Incentives to Encourage Adoption of the NIST Cybersecurity Framework

Preston C. Stinson

Mississippi State University

Washington Internships for Students of Engineering 2014

July 31, 2014

Contents

Executive Summary

Cyber-attacks against the nation's critical infrastructure represent one of the greatest threats to the nation's security, economic security, and public health. The Administration released Executive Order 13636 to begin addressing the issue of critical infrastructure cybersecurity. As part of the of the Executive order the National Institute for Standards and Technology produced the Framework for Improving Critical Infrastructure Cybersecurity (the Framework). Also, in accordance with the Executive order, the Department of Homeland Security, Department of the Treasury, and Department of Commerce each produced sets of incentives to encourage critical infrastructure organizations to adopt the Framework.The incentives are: cybersecurity insurance, clarification of liability, federal grants, tax incentives, improved information sharing, federal sponsored technical assistance, federal procurement, regulatory streamlining, and public recognition programs.

Cybersecurity insurance is insurance covering damages from a cyber-attack. An incentive involving cybersecurity insurance would involve direct government involvement with the cybersecurity market. However, the market is currently underdeveloped. Therefore, it is currently difficult to determine if government involvement in the market is necessary. Given the uncertainty associated with cybersecurity insurance it is recommended that government involvement be postponed until the market has matured.

Critical infrastructure organizations and other organizations in the supply chain are unsure about who is liable for damages resulting from a cyber-attack. This uncertainty is hampering the cybersecurity market. An incentive could take the form of liability protections for Framework adopters. It is recommended that Congress produce legislation addressing liability.

Federal grants could act as an incentive including Framework adoption as a proposal requirement. This incentive is recommended since it consists primarily of administrative changes.

Tax incentives for Framework adoption involve numerous difficulties facing them. The primary issues are scalability and cost. Tax incentives are difficult to scale given the varying sizes of critical infrastructure organizations. They are also one of the most expensive incentive options. Given these issues, it is not recommended that tax incentives be pursued.

Information is one of the primary tools used when defending against cyber-attacks. However, current information sharing schemes are fractured and lack definitive government backing. A centralized cross-sector information sharing scheme offered to Framework adopters could be leveraged as an incentive. It is recommended that an information sharing scheme be produced via a public-private partnership headed by the Department of Homeland Security and the private sector.

Technical assistance for critical infrastructure organizations attempting to adopt the Framework is another incentive option. Technical assistance is already offered to critical infrastructure organizations during cyber-attacks. Therefore, this incentive should not be excessively difficult to implement. It is recommended that the Department of Homeland Security be tasked with implementing such a program.

Federal procurement procedures could be modified to offer preferential treatment to

organizations that have adopted the Framework or produce Framework compliant products. However, the efficacy of this incentive is difficult to determine due to a lack of research. Therefore, it is recommended that more research be performed prior deciding to implement modifications to procurement procedures.

Regulatory streamlining could take the form of expedited security clearances for individuals employed by Framework adopters. However, there are issues facing expedited security clearances. It is therefore recommended that other forms of regulatory streamlining be researched as incentive options.

A public recognition program for Framework adopters is another incentive option. The efficacy of such programs is uncertain and may cause attackers to target organizations that failed to be recognized. If the benefits of such a program are much greater than the disadvantages then it may be advisable to institute a public recognition program. Therefore, it is recommended that further research into the efficacy of public recognition programs be performed.

Regardless of the aforementioned incentives, other actions will need to be taken by all levels of government and the private sector in order to fully address the issue of critical infrastructure cybersecurity. Action must be taken in order to secure the future of the United States.

Preface

About the Author

Preston Stinson in an undergraduate student at Mississippi State University studying electrical engineering. He intends to pursue a master's degree in electrical engineering, and his area of interest is microprocessor design. Preston is the president of his school's IEEE chapter, treasurer of his school's IEEE Eta Kappa Nu chapter, and recording secretary of his school's Tau Beta Pi chapter. Outside of school, Preston enjoys reading and programming.

