Richmond Journal of Law & Technology Volume XXVI, Issue 1

COMPLEMENTARY APPROACHES OR CONFLICTING STRATEGIES? EXAMINING CISA AND NEW YORK'S DFS CYBERSECURITY REGULATIONS AS A HARMONIZING FRAMEWORK FOR A BILATERAL APPROACH TO CYBERSECURITY

By Richard Q. Sterns*

Cite as: Richard Q. Sterns, *Complementary Approaches or Conflicting Strategies? Examining CISA and New York's DFS Cybersecurity Regulations as a Harmonizing Framework for a Bilateral Approach to Cybersecurity*, 26 RICH. J.L. & TECH. no. 1, 2020.

ABSTRACT

The question of whether more aggressive approaches to the enforcement of cybersecurity standards can survive in a time where sharing threat information is crucial to protecting privacy has been ongoing for some time. This paper argues that this is not an either-or proposition and that enforcement frameworks like New York's DFS Cybersecurity Regulations and information sharing frameworks such as CISA can exist in harmony, and that their divergent approaches actually strengthen American cybersecurity law as a whole.

I. INTRODUCTION

[1] The ideal means for public and private sector actors to share cybersecurity threat information has been the subject of debate amongst policy makers at both the state and federal levels for more than a decade.[1] Policymakers and commentators have also offered different perspectives on subsidiary issues to information sharing: whether notice requirements to government entities should be required in the event of a cyber incident;[2] whether private sector actors should be immune from liability when sharing information or responding to cyber threats or vulnerabilities;[3] and

* Associate at Ballard Spahr LLP, J.D. 2018 Antonin Scalia Law School, George Mason University, B.A. 2014 Westminster College (MO) *magna cum laude*.

[1] *See* John Heidenreich, *The Privacy Issues Presented by the Cybersecurity Information Sharing Act*, 91 N.D. L. REV. 395, 409–10 (2016) (arguing that the type of information that could potentially be shared by private entities under the Cybersecurity Information Sharing Act (CISA) is too broad and lacks adequate privacy constraints); Paul Rosenzweig, *The Cybersecurity Act of 2015*, LAWFARE (Dec. 16, 2015, 2:59 PM), https://www.lawfareblog.com/cybersecurity-act-2015 [https://perma.cc/MY2L-9MN9] ("We have white smoke. Finally, after 8 years of discussion, Congress has passed a cybersecurity information sharing bill."). *But see* Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S.C.L. REV. 585, 596–97 (2016) (arguing that CISA lacks a sufficient "carrot" to encourage beneficial information sharing and that minimization procedures for privacy purposes should be shifted away from private sector entities and onto the government).

[2] *See* Brett V. Newman, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 U. ILL. J.L. TECH. & POL'Y 437, 457–58 (2015) (arguing that a strong federal standard is needed for data breach notification that would preempt state law regardless of whether information sharing is occurring and allow states who have already regulated in this area to feel comfortable with the standard). *But see* Paul Merrion, *New York's Tough Cybersecurity Rule Draws Hundreds of Comments*, CQ ROLL CALL, Nov. 18, 2016, 2016 WL 6818304, (arguing that the 72-hour data security notification requirement was unrealistic).

[3] *Compare* Jeffrey F. Anddicott, *Enhancing Cybersecurity in the Private Sector by Means of Civil Liability Lawsuits—The Connie Francis Effect*, 51 U. RICH L. REV. 857, 864–65, 878 (2017) (advocating for the creation of a cyber tort private right of action similar to that which spurred increased hotel and motel security standards following the Connie Francis sexual assault case and calling CISA an improvement but still too much of a

whether private sector entities should be required to have specific cybersecurity measures in place to protect the information of consumers and users.[4] High profile cyber-attacks in both the public and private sector have increased the intensity of the debate concerning the role of both sectors in combating cyber breaches through information sharing and others means. Famous breaches include the breach of the Office of Personnel Management's (OPM) computer systems exposing the personal information of 21.5 million people and the breach of Yahoo's servers resulting in the theft of 500 million users' account information.[5]

[2] Unsurprisingly, high profile cyber breaches such as those referenced above, have led to a bevy of proposed and enacted legislation

"hands off" approach), *with* Genna Promnick, *Cyber Economic Espionage: Corporate Theft and The New Patriot Act*, 9 HASTINGS SCI. & TECH. L.J. 89, 107–08 (2017) (arguing that CISA should be amended to allow private entities to be held liable by the Federal Trade Commission (FTC) if they fail to meet regulatory standards when sharing information but also arguing that private entities should be allowed to "hack back" in the event of a cyber breach).

[4] *See* Stephanie Balitzer, *What Common Law and Common Sense Teach Us About Corporate Cybersecurity*, 49 U. MICH. J.L. REFORM 891, 917–18 (2016) (Arguing that the Federal Communications Commission (FCC) and the Cyber Threat Intelligence Integration Center (CTIIC) should promulgate detailed comprehensive cybersecurity defense regulations). *But see* Jody Westby, *Cyber Legislation Will Cost Businesses & Hurt Economy*, FORBES (Feb. 27, 2012, 5:52 PM) https://www.forbes.com/sites/jodywestby/2012/02/27/cyber-legislation-will-cost-businesses-and-hurt-economy/#5e2a06491563 [https://perma.cc/KEW9-Y66Z] (arguing that government regulation cannot keep pace with evolving technology and that incentives rather than regulatory mandates would work better).

[5] *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0 [https://perma.cc/B98H-LV3B]; Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html [https://perma.cc/TUV5-WBU7].

and regulatory actions at both the federal and state level.[6] Setting aside the multitude of proposed and enacted reforms across the cybersecurity policy space, this article focuses primarily on two implemented pieces of cybersecurity policy: the Cybersecurity Information Sharing Act of 2015 (CISA) and the New York Department of Financial Services (NYDFS) Cyber Requirements for Financial Services Companies (the DFS Regulations), which went into effect in March 2017.[7] In particular, this article focuses on some of the most contentious issues in crafting cybersecurity policy where there are conflicting views—as between CISA and the DFS Regulations—such as the ideal method for information sharing and whether private entities should be mandated to notify the government in the event of certain cyber breaches, face liability for failing to meet regulatory standards, or be required to maintain specific cybersecurity measures.

[3] At the federal level, CISA's enactment was the culmination of two decades of debate on how to better respond to cyber threats.[8] In 1998, the

[6] To illustrate the multitude of attention that cybersecurity legislation and regulation has gotten in recent years, consider that in December 2014, a year notorious for partisan gridlock, Congress passed five different pieces of cybersecurity legislation including the National Cybersecurity Protection Act of 2014, the Federal Information Security Modernization Act of 2014, the Cybersecurity Enhancement Act of 2014, the Department Homeland Security (DHS) Cybersecurity Workforce and Retention Act, and the Cybersecurity Workforce Assessment Act. *See* Caleb Skeath, *Congress Passes Five Cybersecurity Bills*, COVINGTON & BURLING LLP (Dec. 12, 2014), https://www.insideprivacy.com/united-states/congress-passes-four-cybersecurity-bills/ [https://perma.cc/FCF5-2G8N].

