April 2019

Cyberspace: The 21st Century Battlefield

Cameron Ryan Scullen

Cyberspace: The 21st Century Battlefield

Cameron Ryan Scullen*

I. INTRODUCTION

As technology continues to advance over time, the frequency of cyberattacks carried out against the United States has increased. The United States' economy and its people can only be protected through an

* University of Miami, J.D. Candidate May 2017, University of Miami, M.B.A. Candidate May 2017. A special thank you to both Ted Chakos (J.D. Candidate May 2016, University of Miami School of Law) and Professor Rachel Stabler for all their editorial support throughout the entire publication process.

Act that adequately addresses each of the following elements: Liability, Information Dissemination, Privacy Rights, Critical Infrastructure, Small Businesses, and Advancing Technology. While the Cybersecurity Act of 2015 sufficiently addresses liability, information dissemination, and privacy rights, it fails to adequately protect both critical infrastructure and small business and fails to create a platform to continue the advancement of cybersecurity technology.[1]

In May 2015, foreign adversaries carried out a cyberattack against the United States.[2] This cyberattack, if successful, could have both destabilized the nation's economy and compromised the personal information of many United States citizens.[3] To the surprise of many, this China-based cyberattack was not the first of its kind.

Many terrorist organizations and foreign adversaries consistently target the U.S. To many, our nation's economy is the strongest in the world. The United States' Gross Domestic Product (GDP), which measures the productivity of a nation's economy, was $17.419 trillion in 2014.[4] China had the next closest GDP at $10.354 trillion.[5] The economies of Germany and the United Kingdom are arguable competitive with GDPs of $3.868 trillion and $2.988 trillion respectively.[6] Nevertheless, the nation with the strongest economy has the strongest influence across the global sphere. The U.S. having the highest GDP creates incentives for others to target its economy and its citizens through cyberattacks.

Today, our nation is being attacked on a newly developed cyber battlefield that contains some of the most advanced, complex weapons in history. Not only does our nation's cybersecurity technology struggle to combat cyberattacks, but also these cyberattacks can be carried out with limited resources. The ability to carry out these cyberattacks with limited resources exposes our country to additional enemies.

The critical infrastructure of this country is the backbone of our nation's economy. Critical infrastructure is broadly construed as any entity or information system that directly impacts the daily functionality

---

1 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).

2 Lisa Brownlee, *New Report of Malicious Chinese Cyber Attack on A U.S. Government Agency*, FORBES (Dec. 30, 2015, 8:30 AM), http://www.forbes.com/sites/lisabrownlee/2015/09/25/new-report-of-malicious-chinese-cyber-attack-on-a-u-s-government-agency/#2715e4857a0b7f515ae9309b.

3 *Id.*

4 The World Bank Group, *GDP at Market Prices*, http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (Last visited Jan. 31, 2016).

5 *Id.*

6 *Id.*

of financial businesses and utility services.[7] If one of these entities or information systems were hacked and became inoperable, the nation's economy would be severely weakened. Such an impact on our economy could result in an economic panic. While an economic panic could be subdued through quick decision-making, any period of economic weakness could allow existing adversaries, such as China, to gain a foothold in the global sphere.

Moreover, one of the most valuable assets to any individual is that individual's identity. The ability to obtain a legal identity allows an individual to independently create wealth. However, in modern day society, businesses create efficiencies within their services through utilizing information technology systems.[8] When these information technology systems are used, the personal information of consumers is stored on information systems, which in turn are stored in a cyber platform.[9] As a result, hackers are able to steal such information in order to gain access to an individual's accumulated wealth.[10] To protect against the stealing of consumer information, our nation must strengthen the cybersecurity of its businesses.

Our government must find a means to prevent any major cyberattack from effectively compromising either our economy or our citizens' personal information. The government can reduce the impact of cyberattacks by increasing the effectiveness of our nation's cybersecurity. Cybersecurity can be strengthened through cyber information sharing between non-federal entities themselves and between non-federal and federal entities. On December 18, 2015, President Obama signed the Cybersecurity Act of 2015 (the 'Act'). The Act allows non-federal entities to voluntarily share cyber information between themselves and to voluntarily share cyber information with the government.[11]

II. HISTORY

With the development of technology, an increasing number of entities are storing their internal information in a virtual platform. This platform, called *cyberspace*, was created through the advancement of

---

7 *See generally* WHAT IS CRITICAL INFRASTRUCTURE?, DEP'T OF HOMELAND SECURITY (Jan. 8, 2016), https://www.dhs.gov/what-critical-infrastructure.

8 Bert Markgraf, *How Is a Management Information System Useful in Companies?*, Demand Media, http://smallbusiness.chron.com/management-information-system-useful-companies-63415.html (last visited March 13, 2016); *see also infra* note 11.

9 *See generally infra* note 12.

10 *See generally infra* note 12.

11 Cybersecurity Act of 2015.

technology and allows various entities to create efficiencies in their operations that in turn results in increased profitability. As a result, entities utilizing cyberspace are more exposed to cyberattacks from United States adversaries. In particular, motivated hackers have targeted the financial industry, the retail industry, the health care industry, and the United States government itself.

Before the United States can strengthen its cybersecurity it must first understand the technology used by modern businesses and agencies. Today entities rely on information systems to create internal efficiencies and increase productivity. An information system is "a computer system or set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself."[12] Using information systems, an entity stores various amounts of information in cyberspace, which exposes stored information to cyberattacks. The exposure entities face when storing data in cyberspace has created an entirely new global battlefield.[13] "Cyberspace is the new battleground, a battleground for a multitude of adversaries. Foreign nations, international terrorist organizations and organized crime regularly target our citizens, businesses, and government."[14] The amount of potential adversaries to the United States has grown significantly as a result of critical information being stored on cyberspace.

Additionally, enemies are able to carry out large-scale cyberattacks with limited resources. "Unlike traditional combat operations, cyberattacks don't require sophisticated weaponry to carry out their warfare. On the cyber battlefield, a single individual with a laptop computer can wreak havoc on business, the economy, and even our critical infrastructure."[15] Since a hacker is able to conduct cyberattacks with relative ease, it is imperative that our nation develops stronger cybersecurity.

Moreover, the United States has the largest Mutual Fund and Exchange Traded Fund (ETF) Markets within the world.[16] Mutual Funds and ETFs are financial entities that conduct investment strategies to accrue profitable gains.[17] At the 2014 year-end, the U.S. Mutual Fund

---

[12] *Information System Definition*, business dictionary, http://www.business dictionary.com/definition/information-system.html.

[13] 161 Cong. Rec. H2426 (daily ed. April 23, 2015) (statement of Rep. Loudermilk), https://www.congress.gov/amendment/114th-congress/house-amendment/99/text.

[14] *Id.*

[15] *Id.*

[16] *2015 Investment Company Fact Book*, Investment Company Institute (Nov. 16, 2015, 5:00 PM), www.icifactbook.org/fb_ch1.html.

[17] *Id.*

and ETF assets accounted for 53% of the $33.4 trillion Mutual Fund and ETF assets worldwide.[18] A hacker wishing to steal from these entities can do so through successfully hacking into the platform on which these entities run their operations and trading systems. A hacker could even profit by conducting a cyberattack that halts the operations of one of these financial entities, allowing that hacker to execute profitable trades against the open trading positions of a particular financial entity. The ability to achieve large sums of monetary assets in little time with limited resources can incentivize many to carry out cyberattacks against our nation.