About The WISE Program

The Washington Internships for Students of Engineering (WISE) program is a nine week internship for upperclassmen undergraduate students and graduate students enrolled in engineering programs across the country. The program takes place in Washington, D.C. and serves to educate engineering students interested in public policy on the intersection of engineering and public policy. As part of the program, the students attend meetings with various governmental and non-governmental agencies in order to further their understanding of the interactions between engineering and public policy. During the program the students also research a public policy issue related to their fields of study and produce a research paper and presentation detailing their findings. More information about the WISE program can be found at http://wise-intern.org.

Acknowledgments

I would like to thank the Institute of Electrical and Electronics Engineers (IEEE) for sponsoring my enrollment in the WISE program. Thank you to the 2014 WISE Steering Committee for making this program possible. I would like to thank the WISE 2014 faculty-member-in-residence, Dr. Kenneth Lutz, for all of the time and effort in providing an insightful and engaging program. His assistance was crucial in the research paper. My mentor, Dr. Eric Burger, provided excellent guidance and support. John Buydos provided necessary assistance in navigating the Library of Congress' collections. The IEEE-USA office team provided a wonderful, supportive work environment. My fellow WISE 2014 interns also provided support and assistance. Finally, I would like to thank everyone we met with during the program for their insight into the world of public policy.

1 Introduction

Cyber-attacks against the nation's critical infrastructure represent one of the greatest threats to the nation's security, economic security, and public health. On February 12, 2013 the White House released an Executive Order in response to the increasing threat of cyber-attacks against the nation's critical infrastructure. In this Executive Order, critical infrastructure is defined as systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters [1]. In the Policy Directive, sixteen critical infrastructure sectors are defined. The sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial bases; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems [3]. Given the scope of these sectors it is easy to see why their continued functionality is an issue of national importance.

In today's era of technology, systems are becoming more complex and interconnected. A new area of security has arisen which is called cybersecurity. In the same way that individual computer users have to be aware of and mitigate cybersecurity issues that can affect them, such as viruses and malware, organizations from small business corporations to the Federal Government have to develop strategies to deal with their cybersecurity issues. For critical infrastructure owners and operators cybersecurity is becoming increasingly important, and the conventional wisdom is that cybersecurity will only grow in importance. However, critical infrastructure organizations have generally been weak in the area of cybersecurity, and owners have been reluctant to invest in improving cybersecurity as a result of a number of issues that will be discussed later in this paper. The lack of adequate cybersecurity in critical infrastructure has become a more prevalent issue in the political sphere because critical infrastructure affects everyone in the United States, and the effects of a successful cyber-attack on critical infrastructure could range from relatively minor to a national incident.

During April and June of 2009 a security guard at the Carrell Clinic in Dallas, Texas, who went by the online alias GhostExodus, gained access to the hospital's HVAC system along with other systems with the intent to commit malicious acts on July 4, 2009. Thankfully GhostExodus illicit activities were brought to the attention of a cybersecurity researcher at Mississippi State University who determined GhostExodus identity and reported him to the Federal Bureau of Investigation [13]. Fortunately in this case the cyber-attacks that were committed were simplistic and the attacker poorly concealed his identity. Unfortunately, despite the simplicity of the attack GhostExodus still gained access to the hospitals HVAC system. As such, it is easy to see how a more competent attacker could produce large scale damages.

There has not yet been a large scale cyber-attack against critical infrastructure in the United States. However, the ability of malicious actors has continued to increase while critical infrastructure cybersecurity has failed to keep pace. Given the current state of affairs, a large scale cyber-attack against critical infrastructure is increasingly likely. As such, it is imperative the Federal Government take action to assist critical infrastructure owners and operators in shoring up cybersecurity practices in order to prevent future cyber-attacks that may cause irreversible damage to the nation's security, economic stability, or the health and wellbeing of the public. Congress has consistently attempted to produce comprehensive cybersecurity legislation in the past decade but due to the lack of a galvanizing crisis it is unlikely that legislation will be passed anytime in the near future [2].