[7] *See* Cyber Security Information Sharing Act, 6 U.S.C. §§ 1501–1510 (2018); Cyber Security Requirements for Financial Services Companies, 23 N.Y. COMP. CODES R. & REGS. Tit. 23, §§ 500.00-500.23 (2017). CISA was enacted as one Title of the Omnibus Appropriations Bill of 2015.

[8] *See* John Evangelakos & Brent J. McIntosh, *A Guide to The Cybersecurity Act of 2015*, LAW 360 (Jan. 12, 2016, 11:57 AM), https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015 [https://perma.cc/UJ8P-BEMU] ("For nearly two decades, information relating to potential cyberthreats has been shared through industry-specific information sharing and analysis centers. Despite the growth and importance of

Presidential Decision Directive 63 (PDD-63) asked each critical infrastructure sector of the American economy to create information sharing organizations to respond to cyber threats and vulnerabilities.[9] Since then, the question has loomed as to whether these information sharing and analysis centers (ISACs) adequately incentivize information sharing efforts.[10] Participating private entities and commentators argued that the potential risks associated with cyber information sharing, including potential civil liability, antitrust concerns, apprehensions about the protection of intellectual property, and proprietary business information necessitated Congressional action to further incentivize sharing cyber threat information.[11] Moreover, this call for action came despite the fact that many felt ISACs were a fairly beneficial development for cybersecurity overall.[12] After a stalemate over cybersecurity information sharing legislation that dragged on for years, CISA was finally passed and signed into law as Title N of the 2015 Omnibus Appropriations Bill.[13] As this article discusses later in detail, the "hands off" and voluntary approach to information sharing and cybersecurity that

ISACs, participants and commentators have expressed concern that perceived risks associated with information sharing—including potential civil liability, antitrust issues, and the protection of intellectual property and other proprietary business information—have limited the effectiveness of ISACs and other information-sharing efforts.").

[9] *See* Presidential Decision Directive NSC-63, Critical Infrastructure Protection (May 22, 1998), https://fas.org/irp/offdocs/pdd/pdd-63.htm [https://perma.cc/2T3C-DAJX] (discussing the purpose of ISACs). *See generally Critical Infrastructure Sectors*, U.S. DEP'T HOMELAND SECURITY, https://www.dhs.gov/critical-infrastructure-sectors [https://perma.cc/V7DS-25NF] (describing the 16 critical infrastructure sectors of the American economy).

[10] *See* Evangelakos & McIntosh, *supra* note 8; *see also* Presidential Decision Directive NSC-63, *supra* note 9.

[11] *See id.*

[12] See *id.*

[13] *See* Rosenzweig, *supra* note 1.

Congress took with CISA garnered widespread support from industry leaders but drew criticism from privacy advocates and some leading technology companies.[14] Both the privacy advocates and technology companies worried that loose minimization procedures and liability protections for all information shared with the government while meeting CISA's technical requirements, regardless of intent, did not do enough to protect consumers and users.[15]

[4] In New York, the DFS Cyber Security Regulations have been discussed since at least 2013 when the NYDFS began a series of surveys of regulated entities asking for information about their cybersecurity practices, "including corporate governance practices, frequency of and responses to cybersecurity breaches, cybersecurity budget and costs, third-party vendor safeguards, and future plans on cybersecurity."[16] In 2015, NYDFS made clear that cybersecurity was one of the agency's top priorities for the year and released broad guidance on what forthcoming regulations would entail, including required cybersecurity governance practices, requirements for third-party service providers, multi-factor authentication, personnel standards, annual audits and reports, and cyber

[14] *See* Robyn Greene, *Tech Industry Leaders Oppose CISA as Dangerous to Privacy and Security*, THE HILL (Oct. 21, 2015, 1:00 PM), http://thehill.com/blogs/pundits-blog/technology/257601-tech-industry-leaders-oppose-cisa-as-dangerous-to-privacy-and [https://perma.cc/368H-CSBE] [hereinafter *Tech Leaders Oppose CISA*] (noting that major technology companies such as Apple and SalesForce vocally opposed the legislation); *OTI Deeply Disappointed About Passage of Dangerous Cybersecurity Bill*, NEW AMERICA: OPEN TECH. INST. (Dec. 18, 2015), https://www.newamerica.org/oti/press-releases/oti-deeply-disappointed-about-passage-of-dangerous-cybersecurity-bill/ [https://perma.cc/6XLD-EHSS] [hereinafter *OTI Disappointed*] ("Today's final bill represents a significant blow to online privacy. . . ."); Rosenzweig, *supra* note 1.

[15] *See OTI Disappointed*, *supra* note 14; *Tech Leaders Oppose CISA*, *supra* note 14; Rosenzweig, *supra* note 1.

[16] H. Deen Kaplan et al., *New York Department of Financial Services Previews Rigorous Cybersecurity Rules for Financial Sector*, 21 CYBERSPACE LAW. NL 2 (2016).

incident reporting.[17] In September 2016, the first version of the proposed regulations was met with resistance from the industry, which submitted over 150 comments arguing that certain provisions of the regulations were unworkable and that a flexible risk-adjusted approach to compliance would be superior to minimum standards that disregard individualized aspects of the covered entity.[18] After reviewing comments, NYDFS made modifications towards a more flexible risk-adjusted approach and loosened encryption requirements for non-public information, while still mandating fairly strict notice requirements and retaining enforcement authority in the event of a cyber breach or non-compliance with the regulations.[19] When the final regulations went into effect on March 1, 2017, the financial services industry was still very wary of the increased regulatory burden.[20] New York Governor, Andrew Cuomo, and other commentators, touted the strict DFS Regulations as a cybersecurity model for other states and the nation.[21]

[17] *See id.*

[18] *See* Gretchen A. Ramos & Larry P. Schiffer, *New York Revamps Proposed Cybersecurity Regulation for Financial Services and Insurance Entities*, NAT. L. REV. (Jan. 3, 2017), http://www.natlawreview.com/article/new-york-revamps-proposed-cybersecurity-regulation-financial-services-and-insurance [https://perma.cc/SK5X-4F8F].

[19] *See id.*

[20] *See* Jon Oltsik, *New York State Cybersecurity Regulations: Who Wins?*, CSO: SECURITY SNIPPETS (Feb. 23, 2017, 10:59 AM), https://www.csoonline.com/article/3173689/security/ny-state-cybersecurity-regulations-who-wins.html [https://perma.cc/D2N6-C5U6].

[21] *See* Press Release, N.Y. State, Governor Cuomo Announces First-In-The Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions From Cyber-Attacks To Take Effect March 1 (Feb. 16, 2017) [hereinafter Governor Cuomo, Press Release], https://www.governor.ny.gov/news/governor-cuomo-announces-first-nation-cybersecurity-regulation-protecting-consumers-and [https://perma.cc/YHR6-5VQ6]; *see also* Jeff Kosseff, *New York's Financial Cybersecurity Regulation: Tough, Fair, and a National Model*, 1 GEO. L. TECH. REV. 436, 437 (2017) (discussing Governor Cuomo's 2016 remarks regarding cybersecurity regulations).

