fits their needs).

166. *See* NAT'L INST. OF STANDARDS & TECH., RECOMMENDED CRITERIA FOR CYBERSECURITY LABELING OF CONSUMER SOFTWARE 10–15 (2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-1.pdf [hereinafter LABELING OF CONSUMER SOFTWARE].

167. *See* NAT'L INST. OF STANDARDS & TECH., RECOMMENDED CRITERIA FOR CYBERSECURITY LABELING FOR CONSUMER INTERNET OF THINGS (IOT) 5–6, 10 (2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf [hereinafter LABELING FOR CONSUMER INTERNET OF THINGS].

168. *See* Exec. Order No. 14,028, 86 Fed. Reg. at 26,640–41 (clarifying that the Director of NIST will review the consumer labeling program after a year and will then determine what improvements need to be made to move forward with the program).

The consumer labeling program will function similarly to the Environmental Protection Agency's Energy Star certification, which provides a simple way for consumers to choose energy-efficient household products.[169] The consumer labeling program could potentially create a far-reaching impact in the private sector without using direct regulations.[170] Just as with the Energy Star certification, software companies will want to advertise the government certifications that state their software meets a variety of cybersecurity standards. Ideally, market forces would eventually drive most software companies to meet a baseline cybersecurity standard to remain competitive in the market, which would benefit consumers and the private sector and prevent future destructive cyberattacks.

2. *Information Sharing*

By removing the barriers to sharing threat information,[171] the Executive Order may exact an ultimately positive impact on the private sector. While the CISA 2015 Act already includes how private sector entities can share cyber threat indicators with the federal government,[172] the Executive Order expands who must share what information.[173] Specifically, the Executive Order looks at the language the FAR Council requires in contracts with IT and operational technology (OT) service providers and how that language can be modified to better facilitate the sharing of threat information.[174]

---

169. *See* Chloe Albanesius, *Biden Calls for Government-Wide 2FA, Energy Star-Type Labels for Software*, PCMAG (May 13, 2021), https://www.pcmag.com/news/biden-calls-for-government-wide-2fa-energy-star-type-labels-for-software. *See generally What is ENERGY STAR*, ENERGY STAR, https://www.energystar.gov/about?s=mega (last visited May 10, 2022). NIST recommends that a binary label, the same method used for Energy Star certification, is used in conjunction with a layered approach to provide more detailed information online about the product. *See* LABELING OF CONSUMER SOFTWARE, *supra* note 166, at 24–25; *see also* LABELING FOR CONSUMER INTERNET OF THINGS, *supra* note 167, at 19.

170. *Cf. ENERGY STAR Impacts*, ENERGY STAR, https://www.energystar.gov/about/origins_mission/impacts (last visited May 10, 2022) (explaining that most American households have purchased an Energy Star certified product, approximately 75,000 products meet the Energy Star certification, and thousands of companies partner with the Environmental Protection Agency to create energy efficient products and solutions).

171. Exec. Order No. 14,028, 86 Fed. Reg. at 26,633–35.

172. *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501(6) (defining the term cyber threat indicators).

173. *See* Exec. Order No. 14,028, 86 Fed. Reg. at 26,633–34 (explaining that information technology (IT) and operational technology (OT) service providers that contract with the federal government can share cyber threat information with CISA and the FBI).

174. *Id.*

Additionally, the Executive Order seeks to have the FAR Council require that IT and OT service providers share certain information with CISA and the FBI.[175] This information sharing system will differ from the CISA 2015 Act because it will be mandatory, rather than voluntary, for service providers contracting with the federal government.[176] How effective this new information sharing program is will depend on how broadly the FAR Council interprets what cyber incidents require reporting. If the contractor language is narrowly defined and bases the rest of the cyber incident reporting on voluntary measures, this information sharing program will likely be as ineffective as the information sharing program from the CISA 2015 Act.[177] However, if the FAR Council broadly defines which cyber incidents must be reported, IT and OT service providers' information given to CISA and the FBI will actually help federal agencies prevent and respond to cyber incidents.[178] This information sharing can help strengthen private sector partners' cybersecurity.