In July through August of 2014, a "series of coordinated, sophisticated attacks" on JPMorgan Chase siphoned off gigabytes of data.[19] The hackers were able to steal account information of 83 million households and small businesses.[20] However, JPMorgan Chase found no evidence of fraud or misuse of customer information in the following months.[21] Even though Hackers stole information that included customer email addresses, home addresses, and phone numbers,[22] the success of this cyberattack was prevented through JPMorgan Chase's cybersecurity. Nevertheless, on Friday March 25, 2016, U.S. Officials announced seven Iranian hackers were able to coordinate a cyberattack on multiple U.S. banks, such as JPMorgan Chase and Wells Fargo, resulting in the loss of millions in business.[23]

In comparison to the financial industry, hackers have targeted the retail industry, which collects large quantities of financial information from individual consumers. In December 2013, Target Corporation's information system incurred one of the largest data breaches to date.[24] Hackers carried out a cyberattack that resulted in the theft of credit and debit card records of more than 40 million customers,[25] while gaining access to personal information, such as email and mailing addresses, for

---

18 *Id.*

19 Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, The N. Y. TIMES (Dec. 29, 2015, 10:00 AM), http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0].

20 *Id.*

21 *Id.*

22 *Id.*

23 Dustin Volz and Jim Finkle, *U.S. indicts Iranians for hacking dozens of banks, New York dam*, REUTERS (Mar. 25, 2016, 11:13 AM), http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF.

24 Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, The N. Y. TIMES (Dec. 29, 2015, 10:00 AM), http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0].

25 *Id.*

more than 70 million people.[26] The data breach was executed through malware that was installed on Target Corporation's network.[27] The executed malware enabled the hackers to gain access to customer information by siphoning away such information through customer orders and purchases, compromising the financial assets of millions of citizens.

Similarly, our nation's healthcare industry entities collect large quantities of personal information while operating profitable businesses. "The U.S. insurance industry's net premiums written totaled $1.1 trillion in 2014, with premiums recorded by life/health insurers accounting for 56 percent and premiums by property/casualty insurers accounting for 44 percent."[28] In February 2015, a cyberattack targeted Anthem, one of the nation's largest health insurance providers.[29] The cyberattack compromised personal information of "tens of millions of its customers and employees."[30] The hackers were able to breach a database that stored information on past and present customers and employees.[31] The stolen information included "names, Social Security numbers, birthdays, addresses, email and employment information, including income data."[32] Hackers realized that cyberattacks carried out against the healthcare industry could prove to be lucrative.

Although, seeking profit is not always a hacker's primary incentive. For instance, China has targeted the United States to gain an economic advantage.[33] The Chinese economy is the largest emerging market in the world.[34] From 2013 to 2017, China's GDP is forecasted to grow by 45.9%.[35] As the Chinese economy has grown, China's global competitiveness with the United States has grown as well. China, in the hopes of becoming more competitive with the United States, has attempted a series of cyberattacks to try and halt our nation's economy.

---

[26] *Id.*

[27] *Id.* Malware is short for "malicious software" and "refers to software programs designed to damage or do unwanted actions on a computer system." *See Malware Definition*, TechTerms.com, http://techterms.com/definition/malware (last visited Jan. 31, 2016).

[28] *Insurance Industry At A Glance*, Insurance Information Institute, (Jan. 31, 2015), http://www.iii.org/fact-statistic/industry-overview.

[29] Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, The N. Y. TIMES (Dec. 29, 2015, 10:00 AM), http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0].

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *See generally* Brownlee, *supra* note 2.

[34] *The Top 20 Emerging Markets* BLOOMBERG (Jan. 30, 2013 4:18 PM), http://www.bloomberg.com/slideshow/2013-01-30/the-top-20-emerging-markets.html#slide21.

[35] *Id.*

In May 2015, China conducted a weeklong cyberattack named Operation Iron Tiger that targeted United States government contractors.[36] The hackers utilized stolen Office of Personal Management data to infiltrate the information systems of Government contractors, compromising terabytes of data from various defense contractors.[37] This cyberattack appeared to manipulate stolen Office Personnel Management data in order to hack targeted cyberspace.[38] A successful Chinese cyberattack may allow China to gain an economic advantage, or even political leverage, over the United States.

China has become more strategic in targeting our nation's critical infrastructure.[39] As of February 2014, the National Security Agency (NSA) has constructed a map displaying where the Chinese government has carried out massive cyberattacks.[40] The map reveals that these cyber assaults target "all sectors of the U.S. economy, including major firms like Google and Lockheed Martin, as well as the U.S. government and military."[41] The Chinese cyberattacks have successfully targeted over 600 corporate, private, and governmental entities within a five-year period.[42] These cyberattacks concentrated on America's industrial centers and stole "corporate and military secrets and data about America's critical infrastructure, particularly the electrical power and telecommunications and internet backbone."[43] The critical infrastructure of the U.S. must be protected or else our economy will be at risk.

Understanding and appreciating the capability of our nation's adversaries is critical to developing effective cybersecurity. In recent years, cyberattacks have become more focused and have greatly increased their ability to compromise our citizens' personal information and to disrupt our economy's productivity. However, technology is necessary to provide the most effective services to our citizens and to increase the productivity of our nation. As our nation becomes more reliant on technology, it is essential that our nation develop a cybersecurity platform to defend against cyberattacks. We must be one step ahead of our adversaries on this newly established battlefield: cyberspace.

---

36 Brownlee, *supra* note 2.

37 *Id.*

38 *Id.*

39 Robert Windrem, *Secret NSA Map Shows China Attacks on U.S. Targets*, NBC NEWS (Jul. 30, 2015, 6:23 PM), http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

40 *Id.*

41 *Id.*

42 *Id.*

43 *Id.*

III. IDENTIFYING TWO ESSENTIAL ELEMENTS

Our nation's critical infrastructure is composed of many non-federal entities.[44] Many of these non-federal entities are smaller entities that have a limited amount of resources.[45] Building a strong cybersecurity platform requires time and money. However, our nation's critical infrastructure is only as strong as its weakest link. If one entity within our nation's critical infrastructure is compromised, the U.S. economy could potentially stall. On February 12, 2013, President Obama, recognizing the need to provide these entities with the resources to develop effective cybersecurity, signed Executive Order 13,636 (Order).[46] The Order identifies two essential elements in improving our nation's cybersecurity: critical infrastructure and technology.[47]

A. Understanding Critical Infrastructure

The success of the United States' critical infrastructure depends on the functionality of multiple non-federal entities. Because our nation's critical infrastructure relies on the functionality of multiple entities, our nation has the potential of diversifying the risk of cyberattacks. In finance, people diversify their investments to distribute the risk. While our critical infrastructure has many components, the components rely on each other for success. Thus, our critical infrastructure is still at great risk even if only one entity is compromised. As a result, when one entity begins to perform poorly, all interrelated entities will also begin to perform poorly. In order to utilize the notion of diversification, each entity operating in our critical infrastructure must independently have a strong cybersecurity.

In truth, many of our nation's critical infrastructure entities are unable to protect themselves due to limited resources. President Obama, through his Executive Order, identified both the significance of and the necessity of providing cybersecurity to our nation's critical infrastructure.[48] President Obama explains that it is the duty of the United States to find a means of providing the necessary resources to critical infrastructure entities.[49] "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure

---

44 U.S. SMALL BUSINESS ADMINISTRATION, SMALL BUSINESS GDP: UPDATE 2002-2010 (Jan. 2012), https://www.sba.gov/content/small-business-gdp-update-2002-2010.

