The Global Business Law Review

Volume 6 | Issue 1 Note

12-1-2016

Mitigating Cyber Risk in IT Supply Chains

Maureen Wallace
Cleveland-Marshall College of Law

Mitigating Cyber Risk in IT Supply Chains

By: Maureen Wallace

ABSTRACT

This note argues that the United States needs to utilize current federal agencies to begin introducing cyber supply chain risk management regulation for IT supply chains. Cyber supply chain risk management is a critical area of cybersecurity that has barely been recognized by the United States government. The globalization of the digital world has introduced a new spectrum of risk management issues that affect the products exchanged by businesses and consumed by individuals and government agencies. While there have been some initiatives toward the promotion of tighter cybersecurity regulation, most initiatives only concern the public sector, leaving the private sector vulnerable. This note argues that the United States needs to redeploy existing federal agencies to begin introducing cyber supply chain risk management regulation for IT supply chains.

The Global Business Law Review
Spring 2016

I. INTRODUCTION

Cybersecurity is an issue on the forefront of every industry. Governments, businesses, and consumers alike have been introduced to cybersecurity and the many dangers that a "cyberattack" poses. For the purposes of this note, a "cyberattack" is defined as "a deliberate infiltration of a computer system or network with the intent to either extract or destroy confidential information to destroy the functioning of the system or network."[1] Thus, the threat of a cyberattack is something that affects every American, not just the 40 million consumers whose credit card information has been stolen when hackers use malware[2] to digitally compromise computer systems.[3]

As evidenced by the high profile attacks of 2014 and 2015, cyberattacks are becoming a broader trend, with increasing frequency and ferocity "posing grave threats to the national interests of the United States."[4] For example, today there are a total of 22,393,098 different strands of malware, 3,045,722 of which are new strains created between January and June of 2015.[5]

The complexities of cyberattacks are growing exponentially, endangering nearly every entity within the public and private sectors. Though many of these cyberattacks are not well known or picked up by the media, there have been a series of dangerous consequences regarding cybersecurity, especially within the private sector.

For example, in December 2015, Juniper Networks warned of a vulnerability that had been ongoing for two years before discovery.[6] The firmware that Juniper Networks uses to provide firewalls and virtual public networks for government agencies and the financial services sectors was "backdoored,"[7] resulting in a data breach. The Juniper vulnerabilities are an example

of exactly how dangerous encryption backdoors[8] can be for malicious actors to use at their disposal and why it is important for stricter cybersecurity initiatives within the private sector.

Another recent example of a cyberattack is the malicious hacking of the Hollywood Presbyterian Medical Center in February 2016.[9] A hacker seized control of the hospital's computer systems and demanded a ransom in return for the decryption key needed to restore the computer systems.[10] While there appears to have been no loss of life or significant damage from the attack, it is evident that this type of cyberattack could do significant damage under other circumstances.

Though there have been proposals, legislative acts, executive orders, and studies conducted regarding cybersecurity, there is a lack of acknowledgement of the risks associated with the IT supply chain. The IT supply chain is a major source of vital technological products the country as a whole relies on, and there are serious vulnerabilities within the supply chain that must be addressed through proper cyber supply chain risk management (SCRM) procedures. As Michael Hayden, former C.I.A. and N.S.A. director warned, "[d]anger is everywhere and also nowhere; being invisible, cyber crime is easy to put out of your mind…[it] is faceless and creeps in on little cat feet. You know that, like death, it's coming, but all you can do is hope that someone will fix it before it comes for you."[11] While cybersecurity may be an invisible threat, it is simply too important to ignore.

This note will argue for the redeployment of existing federal agencies to begin introducing cyber SCRM into IT supply chains. Of the various types of cybersecurity threats within the supply chain, the threat of malicious hardware is of particular concern. Recent legislative attempts to regulate cybersecurity have only addressed certain federal agencies, leaving the private sector with a framework that is on a voluntary basis.[12]

Part II of this note will provide a background into the global nature of the supply chain, and how this reliance creates security vulnerabilities, as well as the impact on businesses. Part III will discuss the current initiatives attempting to address the nation's cybersecurity needs. This includes a discussion of the legislative and executive initiatives, the private sector's cybersecurity initiatives, and the European Union's recent cybersecurity standard. Finally, Part IV will propose slowly regulating cyber SCRM through the use of current federal agencies, such as the U.S. Customs and Border Protection. Once the federal government begins to introduce cyber SCRM regulation, the government can begin to establish a more permanent regulatory framework for both the public and private sectors,

II. THE SUPPLY CHAIN & THE AFFECT ON INFORMATION TECHNOLOGY

Industrialized nations' social order relies on technology for all types of industries, from communication to entertainment, safety to medicine, transportation to national security. Technology has become so commonplace that there is no question from where or how the pieces of these technological devices end up in computers, phones, vehicles, pacemakers, televisions, or other devices. The reality, of course, is that each part of our technological devices is created with the help of numerous hands, from all over the world. In other words, these devices are products of the supply chain.

The National Institute of Standards and Technology (NIST) has defined "supply chain" as "a set of organizations, people, activities, information and resources for creating and moving a product or service from suppliers through to an organization's customers."[13] Supply chains are not a new concept, especially on the regulatory front. However, the technological boom in the last century introduced a new set of risks to supply chains, especially regarding the field of information technology (IT), which includes equipment such as software, firmware, and services

used in the collection of data or information.[14] This "supply chain risk" is defined as the "risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[15]

To narrow the vast nature of IT for the purposes of this note, it is essential to understand three different elements within IT products. The first element is hardware, which is commonly referred to as the physical component of a computer, such as the motherboard, hard drive, and RAM.[16] Hardware also includes "computer chips, which process and complete the work needed to perform a given task."[17]

Working together with hardware for the essential functions of technological devices is the second element, firmware, which "is the essential, embedded software needed for basic hardware operation."[18] Firmware operates as a "software program or set of instructions programmed on a hardware device [providing] the necessary instructions for how the device communicates with the other computer hardware."[19]

The third element includes embedded systems, which are components of both hardware and firmware. Embedded systems are typically housed on a microprocessor board with the programs stored in ROM.[20] Virtually all devices with a digital interface have embedded systems, including cars, microwaves, televisions, and wrist watches.[21] Due to their prevalence in devices, "embedded systems often provide critical functions that could be sabotaged by malicious parties…[by] send[ing] or receiv[ing] sensitive or critical information using public networks or communications channels accessible to potential attackers…"[22]

An example of how vulnerable hardware may become while in the supply chain is the design and manufacture of computer chips. The critical, everyday devices chips are found in, such as small scale cell phones and computers to large scale power grids, can only run properly if the chips they contain are free of malware.[23] Chip design has become a global enterprise, with around 1500 companies in the world dedicated to it.[24] The full "chip ecosystem," consisting of designers, manufacturers, companies that use chips in products, individuals, and other entities that purchase these products, all rely on the assumption that the chips designed are reliable and secure.[25] Because chip hardware generally cannot be changed once the chip leaves the factory, malware "can only be inserted by someone who can access and alter the design before it is manufactured and placed in a product."[26] For example, "the design process for a single chip can involve contributions from hundreds of people, many of whom may be employed by third party companies that simply provide functional blocks and who have little or no stake or interest in the success of the chip."[27]

The microscopic nature of chips also makes them vulnerable to malware.[28] Outsourcing within the chip industry has been a significant contributor to the list of potential vectors for the insertion of malware.[29] Though outsourcing has economic benefits, including lower labor costs and competition in the industry, "the combination of growth in both complexity and outsourcing means that the number of people with access to the design for a single chip during its development can easily number in the hundreds."[30] While outsourcing the design and manufacture of hardware in the supply chain is part of a global economy, there are still ever-present threats to the security of the hardware being produced and sold to companies and governments that rely on privacy and national security.

Due to the global nature of the essential elements of IT products, the threat of potential malicious attack is prevalent. It is dire for components within technological devices to safeguard the data that the country's privacy and national security rely upon.

The Global Nature of the Supply Chain

Globalization has been greatly aided by technological advancement, causing the IT marketplace to rely on global supply chains to meet its growing needs.[31] Today, IT supply chains include multiple organizations and regions for production, making the supply chain difficult to manage.[32] These supply chains include important products that the world relies upon, such as "servers, routers, and personal computers…that are globally sourced."[33] Due to the "expansive and international field of technology suppliers…these [products] [are] often created with pieces [from] many different companies,"[34] making it difficult to narrow down where each part of the product came from, let alone to a single country. As a result, governments have less insight and less control over how these suppliers conduct their operations, leaving security gaps in the global supply chain.[35]

Because many participants in the supply chain do not have an interest in the success of these products, or may be an adversary, the reliance of the United States on the global supply chain presents risks. These include "threats posed by actors – such as foreign intelligence services or counterfeiters – who may exploit vulnerabilities in the supply chain,"[36] which affects national security, privacy of our information, and the physical infrastructure of our county. With this in mind, the main concern is that "an adversary may sabotage, maliciously introduce unwanted functions, or otherwise subvert design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system in order to conduct surveillance…deny access to, disrupt, or…degrade its reliability or trustworthiness."[37]

Specifically, the insertion of malware into the devices within the supply chain, the creation of "back doors," and the threat of counterfeit hardware are three of the potential risks posed by the lack of strong cybersecurity measures that prevent and mitigate harm.