[5] Given the dissimilar cybersecurity methodologies employed by CISA, the DFS Regulations, and the different allies of each approach, it is reasonable to question whether the divergent regimes represent two irreconcilable paths for the future of cybersecurity law and policy in the United States. One path is driven by the trepidations of an industry understandably worried about risk management in an area where it is impossible to be perfect and another path is motivated by privacy concerns that have been amplified by recent cyber breaches. Although CISA and the DFS Regulations approach information sharing, notice, liability, and mandating the implementation of specific cybersecurity measures differently, this article argues that both are complementary approaches to the same cybersecurity concerns rather than opposing methodologies. This is true even in cases where their policy goals are in opposition. In addition, this article further contends that the different tactics chosen are not inherent dichotomies causing irreconcilable differences. Rather, the different tactics are foreseeable and arguably harmonizing results of the federal government's role in providing for the common defense of the United States, the historical precedent of strict state standards in data breach and privacy law, the divergent interests that motivate state regulators versus federal legislators, and the inherent differences between a statute of general applicability and regulations targeting a specific industry.

[6] The background section of this article reviews the pertinent provisions of CISA and the DFS Regulations, and discusses comments and concerns from both proponents and opponents of both regimes. The legal analysis section analyzes the contrasts between the two approaches and the policy preferences behind them, then continues with an argument for this article's central thesis: that CISA and the DFS Regulations are complementary and not incompatible. This argument is put forth by examining and focusing on the different roles the federal and state governments play in cybersecurity, the history of stricter state standards for data privacy, and the inherent differences in general versus industry-specific regulation.

II. BACKGROUND

[7] In arguing that the requirements of CISA and the DFS Regulations are complementary, it is important to first review the relevant provisions and comments from both proponents and opponents of the regimes. This will allow for a sense of the inherent tensions between legal frameworks for enhancing cybersecurity.

A. CISA Provisions on Information Sharing, Notice, Liability, and Implementing Specific Cybersecurity Measures

[8] This section will focus on the specific requirements in CISA related to information sharing, notice, liability, and implementing specific cybersecurity measures, and illustrate in some instances the fundamental divide between CISA and the DFS Regulations approaches to these issues.

1. Information Sharing

[9] There are a multitude of provisions enumerated in CISA that are related to information sharing, including the authorization to share and receive cyber threat indicators.[22] One of the most relevant provisions of CISA specifically states that it does not create a duty to share a cyber threat indicator[23] or defensive measure—with the government or another private entity—nor does it create a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure.[24] In addition, CISA takes pains to note that participation in the information sharing program designed by the Department of Homeland Security (DHS) under the statute, is entirely voluntary.[25] Further emphasizing the voluntary nature of the information sharing program, CISA includes a specific anti-tasking

[22] *See* 6 U.S.C. § 1503(c) (2018).

[23] *See* 6 U.S.C. § 1501(6) (2018) (defining cyber security threat indicator).

[24] *See* 6 U.S.C. § 1505(c)(1) (2018).

[25] *See* 6 U.S.C. § 1507(f) (2018).

restriction that prohibits a federal entity from requiring a non-federal entity to provide cyber threat information.[26] The anti-tasking restriction also prohibits federal entities from conditioning the sharing of cyber threat indicators it obtains through the program on a non-federal entity's participation in the information sharing program.[27] This particular information sharing provision of CISA has been criticized for creating a classic "free rider" problem, as non-federal entities may make use of cyber threat indicators shared by the federal government and other non-federal entities but are not required to share themselves.[28]

2. Notice

[10] CISA does not contain notice requirements that would require a non-federal entity to alert the federal government in the event of a cyber breach.[29] Since participation in CISA's information sharing program is voluntary,[30] the lack of a notice requirement is essentially a truism because any entity participating would have given notice to DHS or another private entity that they have identified a cyber threat indicator. Those entities not participating are clearly under no obligation to notify. Additionally, CISA exempts disclosure for state, local, and tribal governments participating in the program that might otherwise be compelled to disclose that they

[26] *See* 6 U.S.C. § 1507(h)(1) (2018).

[27] *See* 6 U.S.C. § 1507(h)(2) (2018).

[28] *See on the Current State of DHS Private Sector Engagement for Cybersecurity: Hearing Before H. Subcomm. on Cybersecurity and Infrastructure Protection*, 115th Cong. (2017) (statement of Scott Montgomery, Vice President and Chief Technical Strategist, Intel Security Group) (discussing the "free rider" problem in cyber security where all parties are allowed to consume threat intelligence but gain no direct value from providing it).

[29] *See* 6 U.S.C. § 1503(d)(4) (2018).

[30] *See* 6 U.S.C. § 1503(d)(4)(B) (2018).

shared a cyber threat indicator with the federal government under a local freedom of information law or sunshine act.[31]

3. Liability

[11] As referenced briefly in the Introduction, CISA contains broad liability protections for non-federal entities sharing cyber threat indicators with the federal government.[32] The statute provides an absolute bar on liability for non-federal entities, so long as they share the information in accordance with §1504(c)(1)(B).[33] Sharing in accordance with §1504(c)(1)(B) simply requires that the non-federal entity share the cyber threat indicators in accordance with the process that DHS is instructed to create by the statute.[34] The forms and procedures for sharing cyber threat indicators were finalized by DHS in June 2016, and are primarily concerned with the forms and systems used by non-federal entities to submit cyber threat indicators to DHS, the timeliness of such submissions, and the actions of non-federal entities who choose to connect directly to the DHS-managed system.[35] Although there is a compliance and record keeping burden on non-federal entities, meeting the minimum standards laid out by DHS, regardless of whether the information sharing was in good faith, forecloses any liability for the non-federal entity involved.[36] In

[31] *See id.*

[32] *See* Rosenzweig, *supra* note 1 ("Liability protection will now attend to any information sharing activity that is 'conducted in accordance' with the bill's provisions. Rejecting an intent test, this formulation seems to focus exclusively on the technical requirements for sharing—compliance with which should be relatively easy to document and prove.").

[33] *See* 6 U.S.C. § 1505(b)(2) (2018).

[34] *See* 6 U.S.C.S. §1504(c)(1)(B) (2018).

[35] *See* U.S. DEP'T HOMELAND SECURITY, FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT 3, 6–7 (2016) [hereinafter DHS FINAL PROCEDURES].

[36] *See id.* at 10–11.

addition, federal entities and state, local, and tribal governments are prohibited from using any of the information for regulatory or enforcement actions.[37] Moreover, the sharing of cyber threat indicators between private entities is specifically exempted from antitrust laws.[38]

[12] These far-reaching liability protections were a major area of contention in passing CISA.[39] On one hand, private entities argued that it would be difficult to justify participation in an information sharing program with the government without broad liability protections from private lawsuits and regulatory enforcement actions, particularly, sharing consumer information that is subject to consumer privacy laws.[40] On the other hand, privacy advocates and other commentators worried that the lack of liability for gross negligence or willful misconduct would give private entities too much protection and incentivize companies to adopt "lazy" processes that would permit personal information to flow to the government.[41]

[37] *See* 6 U.S.C. § 1504(d)(5)(D)(i) (2018).

[38] *See* 6 U.S.C. § 1503(e) (2018); *see also* 6 U.S.C. §1507(e) (2018) (clarifying prohibited conduct under cybersecurity law).

[39] *See* Melanie J. Teplinsky, *Fiddling on The Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 277–80 (2013) (arguing that voluntary sharing of cyber threat information is beneficial but also must properly incentivize businesses and limit the risks of sharing). *But see* Promnick, *supra* note 3, at 103–04 (arguing that CISA does not provide enough tools for effective cybersecurity to justify its infringement on privacy and civil liberties).