45 *Id.*

46 *See generally* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

47 *Id.*

48 *Id.* at 11739.

49 *Id.*

and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[50] The President further suggested that the cybersecurity of critical infrastructure can be improved through the sharing of information between non-federal and federal entities.[51]

However, it is essential that our country narrows the definition of critical infrastructure entities. Defining which entities need immediate assistance ensures that the proper resources are allocated in a timely and effective manner. President Obama defined the term *critical infrastructure* to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[52] A risk-based approach was used to identify where a cybersecurity incident could reasonably result in a detrimental effect on our nation and identify critical infrastructure entities at greatest risk.[53] Identifying the most at-risk entities allows the government to address the weakest links in the cybersecurity of our critical infrastructure entities.

B. Advancing Technology

President Obama identified a second essential element in creating stronger cybersecurity: technology.[54] The advancement of technology can ensure that an entity's cyber defense will continue to improve as cyberattacks become more advanced and complex. The Order attempts to provide a customizable cybersecurity framework to each entity through a three-step process: 1. the creation of a cybersecurity framework; 2. the voluntary sharing of such framework; and 3. the consultation in adopting such framework.[55] The National Institute of Standards and Technology (NIST) was responsible for implementing this three-step process.[56]

---

50 *Id.*

51 Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

52 *Id.*

53 *Id.* at 11742.

54 *Id.* at 11741.

55 *See generally* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (hereinafter, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY).

56 *Id.* at 4.

The cybersecurity framework promotes the ability for entities to advance their existing technology by remaining "technology neutral."[57] The NIST relied on existing standards to create a framework that will continue to develop and grow alongside technological advances.[58] "By relying on global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across boarders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances in business requirements."[59] The framework provides both a base to develop a cybersecurity platform and a means to continue technological development within each particular entity.

However, entities will only be willing to adopt the provided framework if that framework will not disturb the profitability of each entity. The NIST needed to ensure that economic success could still be achieved while implementing the developed cybersecurity framework. The NIST argues that "the use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs."[60] The co-alignment of profitability with the development of a stronger cybersecurity platform is a very attractive proposition. An entity will not only be able to continue its level of productivity, but will also be able to provide adequate protection against cyberattacks.

The ability of an entity to maintain a steady level of productivity depends on the ability to implement a new cybersecurity framework smoothly. The NIST framework focused around a multi-layered implementation process: 1. *framework core*, 2. *framework implementation tiers*, and 3. *framework profile*.[61] This three-layered process allows each entity to customize the NIST framework to fit its business model, ensuring a smooth transition when adopting this new cybersecurity platform.

First, the *framework core* ("core") provides a strategic overview that will allow organizations to manage cybersecurity concerns effectively.[62] The *core* is composed of five "concurrent and continuous functions:

---

57 *Id.*
58 *Id.*
59 *Id.*
60 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, 4 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [hereinafter National Institute of Standards and Technology].
61 *Id.* at 4-5.
62 *Id.* at 4.

Identify, Protect, Detect, Respond, and Recover."[63] The NIST has declared these five functions as "a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors."[64] Implementing the *framework core* will provide the proper foundation for an organization to continue developing its cybersecurity platform.[65]

Second, the *framework implementation tiers* ("tiers") help an organization identify both its current views on cybersecurity risk management and the type of process the organization already has in place.[66] The tiers "describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework (e.g., risk and threat aware, repeatable, and adaptive)."[67] The tiers allow an organization to quickly assess its current position in order to implement the most effective cybersecurity platform.

Third, the *framework profile* ("profile") customizes the implementation of the framework to suit a particular organization's business needs.[68] The NIST will provide an entity with a list of framework categories and subcategories to identify the nature of that entity's business operations.[69] The NIST characterizes the profile as "the alignment of standards, guidelines, and practices to the *framework core* in a particular implementation scenario."[70] The profile ensures a smooth transition in implementing the new cybersecurity framework, allowing any entity to continue business operations in an effective manner.

The Order promoted the adoption of the cybersecurity framework through voluntarily offering it to all existing entities.[71] It instructed the Secretary of Homeland Security, along with Sector-Specific Agencies, to establish a voluntary program to support the adoption of this framework.[72] The program would support the framework's adoption by any owner and operator of critical infrastructure, as well as all other interested entities.[73]

---

63 *Id.*

64 *Id.* at 1.

65 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, 1 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

66 *Id.* at 5.

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

71 Exec. Order No. 13,636, 78 Fed. Reg. 11,739, at 11,741 (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. [Executive Order].

72 *Id.*

73 *Id.* at 11739.

The Adoption of the framework is not obligatory but is strongly suggested.[74] This allows various entities that do have the ability to create strong cybersecurity to continue to operate independent frameworks. These independent frameworks may have a proven track record in protecting particular entities against cyberattacks. Additionally, the Order requires agencies responsible for regulating the security of critical infrastructure to consult with the Department of Homeland Security (DHS), the Office of Management and Budget (OMB), and National Security Staff in order to identify and reduce regulatory burdens.[75] Through reducing regulatory burdens, the government is encouraging entities to choose among the best resources available. These resources consist of the framework provided by the NIST that helps individual non-federal entities develop an independent cybersecurity platform.[76] Regardless, the Order has ensured that resources will be available should an entity not have sufficient cybersecurity. However, these resources primarily consist of structural information on how to build a stronger cybersecurity platform. The NIST does not provide the actual technology to develop such a framework. In turn, non-federal entities with financial limitations may not be able to independently acquire the necessary technology to develop more effective cybersecurity.

IV. CURRENT LAW

A. Sharing Electronic Information

The various private and public entities existent in our nation will voluntarily share cyber information only if they can do so without incurring increased liability. A corporation operating in cyberspace likely stores a large amount of personal information on its information systems. Whether this personal information derives from employees or consumers is not important. The significance lays in the liability a company, or entity, can face if it exposes personal information to a third-party.

An entity's ability to collect and store data on information systems to create efficiencies comes with limitations. These limitations are created under the Electronic Communications Privacy Act (ECPA) of 1986.[77] The ECPA is continuously updated through subsequent legislation, including the USA Patriot Act, to "keep pace with the evolution of new

---

74 *Id.*

75 *Id.* at 11,740.

76 *See supra* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, note 60.

77 *See* Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22 (1986).

communications technologies and methods."[78] As of today, "[t]he ECPA protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically."[79] The ECPA identifies the modern significance of communicating via technology and tries to prevent the disclosure of private information through using third-party technology.

The ECPA consists of three titles.[80] The first title constitutes the Wiretap Act.[81] The Wiretap Act protects personal communication by prohibiting "intentional, actual, or attempted interception, use, disclosure, or procurement of any other person to intercept or endeavor to intercept any wire, oral, or electronic communication."[82] The Wiretap Act does provide two specific exceptions that allow a electronic information to be shared. First, a telephone service provider is allowed to listen or monitor phone calls when either law enforcement officers, who are acting pursuant to a valid court order, direct the provider, or the provider's network is being used without having been paid for.[83] Second, law enforcement officials can intercept electronic information if an individual has consented to the use of that electronic information by third parties.[84] There is no liability exception for an entity to voluntarily share cyber information that contains personal information with either another non-federal entity or with a federal entity.