Significant damage is caused when an attacker uses the supply chain to intentionally insert malware into the hardware or firmware of a product, allowing attackers to take control and "read, modify, or delete sensitive information; disrupt operations; [or] launch attacks against other organizations' systems."[38] Because firmware and hardware are intertwined, if malware is inserted into the firmware of a component, it is extremely difficult to detect due to the microscopic nature of the circuits that the malware would be hiding in,[39] making the piece of hardware appear legitimate. Dangerously enough, "it is possible to look directly at malicious firmware and not see anything wrong with it [because] cleverly written malware will perform the kinds of operations that the system is routinely supposed to perform…[but] at exactly the wrong time."[40] By attacking the hardware of IT products while in the supply chain, an attacker then has many opportunities at his fingertips, including overt and covert attacks, the creation of backdoors, and the insertion of counterfeit hardware.

Once malicious code is inserted into the hardware, an attacker is able to launch various types of attacks, including overt and covert attacks. An overt attack allows the malicious hardware to either cease all functioning or impair the functioning of the product.[41] Here, the existence of a problem would be recognized, although the cause of the problem would not be clear.[42] For example, an overt attack of a mobile phone would cause nothing more than inconvenience, however, that same type of attack on a larger scale could be devastating for national infrastructure.[43] On the contrary, a covert attack causes the appearance of normal operation, while the malicious action quietly works in the background.[44] An example would be a

corrupted computer chip within a system that could send copies of confidential data to any third-party destination, without the user's knowledge.[45]

Another type of covert attack is one that leaves the device operating normally, but introduces corruption to the data at some point in time, not necessarily right away. For example, placing a location-based trigger into the malicious code can attack the hardware of a GPS chip.[46] This would leave the GPS functioning normally, until it is reaches a certain geographic region, at which time the trigger would shift the GPS locations by a few hundred feet. This type of attack would not be easily detectable in advance.[47] These attacks showcase the variations of which an attacker can manipulate hardware to trigger the attacks months, even years later.

The creation of "backdoors"[48] is another type of attack. In general, a backdoor is "a malicious program that can potentially give an intruder remote access to an infected computer."[49] Backdoor creation presents a hidden method for bypassing normal computer authentication systems, and is not limited to malware because it also affects chips and memory.[50] One type of a backdoor is "ticking time bombs," which allows the attacker to program the backdoor to automatically trigger "after a pre-determined fixed amount of time after the power-on of a device."[51] This could force the device to crash or operate maliciously[52] making it clear that this could be a devastating attack on a large scale. This type of backdoor has the potential to allow an attacker to "design a kill switch function that could be undetectable by any validation methods."[53]

Furthermore, the installation of counterfeit software and hardware is another significant risk to the IT supply chain. Counterfeit information technology is hardware or software that contains non-genuine components or code.[54] The United States Department of Defense has reported that counterfeit products threaten the "integrity, trustworthiness, and reliability of

information systems" because they are usually (1) "less reliable and therefore fail more often and more quickly than genuine parts," and (2) "counterfeiting presents an opportunity for the insertion of malware or backdoors into the copies that would be more difficult in more secure manufacturing facilities."[55]

Counterfeit components are prevalent among many IT products. A March 2013 study by the International Data Corporation "found that at least one-third of all PC software is counterfeit."[56] The result of counterfeit software causes users to experience decreased computer performance, viruses, spam, or complete failure of the software or computer. Counterfeit hardware is even more difficult to identify and remedy because of the use of backdoors, which could automatically activate malware or wait for the command of a certain date or location.[57]

The harmful effects of counterfeit hardware are exhibited in a recent example affecting the public sector. In October 2011, two people were convicted of selling 59,000 counterfeit circuits produced in China to the U.S. military to be used on U.S. warships, airplanes, and missiles.[58] Through the use of counterfeit hardware, the fake circuits could have "potentially contained serious vulnerabilities that could have disabled, impaired, or stolen information from these important systems."[59] Additionally, the Commerce Department has reported a "doubling of counterfeit incidents between 2005 and 2008 to more than 9,356 cases."[60]

The various tools that attackers have at their disposal are worrisome. These types of attacks are the result of hackers that prey upon the vulnerabilities of a system. Because of this, it is vita to have tightened cybersecurity measures to detect and prevent potential cyberattacks.

Vulnerabilities

In 2012 the United States Government Accountability Office (GAO) was instructed to study and identify risks associated with IT supply chains used by federal agencies, and how

national security-related departments have been addressing these risks.[61] The study found that reliance on the global supply chain leads to many risks posed that could adversely affect government agencies' missions. The study identified and described four supply chain vulnerabilities that can be threatened by the installation of hardware that contains malicious code.[62] These vulnerabilities include (1) the lack of adequate testing for software updates and patches,[63] (2) Incomplete information on IT suppliers, (3) the use of supply chain delivery and storage mechanisms that are not secure, and (4) the acquisition of information technology products or parts from independent distributors, brokers, and the gray market.[64]

The lack of adequate testing for software updates and patches occurs when system updates or patches go untested, which increases the risk that an attacker could insert malware into the system.[65] An example of this would be an agency or contractor that "fails to validate the authenticity of patches with suppliers," leading to an attacker being able to write fake patches that could potentially allow unauthorized access to the system.[66] Lack of adequate testing for updates leaves devices vulnerable to the threat of the installation of hardware or software containing malware.[67]

Incomplete information on IT suppliers occurs when IT equipment is acquired without understanding the "supplier's past performance or corporate structure."[68] By not inquiring into the past performance of a supplier, there could be the risk of deficient products, or the supplier could be an adversary who would now have access to sensitive information.[69] For example, without background knowledge as to who the supplier is and what the structure of the supplier includes, the agency acquiring the IT equipment would not be able to know if the supplier or their employees "are subject to undue foreign control or influence."[70] Inadequate information regarding the IT supplier leaves devices vulnerable to the installation of hardware or software

containing malware, the installation of hardware or software that contains unintentional vulnerabilities, the installation of counterfeit hardware or software, failure or disruption in the production or distribution of critical products, and the possible reliance on a malicious or unqualified service provider for the performance of technical services.[71]

The use of supply chain delivery and storage mechanisms that are not secure causes an increased risk that the IT product would be threatened while in transit to the purchaser.[72] This vulnerability could allow "a[n] [attacker] to gain unauthorized access to the IT product, thereby facilitating unauthorized modification, substitution, or diversion."[73] Ultimately, this could lead to the exposure of sensitive information[74] without the knowledge of the purchaser. The use of unsecure delivery and storage mechanisms leaves devices vulnerable to the threat of the installation of hardware or software containing malware, and the installation of counterfeit hardware or software.

The acquisition of information technology products or parts from independent distributors, brokers, and the gray market increases the risk of encountering substandard, subverted, and counterfeit products.[75] Independent distributors purchase products for the purpose of redistributing them back into the market, without any contractual agreement with the original manufacturer or brokers, that works to locate parts that customer's request.[76] Here, "the gray market refers to the trade of parts through distribution channels that, while legal, are unofficial, unauthorized, or unintended by the original component manufacturer."[77] Dealing with independent distributors and brokers leave devices vulnerable to counterfeit products.

Although the GAO report was commissioned for purposes related to federal agencies, these vulnerabilities are applicable to both the public and private sector. Many recent examples of hardware attacks in consumer products prove how real of a threat cyber attacks can be. To

illustrate the ease of attacking the hardware of common, everyday devices, two examples are detailed below – personal computers and USB drives.

In 2014, Lenovo, one of the world's largest sellers of personal computers,[78] began pre-installing "Superfish"[79] to their products to make it easier to "shop for deals" on the web, and consequently allowed attackers access to a person's Internet traffic and browser history.[80] "Superfish intentionally pokes a gigantic hole into your browser security and allows anyone on your Wi-Fi network to hijack your browser silently and collect your bank credentials, passwords, and anything else you might conceivably type there."[81] Robert Graham, a cybersecurity enthusiast from Errata Security, tested the vulnerability of Superfish, finding it incredibly easy to attack because he was able to intercept the encrypted communications of Superfish victims all while "hanging out near them at a café wifi hotspot."[82] What makes Superfish unusually dangerous is that it is not just another program like Microsoft or Adobe, it is a code that is hidden from everyday users.[83] This is one of the best examples of a hardware "attack"[84] because Superfish was inserted into the Lenovo computers while they were still in production.