[40] *See* Kimberly Peretti, *Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?*, BLOOMBERG BNA: PRIVACY & SECURITY L. REP. 4–6 (2014) (arguing that there are several bodies of law whose norms run counter to having private businesses share cyber-threat information); ANDREW NOLAN, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS 13 (2015), https://fas.org/sgp/crs/intel/R43941.pdf [https://perma.cc/GV3V-4FWC] ("Without any overarching federal law governing private exchanges of cyber-threat information, the potential remains for various laws facially unrelated to cyber-information sharing to discourage such activity within the private sector.").

[41] Promnick, *supra* note 3, at 102–03.

4. Implementing Specific Cybersecurity Measures

[13] CISA also does not contain a requirement that private entities implement specific cybersecurity measures.[42] DHS established final procedures for sharing cyber threat indicators, which note that entities utilizing the CISA-authorized Automated Indicator Sharing (AIS) capability need to have certain technical infrastructure and specifications in order to utilize it.[43] However, this requirement does not obligate participating entities to utilize specific cybersecurity measures such as encryption, penetration testing, or vulnerability assessments.[44] CISA's lack of specific cybersecurity requirements for private entities has sparked debate about the proper role of the federal government in incentivizing private entities to improve cybersecurity, where they have historically under-invested.[45] Some commentators have argued that specific regulations pertaining to corporate cyber defense that require the use of certain tools are necessary to ensure the protection of both consumer information and corporate assets, and incentivize corporations to invest in cybersecurity infrastructure.[46] Others have argued that requiring private entities to have certain cybersecurity systems is an improper role for the federal government and a slippery slope towards massive regulatory overreach.[47]

---

[42] *See* Will Daugherty, *What Companies Need to Know About Cyber Threat Information Sharing Under CISA*, DATA PRIVACY MONITOR (May 19, 2016), https://www.dataprivacymonitor.com/cybersecurity/what-companies-need-to-know-about-cyber-threat-information-sharing-under-cisa/ [https://perma.cc/KVX7-7E9F].

[43] *See* DHS FINAL PROCEDURES, *supra* note 35, at 4.

[44] *See id.* (establishing procedures for sharing cyber threat indicators without providing specific cybersecurity requirements).

[45] *See* Promnick, *supra* note 3, at 90.

[46] *See* Balitzer, *supra* note 4, at 910, 916.

[47] *See* Westby, *supra* note 4.

B. DFS Regulations on Information Sharing, Notice, Liability, and Implementing Specific Cybersecurity Measures

[14] This section will focus on the specific requirements in the DFS Regulations related to information sharing, notice, liability, and implementing specific cybersecurity measures, and illustrate some of the tensions between risk-adjusted based cybersecurity methods and minimum standard based approaches to cybersecurity.

1. Information Sharing

[15] The information sharing provisions of the DFS Regulations are focused on ensuring that NYDFS can enforce Covered Entities regulation compliance through its enforcement power under various applicable laws.[48] Under the regulations, Covered Entities, which include all entities requiring a license or other authorization under New York banking, insurance, or financial services law with limited exceptions,[49] must submit an annual certificate of compliance that is executed by the Chair of the Board of Directors or a Senior Officer.[50] This is the key information sharing provision of the DFS Regulations because if a Board or Senior Officer represents compliance with the regulations, and the Covered Entity is found to be noncompliant, the Board would have made a false representation and could face a NYDFS enforcement action.[51] Further, the DFS Regulations require that each Covered Entity maintain systems with "audit trails" that are based on its Risk Assessment.[52] The systems must be

[48] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.20 (2018).

[49] *Id*. § 500.19.

[50] *See id*. § 500.21.

[51] *See* Steven R. Chabinsky & Jeremy Apple, *NYS Department of Financial Services Cybersecurity Regulation Goes Live: Now What?*, WHITE & CASE (Mar. 1, 2017), https://www.whitecase.com/publications/article/nys-department-financial-services-cybersecurity-regulation-goes-live-now-what [https://perma.cc/6P74-FSNT].

[52] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.06 (2018).

designed to "reconstruct material financial transactions" and include audit trails designed to detect and respond to malicious cybersecurity threats.[53] Additionally under this section, covered entities must maintain records between three and five years, so that NYDFS may review them in the event of a cyber incident.[54]

2. Notice

[16] The DFS Regulations require that a covered entity give notice to the NYDFS Superintendent within 72 hours of making the determination that a "cybersecurity event" has occurred that either: 1) requires notice to be made to any government, self-regulatory, or other supervisory body; or 2) has a reasonable likelihood of "materially harming" any material part of the Covered Entity's normal operations.[55] Additionally, the notice provision requires that each Covered Entity submit an annual certification of compliance with §500.17 and maintain records subject to inspection for five years.[56]

[17] The notice provision was perhaps the most hotly contested issue during the notice and comment period for the DFS Regulations.[57] The proposed regulations required that all cybersecurity events that had "a reasonable likelihood of materially *affecting* the normal operation of the Covered Entity" or that affected non-public information had to be reported

[53] *See id*.

[54] *See id*.

[55] *Id*. § 500.17.

[56] *See id*.

[57] *See generally* Joseph P. Vitale, *NYDFS' Revision of Proposed Cybersecurity Regulation for Financial Services Companies*, HARV. L. SCH. FORUM CORP. GOV'T & FIN. REG. (Jan. 10, 2017), https://corpgov.law.harvard.edu/2017/01/10/nydfs-reversal-of-its-proposed-cybersecurity-regulation-for-financial-services-companies/ [https://perma.cc/UA5Z-Y2YB].

within 72 hours.[58] Commentators argued that the proposed provision was overly broad, would result in reports of little value to NYDFS, and would not allow adequate time to gather the information necessary to make a timely report.[59] However, NYDFS identified being able to swiftly respond to cybercrime and protecting consumer information as two of the primary purposes behind the regulations and believed the notice requirement represented key aspects of those goals.[60] Thus, as outlined above, the compromise final regulation keeps the 72-hour requirement, but modifies the language concerning which cybersecurity events must be reported to those that have a reasonable likelihood of "materially harming" a Covered Entity's normal operations.[61] This is a much narrower standard than the "affects" provision, which would seem to have required almost any cybersecurity event to be reported.[62]

3. Liability

[18] The potential for liability for Covered Entities who fail to comply, or misrepresent compliance, with the DFS Regulations hinges on NYDFS' enforcement power under applicable laws.[63] The New York legislature created NYDFS in 2011 as part of Governor Cuomo's 2011 budget by amending state statute to combine New York State's Banking Department and Insurance Department.[64] The statute gave the newly combined agency

[58] *See id*. (emphasis added).

[59] *See id*.

[60] *See* Governor Cuomo, Press Release, *supra* note 21.

[61] *See* Vitale, *supra* note 57.

[62] *See id*.

[63] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.20 (2018).