The second title of the ECPA is referred to as the Stored Communications Act (SCA).[85] The SCA protects both personal information that is stored by service providers and private information collected as a result of a subscription with the service provider, such as the subscriber's name, billing records, or IP address.[86] The SCA protects consumers' personal information from misuse by service providers.[87] However, there are two exceptions for divulging private information

---

78 U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE ASSISTANCE, PRIVACY & CIVIL LIBERTIES, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last visited Jan 18, 2016, 11:10 AM) (citing Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22).

79 *Id.*

80 18 U.S.C. § 2510-22 (1986).

81 18 U.S.C. § 2511 (1986).

82 *Id.*

83 18 U.S.C. § 2511(2)(a)(1986); *see also* 18 U.S.C. § 2510 (1), (5) (1986) (defining wire communication and providing clarification for electronic communication service as used in 18 U.S.C. § 2511(2)(a)(1986)).

84 18 U.S.C. § 2511 (2)(c)-(d)(1986).

85 18 U.S.C. § 2701-2712 (1986).

86 18 U.S.C. § 2702 (1986).

87 *Id.*

under the SCA: 1. exception for disclosure of communications; and 2. exception for disclosure of customer records.[88] To qualify for an exception the service provider must in good faith, "believe that an emergency involving danger of death or of serious physical injury to any person requires disclosure without delay of information relating to the emergency."[89] The SCA does provide an avenue for entities to share information with the government, but limits that avenue to exigent circumstances.

The third and last title, Title III, requires that government entities obtain judicial authorization before installing and using a pen register and/or trap or trace.[90] A pen register is a device that captures the dialed information, information from out going calls, or communications made by an individual.[91] A trap and trace is a device that captures the actual numbers involved in a telephone call, along with related information of the outgoing or incoming call.[92] For judicial authorization to be granted, the applicant must provide a basis of certification that the information sought is likely to be relevant to "an ongoing criminal investigation being conducted by that agency."[93] This title directly addresses the limitations on the government to acquire personal information from non-federal entities.

Moreover, Title III is necessary to prevent governmental intrusion into the operations of private entities. However, this puts a burden on the non-federal entities to voluntarily share information with the government in order to strengthen our nation's cybersecurity platform. But a non-federal entity is limited through ECPA and the SCA in terms of what information can be shared without incurring liability.

B. Sharing Personal Information

1. Statutory Liability

An individual can prevent financial institutions from sharing personal information through the Gramm-Leach-Bliley Act of 1999.[94] This Act requires financial institutions to disclose to customers what kind of private information it will be allowed to share with other entities.[95]

---

88 *Id.*
89 *Id.*
90 18 U.S.C. §3121-3127 (1986).
91 18 U.S.C. §3127 (1986).
92 *Id.*
93 18 U.S.C. §3122 (1986).
94 *See generally* Gramm-Leach-Bliley Act of 1999, S. Res. 900, 106th Cong. (1999) (enacted).
95 *Id.* at § 502-03.

Additionally, under certain circumstances, this Act allows customers to prohibit information sharing with other entities.[96] The Gramm-Leach-Bliley Act of 1999 created barriers for financial institutions to share personal information that may be existent on relevant cybersecurity information.

Moreover, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) also contains specific rules requiring entities operating within the health care industry to protect the information of customers. [97] HIPAA creates a national standard of protection of both medical records and personal information, which applies to health plans, health care clearinghouses, and health care provides that conduct transactions electronically.[98] "The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization."[99] If the national standard is not adhered to, an entity can face a significant fine. As of 2014, the New York and Presbyterian Hospital (NYP) and Columbia University (CU) both incurred data breaches resulting in the disclosure of electronic protected health information of a cumulative 6,800 individuals.[100] In response, NYP and CU reached settlements with subsequent civil charges brought against them for $3,300,000 and $1,500,000 respectively.[101]

2. Civil Liability

Additionally, entities storing private information on information systems in cyberspace can be exposed to civil liability. Usually individuals whose personal information is compromised through an entities information systems being breach will bring suit under a contract-based action.[102] When individuals elect to utilize the services of a particular entity, they enter into a contract that requires the entity to

---

96 *Id.* § 502.

97 H.I.P.A.A. Enforcement Rule, 45 C.F.R. §160, 164; *see* U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
THE HIPAA PRIVACY RULE (2000), http://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

98 *Id.*

99 *Id.*

100 U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, *Data breach results in $4.8 million HIPPA settlements*, (May 7, 2014), http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html.

101 *Id.*

102 Wayne M. Alder, *Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim*, BECKER & POLIAKOFF ARTICLES, (http://www.becker-poliakoff.com/data-breaches-prevent-and-defend-a-claim).

protect personal information.[103] However, when the contract does not provide the language for such protection, a plaintiff can argue that "an 'implied contract' exists to safeguard data if such data is collected from customers or clients.'"[104] With the possibility of facing an implied contract claim, entities storing personal information are likely going to be exposed to civil suits if a data breach were to be incurred.

V. FUNDAMENTAL INGREDIENTS

The Cybersecurity Act of 2015 (the Act), enacted on December 18, 2015, was the legislative branch's first attempt at improving the cybersecurity of our nation.[105] The Act is a combination of three previously proposed Congressional bills.[106] The three bills, two proposed by the House and one by the Senate, were voted on in the 114th Congress and were respectively titled: the Protecting Cyber Networks Act (PCNA), H.R. 1560, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), H.R. 1731, and the Cyber Security Information Act of 2015 (CISA), S. 754.[107] These three bills were the essential ingredients of the new 2015 Act and various pieces of each particular bill exist within the 2015 Act.[108] The Act directly promotes the sharing of cybersecurity information among non-federal entities and between non-federal entities and the government.[109]

To understand the 2015 Act in its entirety, it is important to understand the various elements that were addressed in drafting such legislation. The PCNA, NCPAA, and CISA were similar, but each bill had unique provisions that were ultimately incorporated into the 2015 Act. [110]

---

[103] *Id.*

[104] *Id.* (citing In re Hannaford Bros., 613 F. Supp. 2d (D. Me. 2009)).

[105] Cybersecurity Act of 2015, H.R. Con. Res. 2029-3, 114th Cong. (2015) (enacted).

[106] *Passage of Landmark Cyber Legislation Likely*, COOLEY MEDIA, (12, 17, 2015), https://www.cooley.com/cyber-legislation-passage-likely.

[107] *See* Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1560; *see also* National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1731?q=%7B%22search%22%3A%5B%22%5C%22hr1731%5C%22%22%5D%7D&resultIndex=1; *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/754.

[108] *Passage of Landmark Cyber Legislation Likely*, COOLEY MEDIA, (12, 17, 2015), https://www.cooley.com/cyber-legislation-passage-likely.

[109] H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).

[110] *See* H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).