It may seem inconceivable that something like this could happen, however, since the 1990s, it has been commonplace for software and programs showing ads to be preloaded without the permission of consumers.[85] Essentially, consumers trust that their devices will not come with vulnerabilities like Superfish, but the reality is that this common practice puts consumers at risk for cyber threats.[86]

Another common device that has been easily attacked are USB drives, also commonly referred to as thumbdrives. These small devices help transport data and information from multiple devices. One of the problems with a USB attack is that these devices were not designed to prevent exploitation.[87] This was proven in July 2014, when two researchers from the Security

Research Labs in Berlin announced their discovery of how to overwrite a USB device's firmware and carry out malicious actions.[88]

The experiment, labeled "BadUSB," showed how an attacker can hack and reprogram embedded firmware to give a USB device "new, covert capabilities," such as "transforming keyboards, web cams, and other types of USB-connected devices into highly programmable attack platforms that can't be detected…"[89] This is especially dangerous because it is impossible for the host device to detect the malicious firmware code, but the firmware code is able to interact and modify the host computer's software unbeknownst to the user.[90] The malicious code is capable of planting other malware in the device, stealing the device's information, and diverting Internet traffic – "all while bypassing antivirus scans."[91] In order to detect a tampered device, advanced forensic methods, including physically disassembling and reverse engineering the device, is required.[92] In addition to lack of detection, BadUSB-corrupted devices are hard to disinfect. "Because the tampering resides in the firmware, the malware can be eliminated only by replacing the booby-trapped device software with the original firmware."[93]

As alarming as these examples may appear, they are simply the "tip of the iceberg" because "any hardware device plugged into your computer with a firmware component can probably be made malicious."[94] Despite the pressing need for governmental action in preventing these types of cyberattacks, the current state of the law does not address these types of threats.

The Impact on Business Interests

Businesses are major actors in the IT supply chain, making the security of their products a top priority to not only safeguard products for government and consumer use, but also to inhibit the costs of potential cyberattacks. Cybersecurity has a substantial impact on the international business realm, especially economically. To enhance this point, it is important to

examine the impact upon business leaders as expressed through reports and surveys of key stakeholders in the business realm.

In general, cybercrime costs the global economy about $450 billion each year, exceeding both the U.S. farming and oil-and-gas markets.[95] A recent report on global risks from the World Economic Forum "found U.S. CEOs are more concerned about cyber-related threats and attacks than fiscal crises, asset bubbles and energy prices."[96]

Furthermore, a recent survey conducted by Mayer Brown LLP, taken from top executives and corporate counsel, demonstrates the importance of cyber SCRM in the private sector. The scope of the survey ranged from fifteen different industry sectors, including financial institutions, professional services, utilities, energy, and healthcare.[97] The survey asked the respondents a number of questions regarding the biggest threat their companies face, the effectiveness of NIST's Cybersecurity Framework, and their overall outlook on cybersecurity. The survey results revealed the importance of cybersecurity in the private sector, especially for the prevention of data breaches. For example, of those surveyed, 63% considered the disclosure of personally identifiable information as the biggest cyber threat to their companies.[98] Cyberattacks are a serious threat to businesses, especially considering the economic consequences in the aftermath of a cyberattack.[99]

The results of the survey also revealed that businesses anticipate more support from the federal government, with 84% of respondents stating they expect clear, national standards on data breach notification to emerge within the next five years.[100] This references the federal government's creation of multiple levels of authority within agencies and sub-agencies that cause confusion, especially when there are various reporting standards, rather than one clear set of standards for information security.[101]

Interestingly enough, though they may be aware of the risks of cyberattack, the majority of U.S. businesses are completely unprepared for cyberattacks. This is evident by the percentage of companies reporting losses of $1 million or more due to cybercrime, a number that has doubled since 2014.[102] For example, the 2016 Global Economic Crime Survey conducted by PwC found that only 48% of U.S. respondents[103] had a first-responder team that handles cyber-related incidents.[104]

These various survey results all reflect the importance of cybersecurity in business, and because the very essence of business has become globally digitalized, the security of the products being exchanged through the IT supply chain is of utmost importance.

III. THE CURRENT STATE OF THE LAW

Executive Initiatives

Today, multiple federal agencies have initiatives to better address cybersecurity, but most of these are directed toward the public sector. Over the past decade, presidents, executive departments, and federal agencies have all addressed cybersecurity needs. Presidents George W. Bush and Barack Obama have both addressed cybersecurity through the use of executive orders.[105] In addition, the Departments of Homeland Security and Defense each have prominent roles within cybersecurity, especially the Department of Homeland Security, which has several sub-departments that address various sectors of cybersecurity. Finally, federal agencies have a role to play as well, especially the National Institute of Science and Technology (NIST), which created a voluntary cyber risk management framework for the use in both the public and private sectors.

In 2008 President Bush launched the Comprehensive National Cybersecurity Initiative (CNCI) as a part of his National Security Presidential Directive/Homeland Security Presidential

Directive.[106] The CNCI set out a list of initiatives to better address the United States' growing cybersecurity needs. Of particular significance is Initiative 11, which is a multipronged approach to address global supply chain risk management, stemming from both domestic and global supply chains.[107] The risks stemming from the supply chain require strategic and comprehensive management "over the entire life cycle of products, systems, and services."[108] Initiative 11 further details that this management will require,

> a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the life cycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices.[109]

After taking office, President Obama addressed the seriousness of cybersecurity and adopted the CNCI, but was advised to build upon it because the Initiative needed some updating and evolving to fit the current needs of the country.[110]

In its report on the IT Supply Chain in March 2012, the GAO examined the effectiveness of the CNCI, and found that it faced many challenges meeting its objectives,[111] including defining the roles and responsibilities of oversight, establishing measures of effectiveness, and transparency, especially regarding supply chain management.[112] One of the greatest setbacks for cybersecurity risk management is the lack of uniform oversight. Rather than having one body of management, there are currently several departments and agencies that address cybersecurity needs. Though there are a number of agencies with roles to play, this note will focus of the oversight of the Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Institute of Standards and Technology (NIST).

Due to the vast nature of cyberspace, including the number of malicious actors that can operate from anywhere in the world, the physical link between cyberspace and critical

infrastructure, and the difficulty in handling every vulnerability of complex cyber networks, the DHS has become instrumental in cyber risk management.[113] As DHS has recognized, with increasingly sophisticated IT systems, the risk of cyber threats upon infrastructure that affects the daily lives of millions of Americans is of grave concern, and therefore warrant the creation of multiple sub-agencies within the Department.[114] The DHS boasts an ample amount of legal authority "to serve as the central repository and distributor of cyber-intelligence for the federal government."[115] Although agencies are important in addressing cybersecurity in the country, the authorities often overlap, "resulting in confusion as to which of the multiple sub-agencies within DHS or even outside DHS" should be managing which threats.[116] It is also important to note that out of the various agencies, advisory groups, and other components of the DHS, there is no specific agency to address cyber SCRM.[117]

For example, in 2006 Congress created the Office of Cybersecurity and Communications (CS&C), which is responsible for enhancing security, resilience, and reliability while protecting the public and private sectors from disruptions to critical infrastructure.[118] The CS&C carries out this mission through its five divisions: the Office of Emergency Communications, the National Cybersecurity and Communications Integration Center, Stakeholder Engagement and Cyber Infrastructure Resilience, Federal Network Reliance, and Network Security Deployment.[119] These sub-agencies each have their own goals addressing aspects of cybersecurity, with the exception of the supply chain.[120]

In addition to the DHS, the Department of Defense (DoD) also has a role in cybersecurity. The DoD works with other U.S. government agencies to help defend the U.S. homeland and interests from attack, including those attacks that occur in cyberspace.[121] In the Department's 2015 Cyber Strategy report, the DoD addressed its three primary missions in

cyberspace. First, recognizing its own dependence on cyberspace for training, organizing, and equipping the U.S. military, the DoD "must defend its own networks, systems, and information" first.[122] Second, to address the significant consequences of cyberattacks such as adverse foreign policy, property damage, economic impact, and possibly loss of life, the DoD "must be prepared to defend the United States and its interests against cyberattacks or significant consequence."[123] Third, in case of cyber military attacks against adversaries or to protect U.S. interests, the DoD "must be able to provide integrated cyber capabilities to support military operations and contingency plans."[124] The DoD's role in cybersecurity is a defense mechanism to be employed when the nation's cyber vulnerabilities are breached.