[64] *See The Department of Financial Services: New York's Newest Financial Regulator*, JONES DAY (Dec. 2011) [hereinafter JONES DAY, *New York's Newest Financial*

broad enforcement power to refer matters to the State Attorney General to protect consumers and investors in financial products and services.[65] The amended statute also created the Financial Frauds and Consumer Protection Division (FFCPD) within NYDFS that has the authority to pursue civil and criminal investigations of violations of financial services, banking, or insurance law.[66] This portion of the statute also gives the NYDFS Superintendent the power to investigate whenever FFCPD has a "reasonable suspicion that a person or entity has engaged, or is engaging, in fraud or misconduct with respect to the banking law, the insurance law," or other relevant law.[67] Needless to say, given NYDFS' aforementioned broad enforcement authority, and the fact that the DFS Regulations require that Covered Entities certify annual compliance with the regulations, a false representation of compliance could lead to an NYDFS enforcement action, fines and other penalties, or even criminal proceedings. However, it is not yet certain how strictly NYDFS will enforce the cybersecurity regulations, as Covered Entities do have a transitional period to comply with regulation, and the agency has broad discretion as to which type of enforcement actions to bring.[68] In the agency's brief history, the majority of enforcement actions have culminated with settlement agreements or consent orders with civil penalties rather than criminal proceedings.[69]

Regulator], https://www.jonesday.com/Department_of_Financial_Services/# [https://perma.cc/85UA-L9MH].

[65] *See* N.Y. FIN. SERV. LAW § 301 (LEXISNEXIS 2018).

[66] *See id*. § 403.

[67] *See id*. § 404.

[68] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.22 (2018); *see also* Chabinsky & Apple, *supra* note 51 (noting that it remains unclear how strictly NYDFS will enforce certain provisions of the regulations, particularly those related to the Covered Entities' Risk Assessment).

[69] *See generally* N.Y. DEPT. FIN. SERVS., Enforcement Actions—General, http://www.dfs.ny.gov/about/eagen.htm [https://perma.cc/N8FA-JTHX] (listing enforcement actions).

4. Implementing Specific Cybersecurity Measures

[19] The DFS regulations are focused on requiring Covered Entities to implement specific cybersecurity measures. These measures include: 1) having a cybersecurity program "designed to protect the confidentiality, integrity, and availability of the Covered Entity's Information Systems";[70] 2) maintaining a written cybersecurity policy approved by a Senior Officer;[71] 3) designating a Chief Information Security Officer (CISO);[72] 4) performing penetration testing and vulnerability assessments;[73] 5) limiting access privileges to non-public information;[74] 6) documenting periodic risk assessment of information systems;[75] 7) utilizing qualified cybersecurity personnel and intelligence;[76] 8) having a third-party service provider security policy;[77] 9) taking steps to protect non-public information, potentially including encryption and multi-factor authentication;[78] 10) disposing of non-public information when it is no longer necessary for business operations;[79] 11) providing regular

[70] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.02 (2018).

[71] *See id*. § 500.03.

[72] *See id*. § 500.04.

[73] *See id*. § 500.05.

[74] *See id*. § 500.07.

[75] *See* N.Y. COMP. CODES R. & REGS. Tit.23, § 500.09 (2018).

[76] *See id*. § 500.10.

[77] *See id*. § 500.11.

[78] *See id*. § 500.12; *see also id*. § 500.15.

[79] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.13 (2018).

cybersecurity awareness training for all personnel;[80] and 12) maintaining a written incident response plan.[81]

[20] As several commentators have noted, many of these measures are systems that sophisticated entities covered by the DFS Regulations will already have in place.[82] However, the risk assessment provision proved particularly controversial during the notice and comment period, as it epitomized the debate over whether to employ a "risk adjusted" based approach, as favored by industry, or a "minimum standards" based approach, as favored by NYDFS.[83] The DFS Regulations that were originally proposed required every Covered Entity to utilize encryption for certain non-public information, multifactor authentication, and limitations on user access, regardless of the outcome of the Covered Entities own Risk Assessment.[84] Covered entities criticized this minimum standards approach in the comments as too much of a "one-size-fits-all" approach,

[80] *See id*. § 500.14.

[81] *See id*. § 500.16.

[82] *See* Ramos & Schiffer, *supra* note 18 (noting that large international financial institutions subject to the European Union's General Data Protection Regulations (GDPR) will likely easily be able to comply with the DFS Regulations); *see also* Eric R. Dinallo et al., *Client Update: New York Eases Proposed Cybersecurity Regulation for Financial Sector, But Practical Issues Remain*, DEBEVOISE & PLIMPTON (Jan. 3, 2017), http://www.debevoise.com/~/media/files/insights/publications/2017/01/20170103c_new_york_eases_proposed_cybersecurity_regulation_for_financial_sector_%20but_practical_issues_remain.pdf [https://perma.cc/5FTJ-LNFC] (noting that smaller entities who rely on outside vendors for compliance will be most affected by the DFS regulations).

[83] *See* Vitale, *supra* note 57 (highlighting the revisions made to the proposed NYDFS regulations as a result of the debate).

[84] *See* Joseph P. Vitale, *NYDFS Proposed Cybersecurity Regulation for Financial Services Companies*, HARV. L. SCH. FORUM CORP. GOVERNANCE & FIN. REG. (Sept. 24, 2016), https://corpgov.law.harvard.edu/2016/09/24/nydfs-proposed-cybersecurity-regulation-for-financial-services-companies/ [https://perma.cc/4WC4-34P8].

and they argued for a more flexible risk-adjusted based methodology.[85] In the final rule, NYDFS compromised on minimum standards and stated that the results of the Covered Entity's own Risk Assessment would determine whether a Covered Entity would be required to meet specific obligations under the DFS Regulations.[86] Nonetheless, illustrating the ongoing tension between these two approaches to cybersecurity regulation, NYDFS retained a provision stating that this flexibility does not allow entities to employ a "cost-benefit" approach to cybersecurity, which has been criticized as defying the conventional wisdom behind cyber risk management.[87]

III. LEGAL ANALYSIS

[21] This legal analysis section begins by analyzing the evident contrasts between CISA and the DFS regulations and examining the legal methodology behind the cybersecurity policy preferences in each approach. Following this discussion of contrasts, this section argues the article's central thesis: that CISA and the DFS Regulations are complementary in nature. This argument focuses on the overarching concepts discussed in the Introduction and applies them to the areas covered by CISA and the DFS Regulations, respectively.

A. Contrasting CISA and the DFS Regulations

[22] As evident in the background section's review of the relevant provisions of CISA and the DFS Regulations, there are some significant differences in the cybersecurity methodologies employed by the respective legal frameworks. This section explicitly analyzes the differences in legal methodology and looks at the cybersecurity policy preferences and goals behind the divergences.

[85] Vitale, *supra* note 57.

[86] *See id*.

[87] *See id*.; *see also* Chabinsky & Apple, *supra* note 51.