A. The PCNA

Through the PCNA, Congress attempted to create a law to strengthen our country's cybersecurity platform.[111] The PCNA, sponsored by Republican Representative Devin Nunes from California, passed the House on April 22, 2015.[112] The PCNA's strengths derive from its provisions addressing small businesses and the dissemination of information.[113]

The PCNA addressed the concern of small businesses being unable to protect themselves against cyberattacks.[114] The bill required the Small Business Association (SBA) to provide assistance to small businesses and financial institutions.[115] The SBA would help smaller firms monitor information systems, operate defensive measures, and share and receive indicators and defensive measures.[116] Indicators can be broadly defined as the unique characteristics of each particular cyberattack while defensive measures consist of various techniques used to build a strong cybersecurity platform.[117]

Additionally, the PCNA attempted to establish a sufficient process to efficiently disseminate all shared information with the federal government.[118] The bill instilled procedures to ensure that cyber threat indicators shared by a non-federal entity with the Department of Commerce, the Department of Energy, the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Department of the Treasury, and the Director of National Intelligence (DNI) are shared in real-time with all appropriate entities.[119] The sharing of information in real-time would allow the government to fully utilize all shared information to prevent large-scale cyberattacks against the government.

---

[111] Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1560.

[112] *Id.*

[113] *Id.*

[114] *Id.* at §103.

[115] *Id.*

[116] Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1560.

[117] Susan Cassidy & Peter Terenzio, *Competing Bills Focus on Cybersecurity Information Sharing But Final Language and Ultimate Passage Remain Unknown*, INSIDE GOVERNMENT CONTRACTS, (July 10th, 2015), http://www.insidegovernmentcontracts.com/2015/07/competing-bills-focus-on-cybersecurity-information-sharing-but-final-language-and-ultimate-passage-remain-unknown/.

[118] Protecting Cyber Networks Act, H.R. 1560, 114th Cong. §102 (2015), https://www.congress.gov/bill/114th-congress/house-bill/1560.

[119] *Id.* at §104.

B. The NCPAA

The NCPAA was the second Congressional attempt to provide a stronger cybersecurity platform for our country.[120] The NCPAA, sponsored by Republican Representative Michael McCaul from Texas, passed the House on April 23, 2015.[121] The most notable element of the NCPAA was its attempt to strengthen the cybersecurity of the federal government.[122] Non-federal entities will only share cyber information with the federal government if they are presented with both liability exclusions and insurance that the federal government has a strong cybersecurity platform.

The NCPAA provided an effective process that would continue to develop the core of our federal government cybersecurity.[123] The NCPAA language would have authorized and codified the EINSTEIN program operated in the DHS.[124] "The EINSTEIN program, as deployed, makes available the capability to protect the Federal agency information and information systems.[125] The EINSTEIN program includes technologies to diagnose, detect, prevent, and mitigate cybersecurity risks involving Federal information systems."[126] Representative Michael McCaul explained that the program, now referred to as the E3A program, would provide participating Federal agencies with the ability to identify cyber threats and help protect their systems from internal and external threats.[127] This protection would ensure that the federal government could prevent various cyberattacks from compromising the information shared by non-federal entities.

C. The CISA

The CISA was the Senate's only attempt to draft a bill that would reinforce our nation's cybersecurity.[128] The CISA, sponsored by Republican Senator Richard Burr from North Carolina, passed the Senate

---

[120] National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1731?q=%7B%22search%22%3A%5B%22%5C%22hr1731%5C%22%22%5D%7D&resultIndex=1.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *National Cybersecurity Protection Advancement Act of 2015: Hearing on H.R. 1731 Before the H. Comm. on Homeland Security,* 114th Cong. 1 (2015) (statement of Representative Michael McCaul, Member, H. Comm. of Homeland Security), https://www.congress.gov/amendment/114th-congress/house-amendment/99/text.

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/754.

on October 27, 2015.[129] Although each bill provided provisions to address the concerns of protecting our country's critical infrastructure, the CISA provided an additional focus on our nation's health care industry.[130] "The Department of Health and Human Services must convene a task force to: (1) plan a single system for the federal government to share intelligence regarding cybersecurity threats to the health care industry, and (2) recommend protections for network medical devices and electronic health records."[131] Entities operating in the healthcare industry use information systems that store large amounts of personal information in cyberspace. It is essential that such entities be provided with the proper resources to fend off cyberattacks.

D. The Key Difference

The PCNA, the NCPAA, and the CISA each had a unique provision, or provisions, to offer. However, each bill differed greatly in defining how cyber information would be shared between non-federal entities and the government.[132] The PCNA dictated that information should be shared with "appropriate federal entities except [the Department of Defense] DOD" and the procedure governing the sharing would be developed by the Director of National Intelligence (DNI).[133] The PCNA would also establish a Cyber Threat Intelligence Integration Center (CTIIC) that would be located within the DNI.[134] The CTIIC would serve as "the primary organization within the federal government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to cyber threats."[135] The PCNA was the only bill that created a new organization to process shared cyber information.[136]

In contrast, the CISA specified that information would be shared with the federal government in real-time.[137] The Department of Homeland Security (DHS) would be responsible for developing the real-

---

129 *Id.*

130 *Id.* at §405.

131 *Id.*

132 Cassidy, *supra* note 117.

133 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. §104 (2015), https://www.congress.gov/bill/114th-congress/house-bill/1560.

134 *Id.*

135 *Id.*

136 *Compare Id.* § 104, *with* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/754 *and* National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. (2015).

137 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. §103. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/754.

time process referred to.[138] Lastly, the NCPAA cited the DHS's National Cybersecurity and Communications Integration Center (NCCIC) as the primary clearinghouse for data.[139] Although the CISA and the NCPAA both called for information to be shared through the DHS, they addressed how the DHS would handle shared cyber information differently.[140]

The most effective way to disseminate shared information is to assign the task of sharing such information to one agency. A non-federal entity is exposing itself to additional risk by sharing cyber information to the government. Along with additional liability exclusions, a non-federal entity may be more inclined to share information if it knew that such information would be fully utilized. As a result, it was essential for the 2015 Act to come to a final decision on how information should be shared between non-federal and federal entities.

VI. CONSOLDIATED SOLUTION

The United States' non-federal and federal entities are exposed to cyberattacks everyday. To prevent the impact of cyberattacks our nation must develop stronger cybersecurity through addressing these essential elements: Liability, Information Dissemination, Privacy Rights, Critical Infrastructure, Small Business, and Technology. Understanding the severity of a successful cyberattacks, Congress enacted the Cybersecurity Act of 2015.[141]

The Act is Congress' first successful attempt to provide a basis for improving the cybersecurity of our country. The Act promotes the sharing of cybersecurity information between non-federal and federal entities, as well as between non-federal entities themselves.[142] The sharing of cyber information will allow our nation to pool resources to more effectively combat the various cyberattacks carried out against all entities domiciled in the U.S.

However, the Act does not adequately address all the essential elements necessary to building a strong cybersecurity platform. While the Act sufficiently addresses liability, information dissemination, and privacy rights, it inadequately addresses critical infrastructure, small business, and technology.

---

138 *Id.* § 105.

139 National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. §2 (2015), https://www.congress.gov/bill/114th-congress/house-bill/1731?q=%7B%22search%22%3A%5B%22%5C%22hr1731%5C%22%22%5D%7D&resultIndex=1.

140 *Id.* at §2; *see also* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. §105. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/754.

141 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).

142 *Id.*

A. Reducing Liability

To encourage non-federal entities to share cyber information both among each other and with federal entities, the Act must reduce non-federal entities exposure to both statutory and civil liability. However, the Act needs to do more than provide liability exclusions to encourage non-federal entities to share cyber information that may possibly contain personal information.