Following the failure of the Cybersecurity Act of 2012,[125] President Obama issued Executive Order 13,636: Improving Critical Infrastructure Cybersecurity (Cybersecurity EO).[126] The Cybersecurity EO called for increased information sharing between federal agencies and the private sector, and it also called upon "federal agencies to address privacy and civil liberties concerns at the highest agency levels."[127] The Cybersecurity EO makes the Attorney General, Secretary of Homeland Security and the Director of National Intelligence the principal coordinators of the EO.[128]

In addition, the Secretary of Homeland Security must work with the Director of the National Institute of Standards and Technology (NIST) to "lead the development of a framework to reduce cyber risks to critical infrastructure (the Framework)."[129] The Cybersecurity EO requires the Cybersecurity Framework to "include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" while also aiming to incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[130]

The Framework's purpose is to be a flexible, repeatable, cost effective approach to the reduction of cyber threats.[131] The Framework consists of a collaboration of federal agencies and other stakeholders, giving those within the public and private sectors the opportunity for an open public review and comment process.[132] The Framework is implemented as a part of the "Voluntary Critical Infrastructure Cybersecurity Program established by the Secretary in conjunction"[133] with other agencies in order to support the "adoption of a Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities."[134] The Cybersecurity EO does address important cybersecurity risk management efforts, however, it does not explicitly reference the issue of cyber SCRM.[135]

As a result of the Cybersecurity EO, NIST launched the first version of the Cybersecurity Framework (the Framework), in 2014, along with a "Roadmap" to outline NIST's next steps, and to identify key areas of cybersecurity development.[136] Since its release, the Framework's value has been validated by "a large volume and breadth of interactions between NIST and industry."[137]

The Framework's most frequently cited benefit is the common cyber risk management language that allows for efficient and precise discussions across a company's management structure, from auditors to supply chain partners.[138] Another benefit of the Framework is its versatility. "The Framework was designed as a multi-sector document that individual sectors could tailor in ways that might make it more relevant and useful to organizations operating within their sector."[139] The availability and ease of the Framework makes it a realistic and workable part of any company, agency, or industry leader's cybersecurity policy.[140]

In addition to its Cyber Supply Chain Risk Management Best Practices,[141] in April 2015 NIST released its Special Publication 800-161, Supply Chain Risk Management Practices for

Federal Information Systems and Organizations.[142] Special Publication 800-161 is a 282-page report that painstakingly details a multi-tiered approach for federal government agencies to follow. The Publication addresses the concerns of federal agencies about the risks associated with IT products and services within the supply chain, acknowledging vulnerabilities due to malware, counterfeit products, and poor manufacturing practices.[143] It also "provides guidance to federal agencies on identifying, assessing, and mitigating" IT supply chain risks, and integrates IT SCRM into federal agency risk management activities.[144]

Along with the various executive actions taken by United States departments and agencies over the past several years, in 2012 President Obama announced a National Strategy for Global Supply Chain Security (hereafter the Strategy).[145] The announcement introduced two goals: (1) "to promote the efficient and secure movement of goods," and (2) "to foster a resilient supply chain."[146] The Strategy provides guidance to U.S. departments and agencies, and identifies the country's priorities for stakeholders going forward.[147]

The Strategy calls for a better understanding of supply chain threats and risks by the United States government, advancing technology by building more resilient critical infrastructures, identifying and promoting necessary legislation that prioritizes supply chain standards, and fostering the sharing of information and policies with industry partners, critical infrastructure owners and operators, and other stakeholders.[148] The Strategy addresses supply chain concerns in the fields of medicine, cargo, transportation, nuclear detection, national security, and multi-national corporations. Although there has been some progress in these areas, and the government has a better understanding of the threats to the supply chain, there is still much work to be done.

As President Obama's presidency comes to a close, the Administration has been strengthening his legacy by attempting to increase the country's cybersecurity spending by 35% as well as by attempting to establish a Cybersecurity National Action Plan.[149] In the final budget of his presidency, President Obama has included a $19 billion cybersecurity request, $3 billion of which would be used to update the government's computer systems, some of which have software systems dating back to the 1960s.[150]

Through the Cybersecurity National Action Plan, the Commission on Enhancing National Cybersecurity is to be established with the collaboration of "strategic, business, and technical thinkers from outside of government."[151] Given the importance of cybersecurity for government and consumers alike, the Commission is to focus on a National Cybersecurity Awareness Plan to help raise awareness about the increasing threats of the digital world upon consumers and businesses. The National Action Plan is designed to help modernize current federal IT systems, as well as keep the citizenry informed and aware of the potential risks posed by cyber threats. In addition, the Plan helps establish the position of Chief Information Officer, who is to help drive these new initiatives across the public sector.[152] While the new Cybersecurity campaign and initiatives are a positive step toward a more secure digital world, like the majority of other executive initiatives, neither the Plan nor the Commission have incorporated an in-depth solution towards cyber SCRM.

With all the executive actions taken toward heightened cybersecurity, only NIST's Cybersecurity Framework applies to the private sector. It is important to address federal agency cyber SCRM, but the private sector is just as vulnerable. While these executive actions are a good start towards a more secure supply chain, more legislative action in this area is needed to enhance the executive actions.

Legislative Initiatives

There have been several legislative initiatives regarding cybersecurity, but since 2014 only a handful has become law.[153] At the end of 2014, during a lame-duck session of Congress, four cybersecurity bills were enacted to law.[154] Aside from cybersecurity bills, Congress has also included cybersecurity provisions within appropriations bills for certain agencies and the Defense Authorization Act of which explicitly mention cyber SCRM. This section will detail the four cybersecurity bills enacted to law in 2014, the Appropriations Acts of 2014 and 2016, and the Defense Authorization Act of 2011. Just as the executive initiatives toward cybersecurity and cyber SCRM have been primarily focused on the public sector, the legislative actions taken thus far have also been focused on the public sector, leaving the private sector to its own devices.

The Federal Information Security Modernization Act (FISMA) was passed as a way to reform oversight of federal information systems[155] by amending and modernizing the 2002 Federal Information Security Management Act (FISMA). The amendments grant authority to the DHS in the implementation of security policies, shifting the focus of threats and vulnerabilities to data involving personal information.[156]

The second act passed was the National Cybersecurity Protection Act, which amends the Homeland Security Act of 2002,[157] essentially codifying the Department of Homeland Security's National Cybersecurity and Communication Integration Center (NCCIC).[158] The third act passed was the Cybersecurity Enhancement Act. This Act amends the National Institute of Standards and Technology Act by codifying NIST's Cybersecurity Framework.[159] The fourth act is the Cybersecurity Workforce Assessment Act, which enhances cybersecurity in the workforce.[160] This Act gives the Secretary of Homeland Security the authority to assess the cyber workforce, while developing, maintaining, and updating a comprehensive workforce strategy.[161]

Aside from direct cybersecurity legislation, Congress has implemented cyber SCRM into (1) the appropriation bills for the Departments of Commerce, Justice, NASA, and the National Science Foundation, and (2) the 2011 National Defense Authorization Act. In the 2015 appropriations bill, Congress added a section that addresses specifications for the appropriation of funds when acquiring "high-impact" or "moderate impact" information systems.[162] The bill prohibits the acquisition of these systems unless the agency has: (1) reviewed the supply chain risk against criteria developed by NIST, (2) reviewed relevant threat information provided by the Federal Bureau of Investigation (FBI), and (3) consulted the FBI in assessing any risk of cyber-espionage or sabotage associated with the acquisition of the system, including risks associated with production, manufacture, and assembly by entities identified by the United States as posing a cyber threat, especially products handled by China.[163] In addition, no funds appropriated may be available unless the head of the assessing entity has, (1) worked with NIST to develop a mitigation strategy for identified risks, (2) determined that the acquisition is in the national interest of the United States, and (3) reported that determination to Congress.[164]

In the National Defense Authorization Act for fiscal year 2011, Section 806 lists the "requirements for information relating to supply chain risk."[165] This section examines the rights of the DoD in the "covered procurement"[166] of goods and services for government purposes.[167] The Act sets out specific provisions for the agency head to consider when procuring goods, including the national security implications and the appropriate congressional committees to be notified of procurement.[168] The Act defines "covered procurement action" as,

> (A) The exclusion of a source that fails to meet qualification standards…for the purpose of reducing supply chain risk in the acquisition of covered systems. (B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order. (C) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a

> contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.[169]

The National Defense Authorization Act is to be renewed for fiscal year 2016, which does not include the cyber SCRM provisions as the 2011 Act.[170] On October 22, 2015, President Obama vetoed this draft of the bill.[171]

The most recent legislative action was the 2016 Appropriations Act, which was signed into law in December 2015, and acknowledged cybersecurity by including a section explicitly labeled the Cybersecurity Act of 2015. The Act is a ten-year provision that broadens the powers of network operators to monitor and disclose information.[172] The Act mandates the efforts of the Attorney General and the Secretary of Homeland Security to jointly develop and make publicly available guidelines to help assist and promote the sharing of "cyber threat indicators"[173] with federal entities.[174] This Act is an extension of information sharing that the U.S. government has been akin to promoting in recent pieces of legislation.

Although information sharing between the public and private sectors is essential to help prevent cyberattacks, no duty is imposed on entities to actually abide by the Act. To protect against liability, the Act explicitly states that it is not to be construed to "create a duty to share a cyber threat indicator or defensive measure; or a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure."[175] In addition to not establishing a duty to disclose this information, the Act makes no mention of the cyber SCRM principles.

These legislative initiatives are proof of the importance of cybersecurity, and the growing need for standards when dealing with cyberattacks. However, as important as these initiatives are, there is still a need for more direct legislation that addresses cyber SCRM in the private sector.