The Executive Order and the Policy Directive are two recent attempts by the White House to help rectify the issue of critical infrastructure cybersecurity. In accordance with the Executive Order, the National Institute of Standards and Technology published the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014. The Framework is a voluntary system designed using existing standards, guidelines, and practices to assist critical infrastructure organizations in improving their cybersecurity posture [14]. Along with the creation of the Framework, the Executive Order also called for the Secretary of Homeland Security to establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure. In conjunction with the Program, Executive Order also required the Secretaries of Homeland Security, the Treasury, and Commerce to propose a set of incentives designed to promote participation in the Program [1].

This paper will analyze the incentives proposed by the Department of the Treasury, Department of Commerce, and Department of Homeland Security, and examine policy options for the implementation of each incentive. The goal of which is to encourage critical infrastructure owners and operators to adopt the Framework.

2 Background & Key Conflicts

The issue of cybersecurity is inextricably linked to the rise of networked communication systems and personal computing. However, not all of the aspects of cybersecurity are wholly modern. Cryptography, which is one of the primary methods of securing data, originated around 1900 BCE [15]. Other aspects of cybersecurity, such as intrusion prevention and user clearance levels, are analogous to physical security measures and can be historically traced back even further than 1900 BCE. The Computer Fraud and Abuse Act, the first piece of federal legislation addressing cybersecurity issues, was enacted in 1986 [12]. However, federal legislation has not kept pace with changes in the cybersecurity landscape. A report published by the Congressional Research Service in October of 2013 stated that no comprehensive cybersecurity legislation has been enacted since 2002 [18]. Comprehensive cybersecurity legislation is difficult to develop since the cybersecurity landscape is in a constant state of flux [4]. A more adaptive approach to legislation that allows individual critical infrastructure owners and operators to determine what cybersecurity practices are needed to meet government sanctioned cybersecurity standards is required [4, 6]. Cybersecurity legislation must also ensure that data containing private information regarding customers and employees is protected while still maintaining privacy and civil liberties. One of the ways of overcoming some of the legislative issues associated with cybersecurity is to empower regulatory agencies with the ability of oversight regarding cybersecurity issues in the critical infrastructure sectors. Many regulatory agencies are well-positioned to assume responsibility for cybersecurity oversight because they have experience developing regulations for the different critical infrastructure sectors. In addition, these agencies have already developed relationships with critical infrastructure stakeholders through their already established regulatory responsibilities [4]. Furthermore, some regulatory agencies have already enacted cybersecurity regulations in accordance with legislative mandate, such as the Federal Energy Regulatory Commission in the energy sector, the Nuclear Regulatory Commission in the nuclear sector, and the Federal Trade Commission in the financial sector. However, established efforts by regulatory agencies are not coordinated, resulting in a fractured cybersecurity landscape [19]. The Executive Order is attempting to rectify this issue by centralizing critical infrastructure cybersecurity efforts in the White House and DHS and using the Framework as a guideline to cybersecurity in order to assist in coordinating efforts by the different regulatory agencies. However, there are limits to the power of an executive order and as such, legislation will still be required to initiate many of the changes that will be required to improve the cybersecurity stance of US critical infrastructure [16].

A reasonable argument against government intervention in critical infrastructure cybersecurity is to say that the free market will force critical infrastructure owners and operators to adopt necessary cybersecurity practices to ensure their competitiveness in the marketplace. The idea of the free market dictating cybersecurity measures has been the underlying logic guiding previous legislation regarding critical infrastructure cybersecurity. A number of interrelated issues have resulted in a market failure in critical infrastructure cybersecurity market [10]. The economics of cybersecurity is the main feature causing this issue. Many researchers have modeled the relationship between malicious actors and critical infrastructure organizations using economic principles of supply and demand. The models show that as the overall investment in cybersecurity increases the number of cyber-attacks decreases. This relationship exists because increased investments in cybersecurity requires malicious actors to use increased resources to instigate a cyber-attack. The cost to defend against a cyber-attack is much greater than the cost to perform a cyber-attack, which results in underinvesting in cybersecurity [4, 6, 2, 19].