III. RECOMMENDATIONS FOR IMPROVING CYBERSECURITY

The federal government has relied on outdated, minimal, or voluntary regulations and laws for cybersecurity protection for too long. It should act to make broadly applicable mandatory cybersecurity statutes and regulations, rather than only focusing on mandatory provisions for the federal government and with its contractors. Specifically, the critical infrastructure owned by the private sector needs to be properly regulated to protect against national security threats.

A. Critical Infrastructure Regulations

Because much of the nation's critical infrastructure is owned and operated by private companies, the federal government should, at a minimum, create mandatory cybersecurity standards for the critical infrastructure sectors.[179] CISA is described as "the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future."[180] CISA is

175. *See id.* at 26,633–35 (stating that the Department of Homeland Security (DHS), the National Security Agency, the Attorney General, and the Director of OMB will recommend what types of information the Federal Acquisition Regulatory Council should require IT and OT service providers to share).

176. *See* 6 U.S.C. §§ 1503–04.

177. *See supra* text accompanying notes 86–91.

178. *See* Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,633.

179. *See supra* note 28 and accompanying text.

180. *Site Resources*, CISA, https://www.cisa.gov/site-resources (last visited May 10, 2022).

currently housed under the DHS; however, to give cybersecurity the attention necessary to protect and defend the nation's national security and critical infrastructure, CISA should become its own federal agency.[181] As part of the statute creating CISA as its own agency, Congress can authorize CISA to make the comprehensive and detailed cybersecurity regulations needed for the critical infrastructure. Given this general authority by Congress, CISA could base its regulations on its current guidelines and recommendations to better regulate the private sector and to protect the nation's critical infrastructure from future cybersecurity threats.

To best facilitate proper cybersecurity regulations, this Comment also recommends adding a new title in the *Code of Federal Regulations* (C.F.R.) for the specific subject matter of cybersecurity.[182] The C.F.R. already contains individual titles for such subjects as agriculture, energy, highways, and public health.[183] With the way technology, computers, and the Internet have become so relied upon for all facets of life, an individual title in the C.F.R. is necessary to properly regulate cybersecurity, rather than having cybersecurity regulations spread throughout different titles.[184] CISA already has the authority to give "binding operational directives" on cybersecurity matters to other federal agencies under FISMA.[185] With this authority, it would be logical for CISA to be charged with drafting the proposed regulations.[186]

---

181. *See* Tatyana Bolton & Bryson Bort, *America Deserves a Cabinet-Level Department of Cybersecurity*, HILL (June 30, 2021, 1:00 PM), https://thehill.com/opinion/cybersecurity/560920-america-deserves-a-cabinet-level-department-of-cybersecurity (describing that the politicization of DHS, manipulation of cybersecurity standards to fit the DHS narrative, and budget size all contribute to why CISA should become its own agency).

182. *See generally About the Code of Federal Regulations*, GOVINFO, https://www.govinfo.gov/help/cfr (last visited May 10, 2022) ("The C[.]F[.]R[.] is divided into [fifty] titles that represent broad areas subject to [f]ederal regulation.").

183. *See* 7 C.F.R., 10 C.F.R., 23 C.F.R., 42 C.F.R. (2021).

184. *See* 45 C.F.R. § 164.306 (2021) (HIPAA cybersecurity regulations); 16 C.F.R. §§ 314.3–.4 (2021) (financial sector cybersecurity regulations); FAR 52.204-21 (2021) (federal government cybersecurity regulations for private sector contractors). *See generally* CAMILLE RYAN, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2016 4, 6 (2018), https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf (presenting that among households who owned a computer in 2016, 76% owned a smartphone and 58% owned a tablet).

185. Federal Information Security Modernization Act of 2014 § 2(a), 44 U.S.C. § 3553(b)(2).

186. *Cf.* 2 C.F.R. §§ 1.215, .300 (describing how OMB's prior circulars formed the basis for most of Title 2, which contributed to OMB being responsible for issuing Title 2, similar to CISA being responsible for developing the new regulations using its binding operational directives).

Under the cybersecurity title, CISA would provide the broad overarching rules that apply generally to the private sector controlling the critical infrastructure under "Subtitle A." These regulations would include such rules as requiring password updates, using multi-factor authentication, creating IT security procedures, and protecting backup data.[187] While these general cybersecurity requirements can apply to all sectors, it will be important to have unique regulations for each critical infrastructure sector to give the detailed cybersecurity that is needed.