Private Sector Initiatives

One of the most prominent international private organizations specifically addressing cyber SCRM is the Open Group. The Open Group is a "technology consortium dedicated to improving business through IT standards."[176] The organization has developed the Open Trusted Technology Provider Standard (O-TTPS) and Framework as a "collaborative, business-developed list of flexible, technology-neutral, and continually updated best practices for supply chain security."[177] The Open Group boasts more than 500 member organizations that include customers, systems and solutions, suppliers, tool vendors, integrators, consultants, academics, and researchers.[178] The Mission of the Open Group is to "drive the creation of Boundaryless Information" achieved by:

- Working with customers to capture, understand and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Development and operation of the industry's premier certification service and encouraging the procurement of certified products[179]

Members of the Open Group participate in forums and workshops that allow members to be introduced to developing IT standards, and also allow members to interact with peers, experts, and industry leaders.[180] The Open Group has various certification programs available in both the professional realm and products and services realm. The certification programs "provide worldwide professional credentials and knowledge" and a "worldwide guarantee of conformance" for products and services.[181]

The Open Group publishes many reports and analyses throughout the year regarding trends and risk assessments. In the 2015 IT Risk Management Survey Summary, the Open Group in association with the Society of Information Risk Analysts (SIRA), and CXOWARE, Inc., presented analysis to help enterprises understand their maturity on risk management practices and to help identify areas that need additional work.[182] The survey questioned 109 IT security executives, professionals, analysts and architects, with the majority being Security IT Risk Managers.[183]

An important observation from the survey results was that risk managers do not tend to rely on a single methodology to frame IT, instead the use of multiple frameworks are a part of their IT risk management efforts.[184] Additionally, it is not surprising that next to regulations, the second most common driver for establishing a risk program are external threats (82%), "given the large number of external threats and cybersecurity events that have occurred within organizations across all industries in the past couple of years."[185] A final observation of the survey is the significance of auditing. Of the numerous ways organizations identify risks, 78% of companies surveyed use auditing, both internal and external, as major parts of risk management programs.[186]

A second private organization that addresses cyber risk management is Crowdstrike, which specializes in incident response and proactive services and is "a leading provider of next-generation endpoint protection, threat intelligence, and pre- and post incident response services."[187]

Crowdstrike is a subscription-based business that gives customers flexibility to use it as a 24/7 service in addition to the customer's own security protocol.[188] Crowdstrike customers

include some of the largest businesses, along with financial service companies, and sectors including energy, oil and gas, telecommunications, retail, and technology.[189]

One of the unique qualities of Crowdstrike is its focus on the adversary as opposed to just malicious attacks.[190] The company's Crowdstrike Falcon program is software that detects, prevents, and responds to attacks at any stage.[191] Falcon "enables customers to prevent damage from targeted attacks, detect and attribute malware and adversary in real time, and effortlessly search all endpoints, reducing overall incident response time."[192] Crowdstrike recognizes that the threat level for a cyber breach has never been higher for organizations trusted with protecting valuable data.[193] The company's relevance today is evident by the recent headlines that prove no company or agency is completely immune to targeted attacks by skilled adversaries.[194]

In 2014 Crowdstrike published the Global Threat Intel Report that studied the various cyber breaches that occurred over the course of the year, from nation-states to point-of-sale (PoS) breaches.[195] The report concluded that the 2014 cyber adversaries were dynamic, persistent and innovative, and to combat these adversaries, defenders must be inventive, diligent, and decisive in their efforts.[196] The report also determined that the most important advantage for defense is having an intelligent defensive team.[197] Incorporating intelligence into the daily defense of an enterprise will continue to be paramount, and the use of this intelligence is essential to stay ahead of the adversary.[198]

The Open Group and Crowdstrike are just two of many private organizations aimed at cybersecurity prevention and mitigation. Both of these organizations are extremely efficient in their practices and have gained international attention by both the private and public sectors. The methods of both organizations should be evaluated by the United States government, and should serve as inspiration for cyber SCRM standards within the private sector.

International Initiatives – the European Union

Due to the globalization of the digital world, every country is affected by the threat of cyberattack and therefore the need for enhanced cybersecurity it prevalent. While most countries have adapted their own various standards to address these growing needs, the European Union (EU) has agreed on the implementation of standard rules, mandating each member-country's participation.

Towards the end of 2015, the EU agreed on its first ever cybersecurity rules.[199] The "patch-work quilt" of cybersecurity breach notification requirements within some member-countries, but not within others, has now turned into a pan-European notification obligation.[200] The actual text of the agreement still needs to be formally agreed upon, which will then give member-countries 21 months to many any necessary changes to their national legislation.[201]

The cybersecurity rules include the regulating of Internet service providers by requiring network companies that provide essential services[202] to ensure their infrastructure is secure and to report any major security breaches.[203] These industries will also be required to fulfill security measures to ensure they can withstand cyberattacks.[204]

To ensure cooperation among all member-states, the rules provide for a strategic "cooperation group" that will exchange best practices, draw up guidelines, and assist member-states in the mandatory adoption of the rules.[205] In addition, each member-state will be required to "set up a network of Computer Security Incident Response Teams (CSIRTs), to handle incidents and risks, discuss cross-border security issues and identify coordinated responses. The European Network and Information Security Agency (ENISA) will also play a key role in implementing the directive, particularly in relation to cooperation."[206]

The EU's cybersecurity rules are important because the rules integrate the standards among essential services, such as energy and transportation, as well as online marketplaces, such as eBay and Amazon.[207] While the rules for Internet service providers would be less strict than those for the essential services sector,[208] the EU still acknowledges the importance of including those providers. These rules are an excellent example of how the United States could begin to standardize cybersecurity within the private sector.

IV. PROPOSED REGULATORY RESPONSE

Despite the vast number of agencies, sub-agencies, and departments working on cybersecurity matters, cyberattacks are still frequent and ferocious.[209] Much of these initiatives focus on securing the supply chain for public sector needs. While these efforts are an important step toward better cybersecurity policy, private sector business interests are not acknowledged, even though the private sector has been frequently affected by cyberattacks.[210]

The analysis of the current state of the law, legislative and executive initiatives, private sector action, and the European Union's cybersecurity rules, demonstrates that the global IT supply chain continues to be unprepared for the increasing number of cyber threats. The United States government has been primarily focused on public sector safeguards, leaving the private sector - where the majority of cybersecurity breaches occur - with a list of best practices and a voluntary framework. Private sector organizations, such as the Open Group and Crowdstrike, have been successful in risk prevention and mitigation; however, the scope of these groups does not encompass the majority of cyber supply chain stakeholders. Finally, while the European Union's cybersecurity rules are an important start toward standardization, the rules do not address supply chain issues.

Effective management of cyber SCRM cannot be achieved quickly or by using one-size-fits-all approaches. To truly combat the issue of cyber SCRM, the United States must address the issue in phases. First, the reality of the threat posed to the IT supply chain must be addressed by the government, and should form the basis for a national conversation to educate the public and businesses about IT supply chain insecurity, its consequences, and preventative steps needed. Second, the government should reconceive the role and better deploy existing agencies, such as the U.S. Customs and Border Protection, as a regulatory mechanism. Third, once the government has educated the public and businesses, and addresses cyber SCRM through current agencies, the final step is to work toward creating a permanent regulatory structure that is dedicated to and expert in resolving cyber SCRM.

Despite the legislative, executive, and private sector efforts thus far, cyber SCRM is still not prioritized. One of the reasons this may be is the fact that many Americans are simply unaware of the dire cybersecurity risks within the IT supply chain. If the United States government brought cyber SCRM to the forefront of the cybersecurity movement, the public demand for more action could compel more regulatory support and initiative.

The U.S. Customs and Border Protection (CBP) is one of the world's largest law enforcement organizations, with a mission that includes safeguarding America's borders by keeping terrorists and their weapons out of the country.[211] In 2001, the CBP established the Customs-Trade Partnership Against Terrorism (C-TPAT) that works with the trade community to strengthen international supply chains and improve border security.[212] When C-TPAT was established, there were seven major partners, a number that today has grown to over 10,000.[213] These 10,000-plus partners account for over 50 percent (by value) of what is imported into the country.[214] The Partnership allows for better risk assessment and targeting through the use of

clear supply chain criteria for partners to meet, and in return provides incentives and benefits, such as expedited processing, for compliance.[215]

In order to gain and retain membership, partners of C-TPAT must meet certain criteria. Upon joining the partnership,

> companies sign an agreement to work with CBP to protect the supply chain, identify security gaps, and implement specific security measures and best practices. Additionally, partners provide CBP with a security profile outlining the specific security measures the company has in place. Applicants must address a broad range of security topics and present security profiles that list action plans to align security throughout their supply chain.[216]

Once the criteria are met, partners are considered low-risk and are less likely to be examined by CBP. Low-risk designation is also based on a "company's past compliance history, security profile, and the validation of a sample international supply chain."[217]

Within this process, "C-TPAT routinely highlights security matters for the purpose of raising awareness, renewing Partners' vigilance, and recognizing best practices implemented to address supply chain security concerns."[218] In doing so, C-TPAT uses FireEye, one of the leaders in cybersecurity solutions, to help partners become aware of their exposure to indirect cyberattack through both the supply chain and third-party relationships, as well as to make them aware of federal cyber defense resources.[219] Currently, C-TPAT is urging its partners to "develop an integrated cybersecurity risk management plan that incorporates security controls and best practices that mitigate risk associated with advanced cyber threats and the use of sophisticated techniques."[220] This includes, NIST's Framework and Special Publications regarding supply chain risk management best practices.[221]

The C-TPAT program has been successful incorporating importers, brokers, consolidators, carriers, foreign manufacturers, and MPTOs within the 10,000-plus certified partners.[222] As of December 2014, 26,624 total validations have been completed, resulting in

1,947 suspensions and 1,375 removals from the program.[223] Because of its success, the program has proved to be an asset to CBP.