1. Information Sharing

[23] First and foremost, the information sharing provisions of CISA are all *entirely voluntary*, while the DFS Regulations affirmatively require the potential for information sharing through the certification of compliance and the maintenance of records provisions concerning audit trails and systems security.[88] Additionally, as discussed previously, NYDFS has broad enforcement authority to conduct investigations into violations of New York financial services law and thus the DFS Regulations could lead to *forced* information sharing in the event NYDFS were to bring an enforcement action or refer an investigation to the State Attorney General.[89] Second, CISA authorizes (but does not require) the sharing of cyber threat indicators amongst private entities while the DFS Regulations are strictly concerned with mandating that certain records be maintained (and potentially shared) to demonstrate compliance with the requirements as a whole.[90]

[24] This contrasting approach to information sharing demonstrates the very different policy goals behind CISA and the DFS Regulations. CISA is designed as a national security statute which aims to incentivize the voluntary sharing of cyber threat indicators by private entities with the goal of lowering cybersecurity risks for both the public and private sector by better calculating efficient levels of cybersecurity.[91] It approaches information sharing as a necessary prong of the nation's cybersecurity program that must be incentivized rather than expected or required of the private sector through more direct regulation or legislation.[92] On the other

[88] *See supra* text accompanying notes 25, 49–50, 52–53.

[89] *See supra* text accompanying notes 62–65.

[90] *See supra* text accompanying notes 26, 47–52.

[91] *See* Promnick, *supra* note 3, at 100–01.

[92] *See* Jaffer, *supra* note 1, at 589 (discussing how CISA's information sharing provisions come with a "carrot" of liability protection).

hand, the DFS Regulations' top priority is the protection of non-public information at financial services companies from cyber criminals.[93] Perhaps because of its expansive authority to regulate in the financial services space, NYDFS clearly did not see the need to offer any particular "carrots" to industry with regards to incentivizing the required information sharing under the DFS regulations.[94] Thus, although the regimes are aimed at the same general goal of improving cybersecurity in the private sector, they take divergent approaches based on more specific policy preferences.

2. Notice

[25] CISA's lack of a notice provision in the event of a cybersecurity incident is the obvious variance between that framework and the DFS Regulations, which require a covered entity to notify the superintendent of NYDFS within 72 hours of a determination that a cybersecurity event has occurred that either 1) requires notice to any government body, self-regulatory agency, or any other supervisory body; or 2) has a reasonable likelihood of materially harming any material part of the Covered Entity's normal operations.[95] This difference can also be explained by the divergent structure and policy preferences of CISA versus the DFS Regulations. Structurally, a required notice provision embedded in CISA would be meaningless as an entity that chooses to share in accordance with the Act is already putting DHS or another private entity on notice that it has at least received a cyber threat indicator that could be potentially (or

[93] *See* Press Release, N.Y. State, Governor Cuomo Announces Action to Protect New Yorkers' Private Information Held by Credit Reporting Companies (June 25, 2018) https://www.governor.ny.gov/news/governor-cuomo-announces-action-protect-new-yorkers-private-information-held-credit-reporting [https://perma.cc/V6DH-J9BS].

[94] To be sure, as discussed throughout the prior section laying out the DFS Regulations, NYDFS did make concessions and compromises with industry on some provisions after the initial proposed regulations received over 150 comments. However, these are not "carrots" in the same way the incentives of CISA are. *See generally* Dinallo et al., *supra* note 82; *see generally* Vitale, *supra* note 57.

[95] *See supra* paras. 10, 16.

actually) harmful to the private entity's systems.[96] Additionally, if CISA contained a notice requirement similar the DFS Regulations, it would likely constitute a detrimental *stick* in a statute that has already been criticized by some commentators as not containing enough *carrots* to incentivize private entities to share cyber threat indicators.[97]

[26] In contrast, without a notice requirement, NYDFS would lack the ability to be apprised of cyber events on a timely basis and would rely solely on Covered Entities' representations that they had complied with implementing the DFS Regulations' specific cybersecurity measures.[98] Although NYDFS compromised on what cyber security events require notice, it is evident they felt strongly about maintaining some notice requirement for this reason.[99] Another likely reason for this position is that the DFS Regulations are designed to be enforced through NYDFS' enforcement authority—an authority that would be undermined if the agency could not analyze cybersecurity events that occurred at Covered Entities to determine whether the event could have been caused by noncompliance with the DFS Regulations.[100] These contrasts between CISA and the DFS Regulations concerning notice provisions demonstrate the conflicting goals behind a statute designed to incentivize information sharing as opposed to a regulation promulgated with the potential for enforcement of specific standards in mind.

---

[96] *See* 6 U.S.C. § 1501(6)(F) (2018) ("the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat").

[97] *See* Jaffer, *supra* note 1, at 593–94 (discussing the fact that industry is concerned about DHS' role under CISA as it is the very agency at the forefront of a larger regulatory movement surrounding cybersecurity infrastructure and protection).

[98] *See supra* paras. 17, 20.

[99] *See* Vitale, *supra* note 57.

[100] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.20 (2017).

3. Liability

[27] CISA's broad liability protections for entities sharing cyber threat indicators with the federal government are certainly a contrast to the DFS Regulations which actually create the potential for liability by incorporating NYDFS' enforcement authority.[101] To be sure, CISA's broad liability protections are to some extent driven by the fact that without them, the potential for private entities to incur liability from various laws unrelated to cyber information sharing would likely render the statute ineffectual.[102] However, in implementing CISA, Congress limited liability to such an extent that even information sharing done in bad faith (so long as it is done in accordance with proper procedures) receives the same broad liability defense.[103] This type of liability shield demonstrates how concerned Congress was with offering the utmost incentive to private entities to share cyber threat indicators even when those indicators might be shared with questionable intentions. Although this policy preference might be seen as an invitation for problematic decisions, it really illustrates that the potential for better preventing cyber breaches such as those at OPM and Yahoo clearly drove Congress in the direction of overarching liability protection.[104] Additionally, illustrating the difficulty in implementing this policy preference, some commentators have said private entities should remain skeptical of the broad liability protections and actually need more overarching liability shields if Congress desires to efficiently effectuate the statute's intent of encouraging cyber information sharing.[105]

---

[101] *See supra* paras. 11, 13, 18–19.

[102] *See* Nolan, *supra* note 40, at 13.

[103] *See supra* para. [12]; *see* Promnick, *supra* note 3, at 102–03.

[104] *See supra* paras. 2, 11.

[105] *See* Jaffer, *supra* note 1, at 594–95 (arguing for expanding liability protection under CISA to include decisions made by companies in receipt of shared information).

[28] In contrast, the DFS Regulations specifically reserve the right to utilize NYDFS' enforcement power.[106] While NYDFS was clearly open to negotiation with Covered Entities in several areas of the DFS Regulations, it made no such concessions on enforcement power.[107] In contrast with the implementation of CISA, this demonstrates a specific policy preference for maintaining the risk of liability, a significant dissimilarity given both statutes' similar goal of improving cybersecurity.[108]

4. Implementing Specific Cybersecurity Measures

[29] Clear contrasts are also evident between CISA's and the DFS Regulations' approach to requiring private entities to implement specific cybersecurity measures. CISA contains no provisions requiring any specific cybersecurity measures and the DFS Regulations are predominately focused on requiring certain cybersecurity measures.[109] Federal legislators drafting CISA incentivized cyber information sharing as the leading policy goal behind the statute's implementation and were understandably wary at the prospect of mandating specific cybersecurity measures in conjunction with, or as a prerequisite too, encouraging information sharing.[110] Congress' rejection of the Obama administration's

[106] *See supra* para. 18.

[107] *See* Vitale, *supra* note 57 (describing key modifications such as tailoring risk and cybersecurity event reporting); *supra* text accompanying notes 61–62, 86 (describing other modifications in which the NYDFS compromised*); see also* N.Y. COMP. CODES R. & REGS., tit. 23, § 500.20 (2018) (demonstrating like compromises in enforcement).