For a non-federal entity to understand the liability it will be exposed to if it were to share cyber information, the Act must adequately define what type of cyber information can be shared. The Act indicates that non-federal and federal entities can share two types of cyber information: 1. cyber threat indicators, and 2. defensive measures.[143] A *cyber threat indicator* is generally defined as any information that helps identify a malicious attempt to infiltrate and appropriate information stored in cyberspace through exploiting vulnerabilities existent within cybersecurity.[144] Additionally, a defensive measure is defined as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[145] Both *cyber threat indicators* and *defensive measures* are defined broadly.[146] As a result, it is very likely that non-federal entities will share information with other entities that contain personal information.

The ability to protect shared cyber information will help reduce the liability that non-federal entities will be exposed to by sharing such information. The Act presents a provision that attempts to protect shared cyber information by strengthening the core cybersecurity platform of federal entities.[147] The Act requires the DHS to assess whether or not the DHS itself can "create an environment for the reduction in cybersecurity risks in Department data centers, including by increasing compartmentalization between systems, and providing a mix of security controls between such compartments."[148] In comparison, financial advisors and money manages utilize the concept of compartmentalization by diversifying the investment strategy of clients' assets. A financial advisor's diversified investment strategy decreases the overall risk of loss that a particular client's investments are exposed to. The

---

143 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §105).
144 *Id* at §102.
145 *Id.*
146 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §102).
147 *Id.* at §203.
148 *Id.* at §206.

government's ability to develop a similar strategy could significantly reduce the impact of one cyberattack.

For example, if a DHS data center is attacked and its information system, and thus cyber information, becomes compromised, the stored shared information existent on other DHS data centers' information systems will still be protected. The Act's ability to reduce the impact of cyberattacks on the federal government will in turn reduce the liability that a non-federal entity will be exposed to by sharing cyber information. A non-federal entity's liability exposure will be reduced because it will become less likely for shared cyber information, which may or may not contain personal information, to become compromised.

As noted above, non-federal entities will also need to be provided with the proper exclusions from civil liability.[149] The Act provides language that directly excludes non-federal entities from civil liability if they voluntarily share cyber information with each other or with the government.[150] Additionally, the Act explains that a non-federal entity will not waive any privilege or protection when that non-federal entity decides to share cyber information.[151] Furthermore, when a non-federal entity decides to share cyber information with the federal government, that cyber information, being a cyber threat indicator or defensive measure, will be "considered the commercial, financial, and proprietary information of such non-federal entity."[152] However, the Act expressly identifies that to claim cyber information as proprietary, the non-federal entity must designate that the shared information is proprietary in nature.[153] The Act has sufficiently reduced the liability a non-federal entity is exposed to when sharing cyber information.

B. Disseminating Information

A streamlined process for dissemination relevant cybersecurity information will allow the government to fully utilize shared cyber information. Furthermore, the shared cyber information will only be helpful if such information can be analyzed and leveraged to provide further insight into defending against current and future cyberattacks. The ability to properly disseminate and to sufficiently utilize shared cyber information depends on what organization(s) are responsible for handling this information.

---

149 *Id.* at §106.
150 *Id.*
151 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §105).
152 *Id.* at §105.
153 *Id.*

The strongest method and most effective process for taking advantage of shared cyber information is for the government to assign one federal agency as the primary portal for information sharing. The Act, through amending the Homeland Security Act of 2002, assigns the DHS as the primary federal entity responsible for collecting, analyzing, and disseminating shared cyber information by non-federal entities.[154] Additionally, the Act provides that the DHS will further delegate its responsibilities for sharing information with multiple DHS data centers.[155] The DHS data centers will allow large quantities of data to be assessed and leveraged within a shorter period of time. More importantly, each data center will be focused on conducting analysis of, and sharing information with, specific industries.[156] This will allow the government to perform the necessary due diligence before sharing information with each particular industry.

The DHS must be able to quickly provide beneficial information to both non-federal and federal entities after analyzing shared cyber information. Cyberattacks are constantly carried out against non-federal and federal entities. Additionally, the hackers who carry out these cyberattacks adapt and alter their approach based on the current cybersecurity platform of various entities. Therefore, the information shared by non-federal entities may only be useful for a short period of time. The Act provides that the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate federal entities, will collaboratively define the proper procedures to ensure useful information is shared in real-time.[157] This team of individuals will draft procedures that attempt to facilitate the following aspects of sharing cyber information.[158] First, they will address the federal government's sharing of classified cyberthreat indicators and defensive measures with relevant federal and non-federal entities with adequate security clearance.[159] Second, they will focus on the federal government's sharing of declassified cyber threat indicators, defensive measures, and information related to cybersecurity threat with relevant non-federal and federal entities.[160] Third, they will provide insight on the federal government's sharing of unclassified cyber information with relevant federal and non-federal entities, as well as the public in certain

---

154 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §105 §204).
155 *Id.* at §206.
156 *Id.*
157 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §103).
158 *Id.*
159 *Id.*
160 *Id.*

circumstances.[161] Fourth, they will direct the federal government's sharing of cyber information that will help entities prevent or mitigate the adverse effects of cyberattacks with relevant federal and non-federal entities.[162] Finally, they will concentrate on the federal government's periodic sharing of developed best practices to improve cybersecurity with a particular focus on small businesses' ability to access and implement the best practices.[163] Through real-time processing, the quick assessment and dissemination of shared cyber information can be sufficiently conducted through the Act's development of the above procedures.[164]

The federal government must be willing to share its own collected cyber information with non-federal entities. Non-federal entities will be more willing to expose their cyber information to the vulnerabilities of the federal government's cybersecurity only if that federal government is willing to do the same with non-federal entities. The Act requires, that when appropriate, the federal government will share cyber threat indicators and defensive measures with relevant non-federal entities.[165] The Act has created a *two-way* door for sharing cyber information that will begin to build a trust between non-federal and federal entities that will further promote the sharing of cyber information.

C. Protecting Privacy Rights

Non-federal entities will have an exclusion from civil liabilities if they share their cyber information in accordance with proper procedures. These procedures ensure that non-federal entities will not expose the personal information of our nation's citizens unnecessarily. The personal information of our citizens is their privacy and the Fourth Amendment ensures that each citizen has a right to his or her own privacy.[166] The federal government must ensure that private information is only shared in order to prevent hackers from accessing and appropriating this personal information.

The Act lists basic steps that must be conducted before a non-federal and federal entity share cyber information.[167] The federal government created these steps to define both what type of cyber information could be shared and under what circumstances this information could be shared by non-federal entities. The Act explains that non-federal entities should

---

161 *Id.*
162 *Id.*
163 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §103).
164 *Id.*
165 *Id.*
166 U.S. CONST. amend. IV.
167 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §105).

not share information that "is not directly related to a cybersecurity threat; and is personal information of a specific individual or information that identifies a specific individual."[168] However, non-federal entities store large amounts of data in cyberspace and it is very likely that a non-federal entity may unintentionally provide personal information to other entities. Furthermore, a non-federal entity may only be able to share vital cyber threat indicators or defensive measures if personal information of employees or customers is also shared.