While C-TPAT's strategy of encouraging development of cyber SCRM plans and implementing NIST's cybersecurity best practices will help its partners to help prevent and mitigate risk, the C-TPAT program has the potential to have a greater influence on supply chain security. By serving as a level of CBP's cargo enforcement strategy,[224] C-TPAT would be a positive first step toward a national regulatory mechanism that specifically regulates imported technological devices from the IT supply chain.

For example, C-TPAT could begin to extend its membership to the largest IT product suppliers. The CBP along with the government could begin requiring all IT products imported to the United States through the supply chain to be imported by either a partner of C-TPAT or be subjected to spot-check audits of products by CBP. The benefits of compliance already offered to C-TPAT partners would serve as an incentive to expand membership, thereby warranting a more secure supply chain.

Additionally, incentivizing membership within C-TPAT could potentially standardize the flow of products within the IT supply chain. By issuing strict criteria for partners to meet in order to import products into the United States, foreign manufacturing companies would likely become members in order to be considered "low-risk" and to expedite the product flow.

Furthermore, though the idea of auditing IT products from foreign adversaries is not currently implemented by the United States, it is a practice of other countries, such as China.[225] In early 2015, a deal was reached between China and Apple, Inc. for the auditing of Apple products upon arrival to China's market. China's State Internet Information Officer requested, "spot network security audits" on Apple products "in an effort to counter concerns that other

governments are using its devices for surveillance."[226] Although China is one of Apple's largest markets, the country needed assurances that Apple products protect the privacy of its users and China's national security.[227] This is a prime example of how auditing products coming into the United States from the global supply chain can be managed to effectively prevent and deter future cyberattacks.

While the phased approach of better educating the public, redeploying current federal agencies, and beginning to establish a permanent regulatory structure to address cyber SCRM is only a preliminary approach, the United States should use its available resources to begin addressing cyber SCRM. Such standards would need to be flexible in order to adapt to each various sector of business in the cyber supply chain because with such diverse IT fields within each industry, a uniform set of standards would simply be ineffective. The United States can look to the agencies and organizations mentioned in this note as examples to help address cyber SCRM strategies that could help the United States effectively reach the ultimate goal of creating a permanent regulatory mechanism.

V. CONCLUSION

Federal government agencies and private businesses have very different cybersecurity standards. As described above, there are very specific executive and legislative actions that set out to standardize government acquisition of products from the supply chain, yet there are no clear standards for the private sector to follow, even though both the public and private sector interests rely heavily on the IT supply chain. While the private sector does have access to private organizations that offer security products and services, not all global IT supply chain stakeholders are utilizing these organizations. Securing the supply chain would not only benefit the public sector's national security concerns, but would also benefit private sector business

whose products are sold to millions of consumers each year. Because of the reliance of both public and private sectors on the global supply chain, the United States must begin to implement cyber SCRM within IT supply chains vis-à-vis federal agencies already in existence. The U.S. Customs and Border Protection's C-TPAT is a prime candidate to begin this implementation. By slowly implementing a cyber SCRM mechanism, the United States can begin to effectively secure its IT supply chains from cyberattack.

[1] Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions,* CONGRESSIONAL RESEARCH SERVICE (2015), https://www.fas.org/sgp/crs/intel/R43941.pdf. (quoting Jay P. Kesan and Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 439-446 (2012).)

[2] Malware is a malicious code that "can infect computer systems by exploiting operating system, network device, or software vulnerabilities. It can also trick users into activating the malware by opening an email attachment, downloading a file, viewing an image, or visiting a website." Reese Nguyen, Comment, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1094-94 (2013). This type of computer code is designed for the purpose of damaging, disrupting, or stealing data from others. There are other various components of malware as well. Viruses "alter or damage the computer, self-replicate, and spread to other computers when the host file or program to which the virus attaches is intentionally transferred from one computer to another." *Id.* Trojans are another type of malware that appears to be legitimate, but is actually hiding among the common, trusted files. Trojans "require that the user invite the malware in by executing these files on their systems." *Id.* Then there are worms, which are self-replicating and "use computers they infect to seek out other computers to infect." *Id*. Finally, there are bots, which have been identified as one of the biggest threats to Internet stability because they create a "virtual army" that "remotely control[s] these botnets…with Internet commands." *Id*

[3] *Supra* note 1.

[4] *Id.*

[5] Ralf Benzmuller, *G Data Malware Report January – June 2015* (Oct. 20, 2015), https://blog.gdatasoftware.com/blog/article/g-data-malware-report-january-june-2015.html.

[6] Michael J. Schwartz, *Juniper Devices are Under Attack*, BANK INFO SECURITY (Dec. 8, 2015), http://www.bankinfosecurity.com/juniper-devices-are-under-attack-a-8768?rf=2015-12-28-eb&mkt_tok=3RkMMJWWfF9wsRonu6%2FAce%2FhmjTEU5z16O4tXaWwi4kz2EFye%2BLIHETpodcMTcJnN7DYDBceEJhqyQJxPr3FKdENwM10RhPhDw%3D%3D.

[7] *Id.*

[8] "Backdoors" will be defined *infra* Part I.

[9] Richard Winton, *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*, L.A. TIMES (Feb. 18, 2016), http://www.latimes.com/local/lanow/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

[10] *Id.*

[11] John Seabrook, *Network Insecurity*, THE NEW YORKER (May 20, 2013), http://www.newyorker.com/magazine/2013/05/20/network-insecurity.

[12] *See Infra* Part II

[13] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-361, IT SUPPLY CHAIN: NATIONAL SECURITY RELATED AGENCIES NEED TO BETTER ADDRESS RISKS (March 2012), *available at* http://www.gao.gov/assets/590/589568.pdf.

[14] *Id.*

[15] *Id.*

[16] Definition of hardware, TECHTERMS, http://techterms.com/definition/hardware (last visited Dec. 3, 2015).

[17] David Inserra and Steven P. Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, THE HERITAGE FOUNDATION BACKGROUNDER at 2 (Mar. 16, 2014), http://thf_media.s3.amazonaws.com/2014/pdf/BG2880.pdf.

[18] *Id.*

[19] Definition of firmware, TECHTERMS, http://techterms.com/definition/firmware (last visited Dec. 3, 2015).

[20] Definition of embedded system, WEBOPEDIA, http://www.webopedia.com/TERM/E/embedded_system.html (last visited Jan. 14, 2016). Microprocessors control the logic of almost all digital devices. *Id.* ROM stands for read-only memory and once data has been written onto a ROM chip, it cannot be removed. *Id*.

[21] *Id.*

[22]Paul Kocher, et al., *Security as a New Dimension in Embedded System Design*, *available at* http://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/SecurityEmbeddedSystemsDAC.pdf.

[23] John Villasenor, *Ensuring Hardware Cybersecurity*, BROOKINGS INSTITUTE (May 2011), http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Michael Ian Morrison, *The Acquisition Supply Chain and the Security of Government Information Technology Purchases*, 42 PUB. CONT. L.J. 749, 759 (2013).

[32] Taylor Wilkerson, *Cybersecurity in the Supply Chain*, UNITED STATES CYBERSECURITY MAGAZINE at 15, *available at* http://www.lmi.org/(X(1)S(wqoaad45kmmmdwe0k15p2w3n))/CMSPages/getfile.aspx?nodeguid=adf22863-fca9-44ae-a93a-c20e21bae1e6&AspxAutoDetectCookieSupport=1.

[33] Scott Charney and Eric T. Werner, *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*, SCADAHACKER.COM (Jul. 26, 2011), https://scadahacker.com/library/Documents/Threat_Intelligence/Microsoft%20-%20Cyber%20Supply%20Chain%20Risk%20Management%20(White%20Paper).pdf.

[34] *Supra* note 31 at 3.

[35] *Id*.

[36] *Supra* note 32.

[37] *Id*.

[38] *Id*.

[39] Scott Borg, *Securing the Supply Chain for Electronic Equipment: A Strategy and Framework*, THE INTERNET SECURITY ALLIANCE, https://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf.

[40] *Id.*

[41] *Supra* note 23.

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Back door creation has been at the forefront in the news with the recent court order requiring Apple, Inc. to essentially create a back door for the FBI to access the phone of one of the San Bernardino terrorists from the attack in December 2015. While the debate between the tech world and the U.S. government has many different facets, including consumer privacy and national security, the idea of creating a back door within Apple's software is alarming. Once a back door is created, the encryption can be defeated by anyone, leaving the country's data open for exploitation. *See* Apple CEO Tim Cook, A Message to our Customers (Feb. 16, 2016), *available at* http://www.apple.com/customer-letter/.