An important cybersecurity principle that assists in understanding this underinvestment is that the goal of most cyber-attacks is to exploit some vulnerability in a piece of software in a system in order to perform some form of illicit activity [5]. Therefore, the majority of defenses against cyber-attacks are implemented within software. However, developing secure software is time intensive, costly, requires a more specialized skill set than regular software development, and can be in conflict with other software features. These issues result in software developers ignoring security entirely or implementing bare bones security features [4, 2]. This creates strong disincentives at the supplier and consumer levels for engaging in cybersecurity practices. Further exacerbating this issue is that attackers are continuously becoming more effective at producing improved and novel attack methods. Therefore, investment in cybersecurity is a recurring cost [4]. There is also what economists refer to as a lemons problem in the cybersecurity marketplace. A lemons problem is a situation where a superior product costs more than an inferior product, but potential customers have no way of determining which product is superior due to a lack of information [6]. This problem occurs in the cybersecurity marketplace because procurement decisions are often based solely on costs.

One unique issue is that due to the interconnectedness of systems, cybersecurity for individual organizations does not exist in isolation. Suppose for example an organization, called *x*, maintains proper cybersecurity practices but is engaged in a business relationship with another organization, called *y*, that does not implement proper cybersecurity practices. Suppose organization *y* experiences a cyber-attack; then due to the established relationship between organizations *x* and *y*, organization *x* may also suffer as result of the attack on organization *y* [10]. This is a simplistic example of cybersecurity decisions made by one organization endangering other organizations. Due to the different sizes of critical infrastructure organizations, large organizations may be better situated to deal with cybersecurity issues, while intermediate and small organizations may not have the funds necessary to implement cybersecurity practices [4].

There are numerous other factors that have led to the current state of affairs for critical infrastructure cybersecurity. The connecting thread between all of the factors is that critical infrastructure stakeholders are generally underinvesting in cybersecurity. The primary purpose of the incentives proposed by the Treasury, Commerce, and DHS is to encourage critical infrastructure stakeholders to improve their cybersecurity posture. Therefore, the incentives must address the economic issues mentioned previously.

3 Incentives

In the DHS report, an incentive is defined as a cost or benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the Framework under development [9]. This document will utilize the same definition of incentive shall be used. Incentives shall be analyzed using available research to asses the prospective effects, advantages, disadvantages, and policy necessary to implement each incentive. In order to enable effective analysis the following assumptions will be made: first, the Framework is a scalable system that results in improved cybersecurity for organizations that adopt it; second, level of adoption of the Framework is quantifiable; third, the Framework will be updated on a regular basis to adapt to the changing cybersecurity landscape; forth, cybersecurity is equally important for all organizations, regardless of size; and finally, adoption of the Framework result in a market shift causing cybersecurity to become more cost effective and ubiquitous in the marketplace. With these assumptions in place the following incentives shall be analyzed: cybersecurity insurance, clarification of liability, federal grants, tax incentives, improved information sharing, federal sponsored technical assistance, federal procurement, regulatory streamlining, and public recognition programs.

3.1 Cybersecurity Insurance

Cybersecurity insurance is insurance acquired by an organization to cover damages that are the result of a cyber-attack. Cybersecurity insurance is similar to other business insurance policies because it is essentially the transfer of financial risk for damages to a third party in exchange for a premium [20]. However, the major difference between cybersecurity insurance and the majority of other insurance options is that cybersecurity insurance primarily deals with intangible assets and losses. DHS, the Treasury, and Commerce looked at cybersecurity insurance as a possible incentive for adopting the Framework because since insurers will charge lower insurance premiums for organizations with stronger cybersecurity [11, 2]. However, the primary issue associated with cybersecurity insurance is due to the immaturity of the market [10]. Due to this, research surrounding the effectiveness of cybersecurity insurance at improving cybersecurity is contradictory and lacks hard data [8]. Critical infrastructure organizations may avoid improving their cybersecurity stance and instead heavily invest in cybersecurity insurance. Furthermore, cybersecurity insurance insurers have not yet fully developed methods of dealing with the issue of information asymmetry. Information asymmetry is an economic situation that results from one organization having better information than another organization in a market. In cybersecurity insurance market, information asymmetry occurs when a policyholder has a better understanding of its cybersecurity stance than the insurer. However, insurers were able to overcome information asymmetry issues in other markets so it would be reasonable to assume that these issues will be addressed as the cybersecurity insurance market grows [20]. An issue that is unique to the cybersecurity insurance market is the threat of a single cybersecurity vulnerability causing massive damages across the entire cybersecurity insurance market, because of the homogeneity of the market [2, 20]. Despite the issues currently facing the cybersecurity insurance market, the general consensus is that the cybersecurity insurance market will continue to grow and will have an effect on the cybersecurity stance of critical infrastructure organizations [20, 17].