Congress understood the necessity of protecting privacy rights when providing a means for creating a stronger cybersecurity platform through the sharing of cyber information. The Act requires additional steps to be taken by the federal government to serve as a precaution to further protect the personal information of our country's citizens.[169] The Act indicates that before sharing a cyber threat indicator, a federal entity must ensure the cyber threat indicator only contains information directly related to cybersecurity.[170] If the federal entity discovers that the cyber indicator contains information not related to cybersecurity, such as personal information, it must remove such information.[171] The federal entity can do this either by reviewing and removing information contained within a cyberthreat indicator itself, or by implementing a technical process that focuses on reviewing and removing information.[172]

However, non-federal and federal entities may not be able to remove personal information from all cyber threat indicators in time for information to be fully utilized. Hackers are able to conduct cyberattacks in a moment's notice. The DHS and the DHS data centers will be under pressure to assess and disseminate large quantities of data in a relatively short period of time. The federal government may unintentionally provide the personal information as a result of operating under such time pressures.

Additionally, the federal government must limit the use of shared cyber information. Limiting non-federal or a federal entity's use of this information will provide an extra layer of protection to exposed personal information. The Act provides a set of guidelines to create this additional layer of protection. First, it creates a process that will destroy personal information that the federal government is not authorized to utilize.[173] Second, it creates a holding period for shared cyberthreat indicators,

---

168 *Id.*
169 *Id.* § 103 (emphasis added).
170 *Id.*
171 *Id.*
172 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §103).
173 *Id.* at §105.

which can only be retained for the duration of the holding period.[174] Finally, it includes various requirements that safeguard cyberthreat indicators that do contain personal information and implements sanctions against federal agents and employees who act in contravention of the given guidelines.[175] Congress, through adding these guidelines, has created a multi-layered approach to protecting the personal information of United States citizens.

However, Congress must define specific circumstances as to when cyber information can be shared among non-federal and federal entities. Congress, through defining such circumstances, can safeguard situations where citizens' personal information could potentially become exposed. The Act requires that cyber information can only be shared with and between non-federal and federal entities when that cyber information is directly related to a *cybersecurity risk*.[176] The Act generally defines a cybersecurity risk as any "threat to or vulnerability of information or information systems" that can result in "unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems."[177] Through this definition, Congress has narrowed the ability of entities to share cyber information to only circumstances where such sharing is necessary to build a stronger cyber defense. A stronger cyber defense will provide the means for non-federal entity to create a stronger cybersecurity platform and increase the same entity's ability to prevent the success of cyberattacks.

D. Addressing Critical Infrastructure

The United States economy directly relies on our nation's critical infrastructure. Our nation's critical infrastructure allows various industries and businesses to maximize their productivity and carry out necessary tasks. Furthermore, industrial control systems are an essential piece of critical infrastructure.[178] "Industrial control systems are used to deliver utility services to homes and businesses, add precision and speed to manufacturing, and process our foods into finished products."[179] For our economy to function on a daily basis, these control systems need to be operating effectively and efficiently.

---

174 *Id.*
175 *Id.* at 1757.
176 *Id.* at §203.
177 *Id.* at 1787.
178 161 CONG REC H2426, Vol. 161, No. 60 (April 23, 2015) (Statement of Ms. Jackson Lee)
179 *Id.*

According to Dell's report on cybersecurity, cyberattacks against industrial control systems doubled in 2015.[180] In comparison, in 2014, attacks specifically targeting SCADA industrial control systems rose 100 percent from 2013.[181] John Gordineer, director of product marketing for network security at Dell explained: "We have over a million firewalls sending data to us on a minute-by-minute basis. We anonymize the data and see interesting trends."[182] SCADA stands for Supervisory Control and Data Acquisitions and "generally refers to control systems that span a large geographic area, such as a gas pipeline, power transmission system or water distribution system."[183] The Act does not address the concerns of providing the proper cybersecurity to our nation's industrial control systems.[184] This is a significant fault of the Act and further legislation is needed to provide entities operating these control systems with the proper resources to mount a defense against cyberattacks.

However, the Act does attempt to build the cybersecurity platform of our nation's health care industry.[185] The Act strengthens the cybersecurity platforms of health care industry stakeholders.[186] A health care industry stakeholder is defined as any "health plan, health care clearinghouse, or health care providers; advocate for patients or consumers; pharmacist; developer or vendor of health information technology; laboratory; pharmaceutical or medical device manufacturer; or additional stakeholder the Secretary [of Health and Human Services] determines necessary."[187] The Act requires the government's Secretary of Health and Human Services to assess the ability of current entities defined as health care industry stakeholders to defend against cyberattacks.[188]

Nevertheless, a health care entity's cybersecurity may prove to be inadequate against the numerous cyberattacks carried out against the industry. To further support the cybersecurity of health care entities, the Act indicates that the Secretary, in consultation with the Director of National Institute of Standards and Technology and the Secretary of

---

180 Maria Korolov, *Attacks against industrial control systems double*, CSO (April 17, 2015 5:47 AM PT), http://www.csoonline.com/article/2911160/cyber-attacks-espionage/attacks-against-industrial-control-systems-double.html.

181 *Id.*

182 *Id.*

183 Eric Byres, *SCADA Security Basics: SCADA vs. ICS Terminology*, Tofino Security (May 9, 2012 9:00 PM), https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology.

184 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).

185 *Id.* at §405.

186 *Id.*

187 *Id.* § 405.

188 *Id.*

Homeland Security, should create a task force that consists of cybersecurity experts.[189] This task force will have multiple objectives.[190] First, the task force will analyze how various industries, outside of the health care industry, have effectively developed cybersecurity.[191] Second, it will assess the various challenges that health care entities face when implementing a sound cybersecurity framework.[192] Third, it will analyze the various risks existent when an entity or business associate links a medical device, or software, to its information systems in order to effectively utilize health records.[193] Fourth, it will disseminate all aggregated information to health care industry stakeholders so that they can immediately improve their cybersecurity and prepare against future cyberattacks.[194] Finally, it will create an effective plan that will allow the federal government and the health care industry to collaboratively combat a cyberattack in real time.[195] The task force, following these objectives, will sufficiently strengthen the cybersecurity of health care entities. A stronger cybersecurity platform will further protect the personal information of our citizens.

Our nation's ports are another key element of our economy's critical infrastructure. A large portion of the United States' import and export business is run through ports.[196] An estimated 360 commercial ports that provide approximately 3,200 cargo and passenger handling facilities exist in the United States.[197] In 2014, 23.1 million employment opportunities were created through commercial port activities.[198] Of those 23.1 million opportunities, 21.4 were related to an exporter/importer business and their support industries, contributing approximately $4.6 trillion to the United States economy and paying an estimated $321.1 billion in federal, state, and local taxes.[199] In 2014, seaport activities individually accounted for $41 billion in federal, state, and local tax revenues.[200] The ports of the United States represent a large

---

189 *Id.*
190 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §405).
191 *Id.*
192 *Id.*
193 *Id.*
194 *Id.*
195 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §405).
196 AMERICAN ASSOCIATION OF PORT AUTHORITIES, *U.S. Public Port Facts*, http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032 (last visited Jan. 31, 2016).
197 *Id.*
198 *Id.*
199 *Id.*
200 *Id.*

portion of our nation's GDP.[201] As result of contributing to the success of the United States economy, these ports have become an essential component of our country's critical infrastructure. If an adversary to the United States were able to conduct a series of cyberattacks, similar to Operation Tiger, against these ports, our country's economy could be severely damaged.[202]

The United States can protect our nation's ports through providing the proper cybersecurity resources. The Act requires an appointed Under Secretary to create a "report on cybersecurity vulnerabilities for the 10 United States ports that the Secretary determines are at greatest risk of a cybersecurity incident and provide recommendations to mitigate such vulnerabilities."[203] However, an Under Secretary's recommendations to the nation's 10 largest ports are not enough to prevent the impact of large-scale cyberattacks against such ports. Assuming the Under Secretary's recommendations will be disseminated to all entities operating on these 10 ports, there will still remain another 350 ports not being provided with additional cybersecurity support. To help entities operating in this industry, the government should provide these entities with a cybersecurity framework similar to that which was developed under the Order.[204] By providing a cybersecurity framework, the government can ensure that entities have the resources necessary to implement and develop a more combative cybersecurity platform.