[49] *Supra* note 13.

[50] *Hardware attacks, backdoors and electronic component qualification*, INFOSEC INSTITUTE (Oct. 11, 2013), http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/.

[51] *Id.*

[52] *Id.*

[53] *Id*. A second type of backdoor includes "cheat codes," which "is secret data that the attacker uses to identify themselves to hardware backdoor logic," allowing an attacker to program triggers based on "specific input data" by initiating a malicious operation mode. *Id.*

[54] *Supra* note 13.

> A component is not genuine if it (1) is an unauthorized copy; (2) does not conform to the design, model, or performance standards as prescribed by the original component manufacturer; (3) is not produced by the original component manufacturer or is produced by an unauthorized contractor; (4) is an off-specification, defective, or used original component manufacturer product sold as "new" or working; or (5) has incorrect or false markings or documentation. Although not necessarily the result of an IT supply chain attack, these
> incidents highlight the impact that such attacks could have on agency
> operations. *Id.*

[55] *Id.*

[56] *Supra* note 17.

[57] *Id.* at 3.

[58] *Id.* at 4.

[59] *Id.*

[60] *Id.*

[61] *Supra* note 13.

[62] *Id*. at 17.

[63] "A patch is a software update comprised code inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package." Definition of patch, TECHOPEDIA.COM, https://www.techopedia.com/definition/24537/patch (last visited Feb. 28, 2016).

[64] *Supra* note 13.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Lenovo CTO: We're Working to Wipe Superfish App Off of PCs*, DIGITS WALL ST. J. BLOG (Feb. 19, 2015, 3:07 PM), http://blogs.wsj.com/digits/2015/02/19/lenovo-cto-were-working-to-wipe-superfish-app-off-of-pcs/.

[79] Jose Pagliery, *Lenovo slipped 'Superfish' malware into laptops*, CNN MONEY (Feb. 19, 2015, 2:42 PM), http://money.cnn.com/2015/02/19/technology/security/lenovo-superfish/. Superfish is an "internet browser add-on that injects ads onto websites you visit." *Id.*

[80] Seth Rosenblatt, *Lenovo's Superfish security snafu blows up in its face*, CNET (Feb. 20, 2015, 5:00 AM), http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/.

[81] David Auerbach, *You Had One Job, Lenovo*, SLATE.COM (Feb. 20, 2015, 8:23 AM), http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html.

[82] *Id.*

[83] *Id.*

[84] Although this is not a typical cyberattack by an adversary, Lenovo's actions here are an example of how simple it can be to insert malware in the production stages.

[85] *Supra* note 80.

[86] *Id.*

[87] Dan Goodin, *This thumbdrive hacks computers. "BadUSB" exploit makes devices turn "evil,"* ARSTECHNICA (Jul. 31, 2014), http://arstechnica.com/security/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/.

[88] Roger A. Grimes, *The BadUSB exploit is deadly, but few may be hit*, INFOWORLD (Oct. 9, 2014), http://www.infoworld.com/article/2692408/data-security/badusb-is-deadly-but-hackers-wont-use-it.html.

[89] *Supra* note 87.

[90] *Supra* note 88.

[91] *Id.*

[92] *Id.*

[93] *Supra* note 87.

[94] *Supra* note 88. One way to prevent attacks would be for manufacturers to require signed firmware updates for USB controllers or to disable the ability to change the firmware once a device leaves the factory. Some vendors might already do this, but many don't. And even if more manufacturers start doing this, the millions of existing insecure USB thumb drives will linger on for years and users will have a hard time telling them apart. *See* Lucian Constantin, *Security researchers release 'uncatchable' tools that make USB drives malicious*, PCWORLD (Oct. 3,

2014). http://www.pcworld.com/article/2691632/tools-for-creating-malicious-usb-thumb-drives-released-by-security-researchers.html.

[95] *Cybercrime Costs Estimated $450 Billion a Year*, WALL ST. J. (Feb. 18, 2016), http://www.wsj.com/articles/cybercrime-costs-estimated-at-450-billion-a-year-1455830011.

[96] *Id.*

[97] Marcus Christian, *Corporate Perspectives on Cybersecurity: A Survey of Execs*, LAW360 (May 6, 2015).

[98] *Id.*

[99] The average insurance claim for a cyberattack is $673,767. The average legal defense cost is $434,354. The average cost of legal settlement is $880,839. *Supra* note 97.

[100] *Supra* note 97. While legislation has been passed that addresses information sharing, there are no private sector standards.

[101] *Id.*

[102] Samuel Rubenfeld, *Cybercrime Surging as Economic Crime Threat*, WALL ST. J. DATA SECURITY BLOG (Feb. 25, 2016, 12:01 AM), http://blogs.wsj.com/riskandcompliance/2016/02/25/cybercrime-surging-as-economic-crime-threat/.

[103] Respondents included a mixture of businesses with more than 1,000 employees, multinational organizations, publicly traded organizations, and heads of departments. Global Economic Crime Survey 2016, PwC Global, http://www.pwc.com/crimesurvey.

[104] *Supra* note 95.

[105] These two executive orders are discussed *infra*.

[106] *The Comprehensive National Cybersecurity Initiative*, WHITEHOUSE.GOV, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Dec. 3, 2015).

[107] *Supra* note 13 at 6.

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id*. at 7.

[113] U.S. Department of Homeland Security Cybersecurity Overview, DHS.GOV (last published Sept. 22, 2015), http://www.dhs.gov/cybersecurity-overview.

[114] *Id.*

[115] *Supra* note 1.

[116] *Id.*

[117] Organizational Chart of the U.S. Department of Homeland Security, DHS.GOV (Aug. 26, 2015), http://www.dhs.gov/organizational-chart.

[118] U.S. Department of Homeland Security Office of Cybersecurity and Communications, DHS.GOV (last published Oct. 27, 2015), http://www.dhs.gov/office-cybersecurity-and-communications.

[119] *Id.*

[120] Despite the Obama Administration's heavy reliance on DHS to be the lead department on cybersecurity initiatives, the DHS has largely failed this task. Not only have a number of cyber breaches slipped through DHS's control (i.e. the Office of Personnel Management breach in 2014), but after being audited by the Inspector General it has become evident that DHS does not practice what it preaches. A number of DHS systems have not been updated, and the DHS's own employees have been non-compliant of federal rules and policy for cybersecurity. DHS spends more than $700 million annually on cybersecurity measures, but it is unclear whether the tax dollars spent on this is worth it. *See* Senator Tom Coburn, M.D., *A Review of the Department of Homeland Security's Missions and Performance* (Jan. 2015), *available at* https://www.hdiac.org/islandora/object/hdiac%3A315180.

[121] 2015 Cyber Strategy, The Department of Defense, http://[2600:1009:b027:a017:6ab8:3c43:7f20:6851]:8181/http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf at 1.

[122] *Id.* at 4.

[123] *Id.* at 5.

[124] *Id.*

[125] Congress attempted to pass comprehensive cybersecurity legislation in 2012, but the legislation did not pass the Senate. This sparked President Obama's Cybersecurity executive order in 2013. See Jennifer Rizzo, *Cybersecurity bill fails in Senate*, CNN (Aug. 2, 2012 at 4:19 PM), http://www.cnn.com/2012/08/02/politics/cybersecurity-act/.

[126] Exec. Order No. 13,636, 78 F.R. 11739 (2013).

[127] *Supra* note 31 at 768.

[128] *Id.*

[129] *Id.* at 768-69 (quoting *supra* note 77).

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id*. at 769

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] Newsletter Update on the Cybersecurity Framework, NIST.GOV (July 1, 2015), http://www.nist.gov/cyberframework/cyberframework-newsletter-07012015.cfm.

[138] *Id*.

[139] *Cybersecurity Risk Management and Best Practices*, THE COMMUNICATIONS SECURITY, RELIABILITY AND INTEROPERABILITY COUNCIL IV FINAL REPORT (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[140] In accordance with the Framework, DHS launched the Critical Infrastructure Community C^3 Voluntary Program, which helps associate critical infrastructure owners and operators with resources that will assist in the adoption of the Framework and manage their cyber risks.[140] The Voluntary Program assists and guides stakeholders with understanding and implementing the Framework. It also serves as a point of contact and customer relationship manager to assist organizations, and encourages feedback from the stakeholder organizations about their use of the Program. The success of the Framework in conjunction with the Voluntary Program is proof of the need for legislative initiatives to solidify cyber risk management further. *See* U.S.

Department of Homeland Security Critical Infrastructure Cyber Community Voluntary Program, US-CERT (last visited Dec. 3, 2015), https://www.us-cert.gov/ccubedvp.