[108] *Compare* Governor Cuomo, Press Release, supra note 21 (detailing the changes New York intended to implement to protect consumers with the new cybersecurity regulation in mind), *with* Press Release, Jeh C. Johnson, Statement by Secretary Jeh C. Johnson on Implementation of the Cybersecurity Act of 2015 (Feb. 16, 2016) https://www.dhs.gov/news/2016/02/16/statement-secretary-jeh-c-johnson-implementation-cybersecurity-act-2015 (last visited December 3, 2018) (stating the changes that could be made in order to address the new requirements).

[109] *See supra* paras. 13, 19–20.

[110] *See generally* Jaffer, *supra* note 1.

2011 proposal to require certain critical infrastructure operators to implement measures similar to the DFS Regulations, such as having commercial auditors assess cybersecurity risk mitigation plans and having operators certify the plans' sufficiency, demonstrates this policy preference in action.[111]

[30] The contrasts in policy preference in this area are fairly obvious as NYDFS felt mandating specific cybersecurity measures was a necessary step to monitoring and regulating Covered Entities early on in its overall assessment of cybersecurity in the financial services industry.[112] Additionally, consumer protection had a prominent place in NYDFS' policy goals for implementing the DFS regulations and the agency consistently articulated that mandating certain measures to ensure the safety and soundness of covered entities cybersecurity programs was inherently an exercise in building consumer trust in an age of increasing cybersecurity threats.[113] While both Congress and NYDFS made opposite concessions in this area, with Congress granting DHS the authority to issue some guidance on technical cyber infrastructure for certain information sharing and NYDFS adopting a more risk-adjusted approach as opposed to minimum standards, the contrasts in policy preferences on mandating certain cybersecurity measures are still evident.[114]

---

[111] *See* Press Release, White House Office of the Press Secretary, FACT SHEET: Cybersecurity Legislative Proposal (May 12, 2011), https://obamawhitehouse.archives.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal [https://perma.cc/TVJ9-VSZV].

[112] *See* Kaplan et al., *supra* note 16, at 1–2.

[113] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017) ("A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its consumers."); Governor Cuomo, Press Release, *supra* note 21 ("DFS is ensuring that New York consumers can trust their financial institutions have protocols in place to protect the security and privacy of their sensitive personal information.").

[114] *Compare supra* para. 13 (discussing Congress' implementation of cybersecurity measures), *with supra* paras. 19–20 (discussing NYDFS' implementation of cybersecurity measures).

B. CISA and the DFS Regulations as Complementary Approaches to Cybersecurity

[31] After laying out the various contrasts between CISA and the DFS Regulations, this section reaches this article's central thesis: that CISA and the DFS Regulations are complementary approaches to cybersecurity law and policy despite their clear differences in policy preferences. In making this argument, this section looks to recognized legal frameworks, precedent, and theory as a guide for advocating that this dualistic approach to cybersecurity is complementary rather than an inherent dichotomy that needs be remedied through more all-encompassing federal legislation.

1. Information Sharing and the Federal Government's Role in Providing for the Common Defense

[32] As every student of the Constitution learns, Article I Section 8 contains a clause expressly giving Congress the power to "provide for the common Defence […] of the United States" and "provid[ing] for the common defence" is also referenced in the Constitution's preamble.[115] The inclusion of this clause in the Constitution as an express power of the federal government is widely seen as a mechanism to solve the collective action problem that would result if states had to provide for their own defense.[116] As mentioned previously, CISA's inclusion in Title 6 of the United States Code makes clear that it is a statute dedicated to enhancing domestic security for the country as a whole.[117] Therefore, CISA and its information sharing provisions were arguably enacted by Congress pursuant to its authority to provide for the common defense.

---

[115] U.S. CONST. art. I, § 8, cl. 1; *id.* pmbl.

[116] *See* Robert D. Cooter & Neil S. Siegel, *Collective Action Federalism: A General Theory of Article I, Section 8*, 63 STAN. L. REV. 115, 147–148 (2010); *see also* AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 56 (1st ed. 2005) (discussing Article I Section 8 and the funding of national defense as a collective action problem).

[117] *See* 6 U.S.C. § 1501–1510.

[33] This line of reasoning helps illustrate why the information sharing provisions in CISA are so heavily focused on incentivizing cyber information sharing on a voluntary basis, making sure that private entities feel comfortable sharing cyber threat indicators with the federal government, and ensuring mutual communication on cyber threats. Given recent high-profile cyber breaches and the potential for a cyber-attack that cripples a critical infrastructure or industry—a national security incident that would threaten the common defense—understandably Congress focused on its constitutional authority to provide for the common defense when crafting CISA. Without the sharing of cyber threat indicators, there is little way for the public and private sector to communicate about the threats they are addressing (and that others may need to address) on a regular basis. Regardless of policy preferences, Congress knew that if it made sharing cyber threat indicators too hard, cost-prohibitive, or risky under CISA, it would likely fail in facilitating the sharing of cyber threat indicators which would lead to continued vulnerability and a deficient "common defense" in cyberspace.[118]

[34] The DFS Regulations complement CISA's domestic security-driven approach because they are focused predominately on another key area related to information sharing: the protection of consumer information. Because of the structure of American federalism, New York need not worry about national security matters and, in fact, its constitution only references law enforcement and does not contain the phrase common defense or domestic security.[119] As it relates to information sharing, the DFS Regulations focus on certifying compliance with the regulations and maintaining records to ensure that an investigator would be able to audit the covered entity's cybersecurity program to determine if it adequately protected consumers. This difference in goals between CISA and the DFS Regulations is complementary because the federal statute incentivizes

[118] *See generally* Jaffer, supra note 1 (suggesting that even with all of the incentives to share provided by Congress, some commentators have still argued that CISA is deficient in this area).

[119] *See* N.Y. CONST. art. 13, §13.

information sharing to enhance national cybersecurity as a whole, and the state regulation requiring record keeping and compliance protects consumer information. In fact, a private entity subject to the DFS Regulations who chooses to participate in CISA would arguably have some of the most robust cybersecurity systems in the world—sharing and receiving cyber threat indicators with the government and private entities as well as implementing the specific cybersecurity measures mandated by the DFS Regulations.

2. Notice and the Historical Precedent of Strict State Standards in Data Breach and Privacy Law

[35] States have long taken the lead in enacting stricter data breach and privacy statutes with notice requirements to consumers or state governmental bodies.[120] Forty-six states and the District of Columbia have enacted some sort of notice law that private entities must comply with in the event of a data breach.[121] CISA and the DFS Regulations are complementary in reflecting this historical precedent of states determining what kind of breaches will require notice to a governmental entity or consumers. Although several commentators have argued that a comprehensive federal data breach law is necessary to protect consumers, states' fairly swift action in this area should give pause to federal

[120] *See* Robin B. Campbell, *Compliance with Security Breach Notification Laws: Prevention & Mitigation Strategies*, HEALTH LAWS. NEWS 13, 14–15 (2008), https://www.crowell.com/documents/Compliance_Security-Breach-Notification-Laws_Robin-Campbell.pdf [https://perma.cc/46KV-RHGJ].