The critical infrastructure covers a wide array of sectors, each with differing and specific needs.[188] If a single chapter in the C.F.R. attempted to cover all cybersecurity regulations and was only managed by CISA, it would be more difficult to have the sector-specific definitions and applications necessary. Additionally, relying on CISA to enforce all the cybersecurity regulations could become quite burdensome. Therefore, under "Subtitle B," there would be sixteen chapters—one chapter for each critical infrastructure sector where sector-specific regulations are addressed and managed by the sector-specific agency.[189] Currently, the National Infrastructure Protection Plan (NIPP) is similarly designed but addresses a broader range of total infrastructure protection and can only provide guidance to those in the private sector.[190] However, the NIPP's framework can be utilized to help create the unique sector-specific regulations needed to prevent a cyberattack.[191]

Furthermore, making CISA its own federal agency will permit a bigger budget and additional staff to expand its private sector training and evaluations.[192] Specifically, CISA could hire more cybersecurity advisers

187. *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CYBER ESSENTIALS STARTER KIT 2 (2021), https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf (describing CISA's guidance to the private sector on baseline cybersecurity recommendations).

188. *See Critical Infrastructure Sectors*, *supra* note 2 and accompanying text.

189. *See* Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 651(5) (defining sector-specific agencies as agencies responsible "for providing institutional knowledge and specialized expertise of a sector"); *cf.* 2 C.F.R. Subtitle B (2021) (giving regulatory effect to the OMB guidance in 2 C.F.R. Subtitle A and incorporating additional agency-specific grant and agreement regulations).

190. *See 2015 Sector-Specific Plans*, CISA, https://www.cisa.gov/2015-sector-specific-plans (last visited May 10, 2022) (highlighting how sector-specific plans address each critical infrastructure sector's unique cybersecurity risks, from climate change to aging infrastructure).

191. *See id.* (stating that the National Infrastructure Protection Plan is developed in collaboration with both sector-specific agencies and the private sector).

192. *See* Bolton & Bort, *supra* note 181 (noting that CISA has "limited resources" and a "shoe-string budget").

for the private sector with these additional resources.[193] Recognizing that many smaller local companies may operate critical infrastructures, expanding CISA's budget and hiring more cybersecurity advisers will allow for CISA to provide additional help to the companies who do not have the resources or skills necessary to fully implement the new regulations. A larger budget and staff will ensure a better implementation of the regulations across the sectors as companies adjust to the rules.

B. Enforcement of Cybercrimes

The CFAA, with its numerous amendments, has become too broad and generalized to be effectively implemented.[194] Rather than criminalizing all types of cyberattacks in one statute, the statute should be broken into more specific statutes that only apply in certain circumstances and to certain computers. Breaking up the CFAA into more specific statutes should include removing some of the criminal penalties in exchange for civil penalties. CISA and sector-specific agencies could monitor these civil penalties under the cybersecurity title in the C.F.R. CISA could then define terms like "without authorization" and "exceeding authorized access" to make it clear to people and courts when someone is violating the CFAA or regulations.[195] If Congress wanted to still provide criminal penalties for certain offenses, it could base any further amendments to the CFAA or other cybercrime laws on CISA's definitions.

Additionally, CISA could help private sectors develop their "gates-up or gates-down" approach so it is clear when violations of the CFAA occur.[196] Currently, an argument against the Supreme Court's decision defining "exceeding authorized access" is that companies rely on contracts and policies to stop employees from accessing information they do not need because it is expensive and logistically complex to implement the necessary technological barriers.[197] However, CISA can use its cybersecurity advisors

193. Tim Starks, *CISA Starts Identifying Targets Most Necessary to Protect from Hacking*, CYBERSCOOP (Oct. 29, 2021), https://www.cyberscoop.com/sici-easterly-katko-psies-csis-cisa/ (stating how Director Jen Easterly wants CISA's budget to be expanded to $5 billion to help hire more key personnel).

194. *See* Kerr, *supra* note 117, at 1561–62 (arguing that the CFAA is potentially unconstitutional under the void-for-vagueness doctrine).