The major policy question currently faced in regards to cybersecurity insurance is if the government should be involved in the market and if so, how the government should be involved [17]. DHS, the Treasury, and Commerce looked at cybersecurity insurance as an incentive for adopting the Framework because insurers could use Framework adoption to determine eligibility for insurance or premiums. In the reports published by DHS, the Treasury, and Commerce, DHS and Commerce recommended further exploring government involvement in the cybersecurity insurance market while the Treasury recommended that the government avoid interfering in the market [7, 11, 9, 17]. One of the major advantages of cybersecurity insurance is that insurers should be motivated by changes in the cybersecurity landscape to ensure that eligibility requirements and premiums do not become obsolete [10]. There is fear that if cybersecurity insurance providers are mandated to use the Framework and if it becomes obsolete then insurance providers and policyholders would not be adequately protected. The cybersecurity insurance market is currently facing issues regarding how cybersecurity insurance fits in with the current legal framework [20]. The government could enact policy to assist cybersecurity insurance providers in overcoming these challenges in order to bolster the cybersecurity insurance market. Regardless of what policy action is taken in the near future it is almost certain the cybersecurity insurance market will continue to grow and become more ubiquitous.

3.2 Liability

In the incentive recommendations made by DHS, the Treasury, and Commerce all three departments analyzed clarification of legal liability as a method to encourage Framework adoption. The idea behind liability as an incentive for improving cybersecurity is that if critical infrastructure organizations are held accountable for damages incurred by other parties as a result of a cyber-attack against them then critical infrastructure organizations will improve their cybersecurity stance in order to avoid litigation against them [7, 11, 9, 2]. According to the Treasury liability could function as an incentive for adopting the Framework because

> implementing the Framework, - or at the very least, some of its practices could serve this purpose and provide the basis for greater legal certainty sought by many critical infrastructure stakeholders. A firm that does not meet these practices might be found negligent in failing to prevent a cyber incident or failing to take actions to limit the consequences arising from a cyber incident. A firm that meets or surpasses these recommendations, meanwhile, might not be held liable for damages arising from the incident [10].

The primary advantage of using liability as an incentive is that it directly encourages adoption of the Framework while still leaving cybersecurity implementation to individual critical infrastructure organizations. One disadvantage associated with liability is that if the protections granted by adopting the Framework are too broad then issues of moral hazard arise [10]. Moral hazard is a situation where a party takes unnecessary risks because it is insulated against damages that may result from those risks. An example of moral hazard is a situation where a person has insurance that covers all damage to his vehicle with no deductible. As a result of his insurance policy the person would have no financial incentive to avoid minor accidents. Opponents of liability assert that the threat of a liability suit could stifle technological innovation by critical infrastructure organizations and vendors [2]. Also, vendors may be unfairly targeted in litigations because of failures caused by improper installation, use, or maintenance of their products [19]. Another concern is that if liability for cyber-attacks is established, critical infrastructure organizations may be incentivized to avoid assessing their own cybersecurity stance in an attempt to mitigate their liability. Furthermore, the Framework was not developed with liability clarification as a primary concern. Therefore, development of legislation might be difficult. However, future versions of the Framework may be written with clarification of liability in mind or supplementary material may be developed to address this deficiency. Regardless of future modifications to the Framework, if clarification of liability for damages incurred as a result of a cyber-attack is to be implemented Congress will need to pass legislation addressing the issue. In summary, clarification of liability for damages resulting from cyber-attacks is a powerful incentive to adopt the Framework but its effectiveness is highly dependent upon the implementation method used.