However, the critical infrastructure of the United States consists of multiple industries and thousands of unique entities. To sufficiently protect each and every industry, and each and every entity operating within these industries, the government needs to develop a cohesive plan to combat cyberattacks. The Act provides that an appointed Under Secretary will assess the feasibility of producing such a plan.[205] The Under Secretary will conduct a report to determine the possibility of "producing a risk-informed plan to address the risk of multiple simultaneous cyber incidents affecting critical infrastructure, including cyber incident that may have a cascading effect on other critical infrastructure."[206] The plan, if created, could provide a much-needed additional layer of protection to prevent the impact of cyberattacks against our nation's critical infrastructure.

---

201 AMERICAN ASSOCIATION OF PORT AUTHORITIES, *U.S. Public Port Facts*, http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032 (last visited Jan. 31, 2016).

202 *See* Brownlee, *supra* note 2.

203 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §209).

204 *See* Executive Order, *supra* note 71.

205 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §103).

206 *Id.* at §208.

E. Addressing Small Businesses

Small businesses are an integral part of the United States economy. In the first three quarters of 2014 alone, small businesses generated an estimated 1.4 million new jobs.[207] However, small businesses generally have less capital available to invest in their internal infrastructure. This results in allocating capital into multiple aspects of smaller firms. Allocating an already limited amount of capital into various parts of a firm's infrastructure further prevents a smaller firm from being able to invest heavily in cybersecurity. It then becomes necessary to provide the proper resources to these smaller entities to help them build and strengthen their cybersecurity platforms. "In 2014, 31 percent of all cyberattacks were directed not at large businesses but at businesses with less than 250 employees. In 2012, the National Cyber Security Alliance found that 60 percent of small businesses shut down within 6 months of a data breach."[208] While these entities likely shut down due to incurred litigation fees from civil liability suits as a result of personal information having been breached, such lawsuits could have been prevented through stronger cybersecurity. However, the Act does not adequately provide cybersecurity resources to these entities.

The provision of cybersecurity resources can be established through developing a cybersecurity framework similar to that developed by the NIST.[209] However, further protection should be provided through the DHS' assessment and analysis of where small businesses, in general, are most exposed to a cyberattack. The Act only requires relevant agencies to pay "attention to accessibility and implementation challenges faced by small business[es]."[210] The Act's provision, as it stands, will not sufficiently help small businesses develop and implement adequate cybersecurity.

F. Advancing Technology

Technology allows entities, whether non-federal or federal, to create operational efficiencies that then result in increased productivity. However, as all entities rely more on technology, entities store larger amounts of data on cyberspace. A portion of data that entities store on cyberspace will ultimately contain the personal information of employees

---

207 U.S. SMALL BUSINESS ADMIN., SMALL BUSINESS MARKET UPDATE, JUNE 2015, (June 2015), https://www.sba.gov/sites/default/files/Small_business_bulletin_June_2015.pdf.

208 Cong. Record, House of Representatives, 161 CONG REC H2426, Vol. 161, No. 60, NATIONAL CYBERSECURITY, https://www.gpo.gov/fdsys/pkg/CREC-2015-04-23/html/CREC-2015-04-23-pt1-PgH2426-2.htm.

209 *See generally* National Institute of Standards and Technology, *supra* note 60.

210 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113 §103).

or customers. Additionally, the essential functionalities of entities will likely be conducted on information systems that operate on cyberspace. It is necessary to develop a platform to allow current cybersecurity to evolve in-line with technological advancements to prevent the impact of large-scale cyberattacks.

Congress should draft additional legislation that will promote the continued development of cybersecurity technology. While the Act focuses on advancing internal defenses of the federal government, no such provision addresses the important issue of helping non-federal entities advancing their own internal defenses.[211] The Act directs the DHS to "continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity."[212] Although it is important to ensure the advancement of the government's internal defenses, Congress could amend the Act to provide a framework to non-federal entities that addresses how non-federal entities could advance their own internal defenses. Through this framework, Congress could outline in detail, similar to the cybersecurity framework developed by the NIST, the critical aspects of developing and improving existing cybersecurity in order to cope with the complexities of new technology.[213]

VII. THE CONTINUED BATTLE

Federal and non-federal entities ability to share critical cybersecurity information will prove to be beneficial to the United States. Hackers and foreign nations are continuously carrying out cyberattacks against the United States; while the Act effectively addresses the elements of liability, information dissemination, and privacy rights, the elements of critical infrastructure, small businesses, and technology must be strengthened.

The United States' cyberspace not only contains our citizens' personal information, but also provides the ability for businesses to maximize their productivity. While the Act does require various appointed Under Secretaries to analyze how to protect multiple aspects of our economy, the Act does not provide necessary cybersecurity resources to both non-federal entities within our critical infrastructure

---

211 *Id.* at §224.

212 *Id.*

213 *See generally* National Institute of Standards and Technology, *supra* note 60.

and to small businesses.[214] Non-federal entities can only build strong cybersecurity platform if they have access to relevant technology. Large portions of non-federal entities have the financial resources to acquire such technology. However, many critical infrastructure entities and small business entities, due to financial restraints, are unable to acquire necessary information and technology. Congress should address these needs by developing and providing a cybersecurity framework, similar to that developed by the NIST, which will allow entities to access necessary technological resources.[215] However, unlike the framework NIST developed, Congress should ensure that the necessary pieces of technology are available for entities to acquire the necessary technology to implement the newly developed framework.

The federal government can create a cybersecurity framework through creating a task force of cybersecurity experts. This particular task force can develop guidelines and proper steps that non-federal entities could follow to build a stronger cybersecurity platform. Additionally, this task force would provide access to technological resources necessary to build a better cybersecurity platform. However, the federal government must prevent the public disclosure of this technology. If hacker and foreign adversaries acquired these technological building blocks, both could process the information and conduct cyberattacks that would expose the weakness of the technology. As a result, the federal government should require an application process that entities must follow to gain access to cybersecurity technology. An application process will protect the proprietary nature of the key components necessary to build, as well as to continuously advance the technology of a stronger cybersecurity platform.

As the world becomes more technologically reliant, our country's people and our country's economy become exposed to additional vulnerabilities. These vulnerabilities are exposed through the numerous cyberattacks carried out by both financially motivated hackers and foreign adversaries of the United States. While President Obama has signed into force the 2015 Act, the Act does not properly protect critical infrastructure or small business, and fails to address the need of helping entities implement and advance cybersecurity technology.[216] Congress has the ability to strengthen these elements and can and should do so through following the proper legislative channels.

---

214 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).

215 *See generally* National Institute of Standards and Technology, *supra* note 60.

216 H.R. 2029, 114th Cong (2015) (designated as Pub. L. No. 114-113).