[141] *Best Practices in Cyber Supply Chain Risk Management,* NIST.GOV (last visited Dec. 3, 2015), http://www.nist.gov/itl/csd/upload/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

[142] NIST SPECIAL PUBL'N 800-161, SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2015), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[143] *Id.*

[144] *Id.*

[145] *Fact Sheet: National Strategy for Global Supply Chain Security*, WHITEHOUSE.GOV (Jan. 25, 2012), https://www.whitehouse.gov/the-press-office/2012/01/25/fact-sheet-national-strategy-global-supply-chain-security.

[146] *Id.*

[147] *National Strategy for Global Supply Chain Security,* DHS.GOV (last published Oct. 5, 2015), http://www.dhs.gov/national-strategy-global-supply-chain-security.

[148] *National Strategy for Global Supply Chain Security Implementation Update,* WHITEHOUSE.GOV (Jan. 2013), https://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

[149] Jackie Calmes*, Obama's Last Budget, and Last Budget Battle With Congress*, N.Y. TIMES (Feb. 9, 2016), http://www.nytimes.com/2016/02/10/us/politics/obama-budget-cybersecurity-congress.html?_r=2.

[150] *Id.* The 2017 fiscal year budget was introduced in February 2016 and will likely ensue a struggle to be approved by Congress.

[151] *Fact Sheet: Cybersecurity National Action Plan*, THE WHITEHOUSE OFFICE OF THE PRESS SECRETARY (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[152] *Id*. Though it is appreciated that the White House painstakingly provided each detail about the various aspects of the new Action Plan, there are a lot of parts to Plan. From the looks of this "Fact Sheet," the Administration appears to be creating more cybersecurity groups, increasing the amount of confusion as to which group is handling which problem. The delegation of authority within the cyber realm has been a common complaint of the private sector due to a lack of understanding as to which sub-agency works on each issue. This is yet another reason why it is important to establish clear governing standards.

[153] Aside from the five bills mentioned *infra*, there are several cybersecurity related bills recently introduced or in committee. See *Cybersecurity Legislation Watch*, ISACA CYBERSECURITY NEXUS (last visited Dec. 3, 2015), http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx.

[154] Michael Daniel, *What You Need to Know About President Obama's New steps on Cybersecurity*, WHITEHOUSE.GOV BLOG (Jan. 14, 2015, 6:02 PM), https://www.whitehouse.gov/blog/2015/01/14/what-you-need-know-about-president-obama-s-new-steps-cybersecurity.

[155] *In a Surprising Move, Congress Passes Four Cybersecurity Bills*, HUNTON & WILLIAMS PRIVACY & INFORMATION SECURITY LAW BLOG (Dec. 12, 2014), https://www.huntonprivacyblog.com/2014/12/12/surprising-move-congress-passes-four-cybersecurity-bills/.

[156] Stacy Banks, *The Federal Information Security Modernization Act of 2014*, TENABLE NETWORK SECURITY (Jan. 16, 2015), https://www.tenable.com/blog/the-federal-information-security-modernization-act-of-2014.

[157] National Cybersecurity Protection Advancement Act, H.R. 1731, 114th Cong. (2015), *See also* Summary: H.R. 1731 – 114th Congress (2015-2016) National Cybersecurity Protection Advancement Act of 2015, CONGRESS.GOV (last visited Dec. 3, 2015), https://www.congress.gov/bill/114th-congress/house-bill/1731?q=%7b%22search%22:%5b%22cybersecurity%22%5d%7d.

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] *Id.*

[162] Consolidated and Further Continuing Appropriation Act, H.R. 83, 113th Cong. § 515 (2014).

[163] *Id.*

[164] *Id.*

[165] National Defense Authorization Act for Fiscal Year 2011, H.R. 6523, 111th Cong. (2011).

[166]

> Covered procurement means – (A) a source selection for a covered system or a covered item of supply involving either a performance specification...or an evaluation factor…relating to supply chain risk; (B) the consideration of proposal for and issuance of a task or delivery order for a covered system or a covered item of supply…where the task or delivery order contract concerned includes a contract clause establishing a requirement relating to supply chain risk; or (C) any contract action involving a contract for a covered system or a covered item of supply where such contract incudes a clause establishing requirements relating to supply chain risk. *Id.*

[167] *Id.*

[168] *Id.*

[169] *Id.*

[170] National Defense Authorization Act for Fiscal Year 2016, H.R. 1735, 114th Cong. (2015). *See also* National Defense Authorization Act for Fiscal year 2016, CONGRESS.GOV (last visited Dec. 3, 2015), https://www.congress.gov/bill/114th-congress/house-bill/1735.

[171] *Id.* The bill was vetoed primarily for not addressing the closing of Guantanamo Bay, which was an essential goal of President Obama's administration. President Obama, Veto Message – H.R. 1735, THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY (Oct. 22, 2015), https://www.whitehouse.gov/the-press-office/2015/10/22/veto-message-hr-1735.

[172] Orin Kerr, *How does the Cybersecurity Act of 2015 change the Internet surveillance laws?,* WASH. POST (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/.

[173] The term "cyber threat indicator" means,

> (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
> (B) a method of defeating a security control or exploitation of a security vulnerability;
> (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
> (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
> (E) malicious cyber command and control;
> (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
> (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
> (H) any combination thereof.

See Cybersecurity Act of 2015, Title I, Sec. 102. Definitions.

[174] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015), *available at* http://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf.

[175] *Id.*

[176] *Supra* note 23.

[177] *Id.*

[178] The Open Group, HTTP://WWW.OPENGROUP.ORG/ABOUTUS (last visited Jan. 14, 2016).

[179] *Id.*

[180] *Id.*

[181] The Open Group, HTTP://WWW.OPENGROUP.ORG/CERTIFICATIONS (last visited Jan. 14, 2016).

[182] IT Risk Management Survey Summary, The Open Group, 4 (Apr. 2015).

[183] *Id.* at 5.

[184] *Id.* at 13.

[185] *Id*. at 14.

[186] *Id.* at 17.

[187] *Cyber Attack Survival Checklist*, Crowdstrike, 13, http://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperCyberAttackSurvival.pdf.

[188] *Id.* at 14.

[189] Crowdstrike, Inc., WWW.CROWDSTRIKE.COM (last visited Jan. 14, 2016).

[190] *Id.*

[191] *Id.*

[192] *Supra* note 187.

[193] *Id.* at 2.

[194] *Id*.

[195] *Crowdstrike Global Threat Intel Report*, Crowdstrike (2014), http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf.

[196] *Id.* at 73.

[197] *Id.*

[198] *Id.*

[199] Natalia Drozdiak, *EU Agrees to Rules for Internet Firms Providing Essential Services*, WALL ST. J. DELOITTE BLOG (Dec. 8, 2015, 9:26 AM), http://blogs.wsj.com/brussels/2015/12/08/eu-agrees-rules-for-internet-firms-providing-essential-services/.

[200] Samuel Rubenfeld, *The Morning Risk Report: Europe Standardizes Cyber Rules*, WALL ST. J. BLOG (Dec. 10, 2015, 7:19 AM), http://blogs.wsj.com/riskandcompliance/2015/12/10/the-morning-risk-report-europe-standardizes-cyber-rules/.

[201] *Supra* note 199.

[202] These essential services include: energy, transportation, banking, and health, or digital ones, such as search engines and cloud computing. *See* First-ever EU-wide cyber-security rules backed by Internal Market Committee, European Parliament News (Jan. 14, 2016), http://www.europarl.europa.eu/news/en/news-room/20160114IPR09801/First-ever-EU-wide-cyber-security-rules-backed-by-Internal-Market-Committee.

[203] *Supra* note 199.

[204] *Id.*

[205] *Supra* note 200.

[206] *Id.*

[207] *Supra* note 199.

[208] *Id.*

[209] *Supra* note 1.

[210] 2015 Cyber Claims Study, NETDILLIGENCE.

[211] The U.S. Customs and Border Protection, CPB.GOV, http://www.cbp.gov/about (last visited Apr. 25, 2016).

[212] *C-TPAT Alert – Cybersecurity – How to Effectively Secure a Supply Chain and Partner Ecosystem*, (Jan. 2015), *available at* https://www.cbp.gov/sites/default/files/documents/C-TPAT%20Alert%20-%20Cyber%20Security%20-%20How%20to%20Effectively%20Secure%20a%20Supply%20Chain%20and%20Parter%20Ecosystem.pdf.

[213] *Supra* note 211.

[214] *Id.*

[215] *Id.*

[216] C-TPAT: Customs Trade Partnership Against Terrorism, CBP.GOV, http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism (last visited Apr. 25, 2016).

[217] *Id.*

[218] *Supra* note 212.

[219] *Id.*

[220] *Id.*

[221] *Id.*

[222] Chart of C-TPAT Achievements, CBP.GOV, http://www.cbp.gov/sites/default/files/documents/12-1-14%20C-TPAT%20Achievements.pdf (last visited Apr. 25, 2016).

[223] *Id.*

[224] *Supra* note 212.

[225] Grant Gross, *Report: Apple agrees to Chinese security audits of its products*, ITWORLD (Jan. 22, 2015), http://www.itworld.com/article/2874235/report-apple-agrees-to-chinese-security-audits-of-its-products.html.

[226] *Id.*

[227] *Id.*