3.3 Grants

There are two primary methods of using federal grants to incentivize Framework adoption. The first is developing new federal grant programs that fund cybersecurity research [11]. The second method consists of making Framework adoption a criterion for receiving federal grants [9, 10]. The primary benefit of the first method is that research can result in an overall improved cybersecurity landscape by developing new cybersecurity practices and systems. Also, the benefits of such research are not limited to only critical infrastructure organizations, but also to society at large. The primary benefit of the second method is that making Framework adoption a criterion for receiving federal grants will directly reward organizations that have adopted the Framework by giving them preferential treatment [7, 11, 9]. The second method would not require allocation of funds for new federal grants or reallocation of more funds to established grants, this would only entail modifying proposal evaluation procedures. The primary barrier facing the second method is that new statutory authority would be need to be allocated for federal agencies to utilize this incentive [9]. These two methods of implementing federal grants as an incentive for adopting the Framework are not mutually exclusive and implementing one or both of them should lead to increased Framework adoption and improve the cybersecurity stance of critical infrastructure.

3.4 Tax Incentives

DHS, the Treasury, and Commerce all analyzed tax incentives as an incentive to promote Framework adoption and all three organizations determined that tax incentives would be ineffective as an incentive [7, 11, 8]. The first problem facing tax incentives is that they are traditionally designed to favor a specific type of investment and thus could be seen as functionally analogous to government mandated adoption of a particular technology [10]. As previously discussed, mandating the use of a specific technology when dealing with cybersecurity issues is rarely effective and can result in overall reduced cybersecurity. Furthermore, overly large tax incentives could lead to market distortions that could reduce or eliminate use of an effective technology that is not included in the tax incentive [10]. The second problem facing tax incentives is that critical infrastructure organizations vary widely in form and scale. Developing tax incentives that are relevant to large critical infrastructure organizations could result in neglecting smaller critical infrastructure organizations or allocating too many public funds to smaller organizations. Also, some critical infrastructure organizations are non-profits or public utilities and as such do not pay taxes. Tax incentives may cover expenses that critical infrastructure organizations may have incurred regardless of the incentive [8]. The most important issue facing tax incentives is that they would require distributing public funds to private organizations, which makes implementing tax incentives incredibly difficult while also being perceived negatively by a majority of the public. Overall, tax incentives could be used to incentivize Framework adoption, but the challenges associated with implementing them outweigh their benefits.

3.5 Improved Information Sharing

One of the primary tools used by cybersecurity specialists is information about previous and current cyber-attacks. Information is valuable in the cybersecurity sphere because both attackers and defenders make use of the information. Attackers use the information available to them to determine what attack vectors work and do not work, what attacks are being implemented by other attackers, how defenders are reacting to attacks, and other valuable data. Defenders use knowledge gained from previous attacks to design better defense systems and use data about current attacks in order to know what attacks to be on the lookout for. Due to this use of information on both sides of cybersecurity, information has become a valuable commodity in the cybersecurity sphere. As such, improved information sharing has been shown to be an attractive incentive for critical infrastructure organizations to adopt the Framework [10]. There are currently organizations called Information Sharing and Analysis Centers that work in the different critical infrastructure sectors to promote real time sharing of information in order to secure critical infrastructure systems. However, ISACs are primarily focused on information sharing in the particular critical infrastructure sector covered by them and not necessarily critical infrastructure as a whole. The way information is shared between members of an ISAC is different for each ISAC and membership in an ISAC is not necessarily required of a critical infrastructure organization. Improved information sharing with the government would allow for more cross-sector information sharing and would thus improve the cybersecurity stance of critical infrastructure as a whole [11, 10]. However, critical infrastructure organizations have been hesitant to instigate information sharing with the government due to concerns of legal, regulatory, and other barriers to sharing information as well as privacy concerns associated with sharing information with the government [2, 10]. These concerns regarding information sharing could be leveraged to encourage Framework adoption by offering clarification and resolution for legal and regulatory concerns associated with information sharing to critical infrastructure organizations that adopt the Framework. According to the Treasury, the protocols for information sharing between Framework adopters should be crafted to avoid compromising privacy, civil rights, civil liberties, and U.S. national security, as well as to protect reputational and competition concerns of the firms sharing the information [10]. If the protocols address these issues and legal and regulatory issues are overcome then the vast majority of issues critical infrastructure organizations have voiced in regards to sharing information with the government would be alleviated. Also, if the Framework is used when developing an improved information sharing system then the language used in the Framework will become more standardized thus further improving on-going information sharing [17]. One of the problems facing an information sharing system is the fact that as the system grows and more data is shared it is more likely that data could be leaked to third parties which could in turn result in new or additional cyber-attacks. Stripping shared information of identifying elements would assist in avoiding this issue but would not be able to fully mitigate it [10]. Liability associated with shared information is also an issued faced when developing an information sharing system because critical infrastructure organizations may be concerned about shared information being used in litigation against them in the event of damages resulting from a cyber-attack [17]. Anonymizing information before submitting it or legislation clarifying liability for shared information could help alleviate this issue. Another issue facing an information sharing program is that members of the program may be tempted to only receive information in order to ensure the privacy of their own information while still gaining knowledge from information shared by other organizations. Critical infrastructure organizations are also not guaranteed to act upon information they receive [10]. Regardless of the specific implementation, an information sharing scheme will end up relying on Congress to pass legislation addressing the issues facing critical infrastructure organizations in regards to information sharing. The Administration will be required to help organize and maintain an information sharing system. Overall, improving information sharing is a viable incentive for inducing Framework adoption. The issues faced by critical infrastructure organizations in regards to information sharing with the government are the same issues faced by the majority of other private sector organizations and as such, development of an effective information sharing system could benefit the private sector as a whole if developed properly.