195. *See* 18 U.S.C. § 1030; Kerr, *supra* note 117, at 1573 (describing how vague statutes can leave people unaware that their conduct is illegal).

196. Van Buren v. United States, 141 S. Ct. 1648, 1659 (2021).

197. Bryan Cunningham, John Grant & Chris Jay Hoofnagle, *Fighting Insider Abuse After* Van Buren, LAWFARE INST. (June 11, 2021, 12:53 PM), https://www.lawfareblog.com

for the private sector to help companies create and implement these barriers. Companies placing such technological barriers around their information will help with both insider and outsider cybersecurity threats.[198] Likewise, with the Supreme Court's footnote making it uncertain if companies can rely on contracts and policies, it will best serve companies to establish technological barriers if they want to ensure that the CFAA provides a criminal punishment for someone's actions.[199]

To further expand the enforcement options for cybercrimes, and because cybercriminals can be located across international borders, the United States federal government should continue partnering with other countries in sharing information and extraditing alleged cybercriminals.[200] Because the expansion of cybersecurity surveillance risks violating people's privacy and human rights, the federal government should ensure that strong safeguards are in place to prevent such violations from occurring before joining any international agreement.[201] The federal government should not support any international cyber agreements that would allow oppressive governments to restrict Internet access and expression; put journalists, opposition leaders, and human rights defenders at risk; and increase improper surveillance of citizens.[202] Tackling the threats of international cybercrimes is important to protecting countries' citizens and national security but should not come at the cost of violating those citizens' human rights.[203]

/fighting-insider-abuse-after-van-buren (explaining the difficulties of deterring insider access to confidential internal information).

198. *See id.* (explaining that modern technological controls can do more to protect information than the CFAA without the threat to civil liberties).

199. *See supra* note 110 and accompanying text (explaining how companies are more at risk and technological barriers could better safeguard against hackers and cyberattacks).

200. *See* Convention on Cybercrime, arts. 23–24, Nov. 23, 2001, C.E.T.S. No. 185 (stating that each country joining the Budapest Convention will cooperate in sharing information and agreeing to what crimes are extraditable).

201. Deborah Brown, *Cybercrime is Dangerous, but a New UN Treaty Could be Worse for Rights*, JUST SEC. (Aug. 13, 2021), https://www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights/ (describing that limiting data collection to "what is strictly necessary for a legitimate purpose would limit people's vulnerability").

202. *Id.*

203. *See id.* ("Addressing the increasing threat of cybercrime while protecting rights is an urgent issue that few governments manage to get right.").

CONCLUSION

Many large corporations and organizations may go above the minimum standards and regulations put in place by federal statutes and regulations for cybersecurity.[204] Nevertheless, as the Internet continues to create a more interconnected world, regulators need to promulgate more specific rules and regulations on cybersecurity that broadly apply to all Internet users to minimize national security threats.

The current federal cybersecurity statutes and regulations have done little for the prevention and protection against cyberattacks for the critical infrastructure.[205] Most of these statutes and regulations were written in the 1980s to the early 2000s, so contemporary guidelines for today's Internet-dependent society simply do not exist.[206] President Biden's Executive Order will help strengthen and update the federal government and private sector's cybersecurity, but the change is still not as broad and expansive as needed.[207] The laws and regulations are still too far behind for how quickly the Internet and technology changes and develops.

The patchwork of cybersecurity statutes and regulations will only be solved by creating broadly applicable rules and regulations that impact most Internet users. However, the current priority should be addressing the national security threats coming from those in the private sector who control the critical infrastructure and are underregulated. The federal government cannot continue to rely on this patchwork of requirements to protect the nation's national security. The SolarWinds and Colonial Pipeline attacks should be cautionary tales of what can happen to more businesses in the private sector and federal agencies if the federal government continues to rely on outdated and inadequate rules and regulations.

---

204. *See* EISENBACH, KOVNER & LEE, *supra* note 53 and accompanying text (noting how large companies are aware of the risk pertaining to their information).

205. *See supra* Part I (describing instances where the current regulations are insufficient and have failed to protect institutions and companies from cyberattacks).

206. *See supra* notes 103–105 and accompanying text (explaining the structure, purpose, and use of the CFAA for charging violators of the regulations).

207. *See supra* Part II.