[121] *See* GINA STEVENS, CONG. RESEARCH SERV., RL 34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 2 (2010), https://fas.org/sgp/crs/secrecy/RL34120.pdf [https://perma.cc/3YAX-SHL8]; *see also* Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J. L. & POL'Y 467, 467 (2010) (following the enactment of California's first of its kind data breach law in 2003, 46 states and the District of Columbia had enacted some form of data breach notification law by 2010).

legislators seeking an overarching comprehensive solution.[122] States' regulatory actions such as the DFS Regulations should be seen as complementary to legislation like CISA at the federal level which incentivize information sharing without notice requirements. One can imagine that CISA would have been even more difficult to enact, and less likely to be utilized by private entities, if it had included the mandated disclosure of cyber threat indicators to consumers or another governmental entity outside DHS' promulgated procedures for information sharing.

[36] The DFS Regulations' 72-hour provision is a strong notice requirement that provides NYDFS the information necessary to determine whether: 1) the entity in question is compliant with the DFS Regulations and 2) the extent to which an enforcement action is necessary or that consumers need to be notified. Again, the situation creates a balanced scenario where private entities covered by both the DFS Regulations and CISA have the ability to take advantage of cyber threat information sharing nationwide, but are also subject to the 72-hour notice provision if there is a cyber breach that is likely to cause "material harm" to the covered entity's normal operations.[123] The main critics to endorsing this bilateral approach, in addition to those endorsing comprehensive federal data breach legislation, are private entities who argue complying with so many state laws is overly burdensome.[124] This is a valid critique, but the situation can be remedied in other ways as The National Conference of State Legislators and other organizations have worked to create model legislation for states that could cut down on major differences between

[122] *See* Joerling, *supra* note 122 at 467, 486–88; Peter Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime*, 7 J. TELECOMM. & HIGH TECH. L. 107, 108 (2009) (arguing for enhanced federal enforcement in cases of cybercrime).

[123] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.17 (2017).

[124] *See* Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ L. REV. 1171, 1184 (2014) (arguing that current state data breach notification laws are overly burdensome on national entities and confusing for both consumers and private industry).

states' laws.[125] However, regulatory regimes like the DFS Regulations are arguably increasingly necessary for some industries and states which is why this article contends that federal legislative action, like CISA, properly focuses on complementing state laws and regulations in the area of notice.

3. Liability and the Divergent Interests of State Regulators versus Federal Legislators

[37] CISA and the DFS Regulations illustrate how the divergent interests of state regulators and federal legislators can sometimes have complementary effects. CISA's blanket prohibition on holding non-federal entities liable for information sharing, so long as they share in accordance with established procedures, was necessary in the minds of federal legislators and many other commentators because the statute's goal of incentivizing the sharing of cyber threat indicators would be undermined without it. As this article has discussed, some commentators still feel that CISA still has not gone far enough in limiting liability to incentivize the widespread sharing of cyber threat indicators.[126] Nonetheless, it is acknowledged that the bar on liability does provide at least some measure of comfort to private entities.[127] Without this bar on liability, every other incentive to information sharing falls apart as the risk of liability is simply too great for the majority of private entities to justify *sharing information with the government* without this protection. The interests of federal legislators in "provid[ing] for the common defence"[128] and avoiding future high profile cyber breaches understandably outweighed concerns about potential bad faith sharing or gross negligence on the part of private entities. These interests are natural given that Congress often faces a

[125] *See* Joerling, *supra* note 122, at n.33.

[126] *See supra* paras. 12, 27. *See generally* Jaffer, *supra* note 1.

[127] *See supra* paras. 12, 27.

[128] U.S. CONST. pmbl.

public backlash when a high-profile breach occurs, particularly if the government could have done more to stop it or knew about the cyber threat which caused the breach.

[38] It may seem contradictory to argue that a statute which prohibits liability and regulations which allow for liability are complementary, but in the case of cybersecurity, the contention is very much plausible. State regulators at NYDFS have interests that align predominately with protecting consumers.[129] Thus, NYDFS' interests weigh in favor of imposing liability on Covered Entities because their concern is not creating incentives to share but creating incentives to implement specific cybersecurity measures that NYDFS feels are necessary for financial services companies. These divergent interests create a complementary approach because industries can comply with both frameworks and enhance their cybersecurity. In other words, CISA enables entities who would be covered under the DFS Regulations to *better comply* with the DFS Regulations and avoid liability altogether. It is not unreasonable to think that this complementary scenario could play out in many states across the country, particularly in industries like financial services and critical infrastructure.

4. Implementing Specific Cybersecurity Measures and the Inherent Differences Between Statutes of General Applicability and Regulations Tailored to a Specific Industry

[39] The last complimentary aspect of CISA and the DFS Regulations predominately relates to how mandating the implementation of specific cybersecurity measures is more effective if the mandate is tailored to a specific industry and its needs and vulnerabilities. Although some commentators have argued that the DFS Regulations represent a model for the nation and other states generally, it is easy to see how implementing

[129] *See* JONES DAY, *New York's Newest Financial Regulator*, *supra* note 64; *see supra* paras. 18–19.

this type of regulation on some industries or its participants might be overly burdensome and ineffective.[130] This insight explains why NYDFS exempted some entities from all or some of the more burdensome provisions.[131] On the other hand, CISA is a statute of general applicability aimed at incentivizing information sharing for all entities.[132] Thus, requiring that entities participating have specific cybersecurity measures or systems in place would run contrary to the statute's purpose. This purpose also explains why CISA included measures to incentivize small businesses and other less sophisticated entities to participate. The use of a *general applicability* approach at the federal level and a *tailored regulatory approach* at the state level is complementary because it allows the federal government to prioritize its duty to provide for the common defense and prevent high-profile cyber breaches and allows states to tailor a cybersecurity approach that works best for a particular industry and exempt specific entities as needed. The case of CISA and the DFS Regulations highlight these benefits because CISA incentivizes information sharing without imposing specific measures, while the DFS Regulations provide a tailored approach for a large, but specific, industry.

IV. CONCLUSION

[40] Although advocating that complementary legislation at the state and federal level with sometimes opposing policy preferences is a viable option for enhanced cybersecurity, this article makes no attempt to say that discovering complementary features of two very different cybersecurity frameworks means the best option has been found. On the contrary, the cyber realm is an area where legal frameworks often struggle to keep up with rapidly evolving technological capabilities. This struggle often leads to the understandable calls for overarching conceptual changes to legal and regulatory frameworks to bring cybersecurity law and policy into the 21st century. However, history has shown that even when these efforts

[130] *See* Kosseff, *supra* note 21, at 436–38, 444.

[131] *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19 (2017).

[132] *See supra* para. 3.

come to fruition, they often come up short when a new disruptive technology renders a previously well-thought-out structure obsolete. This article's focus on the contrasting but complementary policy preferences of CISA and the DFS Regulations furthers the argument that the statute or regulations that aim to provide an all-encompassing cybersecurity framework in one streamlined approach, however well-intentioned, will often come up short as they attempt to synthesize countless views into effective cybersecurity policy. Perhaps, as this article suggests, a reliance on the precedential divides between the role of states and the federal government, their naturally divergent interests, and the well-traveled path of developing dualistic legal frameworks to solve the country's most pressing issues is the best path forward for superior cybersecurity policy in the years to come.