3.6 Technical Assistance

Government sponsored technical assistance was analyzed as an incentive for adopting the Framework by DHS, the Treasury, and Commerce [7, 11, 9]. There is already government sponsored technical assistance for critical infrastructure organizations suffering from a cyber-attack that request assistance through organizations such as DHSs Industrial Control Systems Cyber Emergency Response Team. However, the technical assistance proposed by DHS, the Treasury, and Commerce differs from established emergency response programs and should not be construed as an attempt to replace or abolish existing technical assistance programs [11, 9]. Technical assistance as proposed to support Framework adoption would not be focused on emergency response but would instead focus on assisting critical infrastructure organizations in adopting the Framework. According to the Treasury, Technical assistance should be thought of as a complement to not a substitute for other information sharing initiatives [10]. This type of technical assistance program would mostly assist smaller critical infrastructure organizations in implementing the Framework because larger organizations would most likely already have the resources required to implement the Framework by themselves [10, 8]. Issues of moral hazard arise from any government sponsored technical assistance program because critical infrastructure organizations may begin to rely on the government before exhausting all of their available cybersecurity resources. As well, establishing and maintaining a large technical assistance program could easily become expensive. However, the Treasury believes that the advantages of a well-designed technical assistance program could outweigh its drawbacks if moral hazard issues are able to be overcome [10].

3.7 Procurement

DHS and Commerce both analyzed adding language supporting the Framework to federal procurement procedures as an incentive option [7, 9]. According to DHS procurement incentives could take the form of introducing a technical requirement in the procurement process for certain types of acquisitions for Framework adopter, or requirements for Framework adoption for Federal information and communication technology providers or other contracts [9]. This type of incentive would directly reward organizations that adopt the Framework or produce products that are complicit with the Framework by giving Framework compliant organizations or products higher priority when evaluating proposals. A fringe benefit of procurement incentives is that organizations that deliver Framework compliant products to the government could also offer the same products to private sector customers [2]. Implementation of procurement incentives would be simpler than some of the other incentive options because the Federal Government has already established preferential procurement treatment for environmentally friendly organizations so adapting procurement processes to favor Framework adopters could be implemented in a similar fashion. Furthermore, modifying procurement evaluation factors would not require allocation of new funds. However, the efficacy of environmental procurement procedures is still undetermined; thus the efficacy of Framework procurement procedures is also undetermined [8]. Developing minimum levels of Framework adoption for procurement purposes may be difficult to establish due to the complex nature of cybersecurity [17]. Overall, modifications to procurement procedure have the potential to be an effective incentive but further research regarding its efficacy and implementation needs to be performed.

3.8 Regulatory Streamlining

The Executive Order explicitly called for DHS to expedite processing of security clearances for appropriate individuals employed by critical infrastructure organizations [1]. As such, DHS, the Treasury, and Commerce all analyzed expedited security clearance and other regulatory streamlining procedures for Framework adopters as incentives [7, 11, 9]. The primary advantage proposed as a result of expedited security clearance is increased ease of information sharing between Framework adopters and the government. The Treasury also recommended overall improvements to current security clearance procedure and improved educational opportunities for private sector organizations to learn about security clearance procedures [10]. These recommendations and opportunities would most likely be relevant for smaller critical infrastructure organizations since smaller organizations likely lack security offices or individuals with experience with security clearance procedures compared to larger organizations [17]. As well, expedited security clearance procedures should not produce undue costs since the majority of actions required to implement expedited procedures are administrative in nature [10]. However, Commerce believe that expediting security clearance procedures are unnecessary at the moment and DHS has already begun doing so in accordance with the Executive Order [**?**, 9]. Given the 2013 Washington Navy Yard shooting and information leaks by Edward Snowden expedited security clearance may not be received well by the public [17]. Other regulatory streamlining procedures such as a Fast-Track Patent Pilot for Framework adopters, elimination of overlaps among existing laws, reduced audit burdens, and other streamlining options were proposed but have not been thoroughly discussed as of yet [7, 9].

3.9 Public Recognition Program

Commerce proposed a public recognition program as a possible incentive [7]. The primary idea behind a public recognition program is to award companies that adopt the

Framework with certification showing their adherence to cybersecurity standards. Hopefully certification would provide a competitive advantage in the marketplace [2]. According to Commerce, public recognition programs have been effective when used to promote environmental policy [8]. Public recognition programs are not known for being cost prohibitive, and implementation could be modeled after environmental public recognition programs. However, there is concern that malicious actors will take public recognition as a challenge to target organizations recognized by the program or use it to determine which organizations are more likely to adhere to less stringent cybersecurity practices [7, 19]. Overall, a public recognition program may be an effective incentive option but research and discussion regarding the topic are currently scarce.

4 Recommendations and Future Actions

Critical infrastructure cybersecurity is of vital importance to the continued prosperity of the U.S. Lack of recognition and action may end up resulting in damages to the nation's economy, security, and public health. Previous policy has relied on market forces to cause critical infrastructure organizations to adopt effective cybersecurity practices. However, the market does not currently favor investments in cybersecurity and instead is skewed heavily in the favor of malicious actors. To address critical infrastructure cybersecurity, the Administration produced the Executive Order in order to begin laying the framework for future actions. As part of the Executive Order NIST produced the Framework, which is a set of guidelines critical infrastructure organizations are recommended to follow to enhance their cybersecurity practices. In conjunction with producing the Framework, DHS, the Treasury, and Commerce separately produced analyses on possible incentives the Federal Government could use to promote adoption of the Framework. The most attractive incentives are: clarification of liability for damages resulting from a cyber-attack, preferential treatment for Framework adopters when receiving federal grants, improved information sharing regarding cyber-threats between critical infrastructure organizations and the government, and government sponsored technical assistance to assist smaller critical infrastructure organizations in adopting the Framework. Modifications to federal procurement procedures to favor Framework adopters, regulatory streamlining, and public recognition programs may be effective incentives, but more research and discussion regarding each option needs to be performed before any concrete conclusions can be made. The majority of available literature predicts that as the cybersecurity insurance market grows it will lead to improved cybersecurity across the entire private sector. However, there is not any decisive evidence showing that direct government involvement in the market will result in improved cybersecurity or growth in the market. It is advisable for the Federal Government to avoid involvement in the cybersecurity insurance market, however the market should be observed to determine if future involvement would be beneficial. The majority of analysis indicates that tax incentives are too rigorous to be able to be implemented effectively to promote Framework adoption and are one of the most costly incentive options analyzed. Therefore, it is advisable that tax incentives not be pursued any further and resources should be directed towards other incentive options.

Given the available information the following actions are recommended: first, Congress should produce legislation addressing the issue of liability for damages resulting from a cyber-attack; second, federal grant procedures should be unilaterally modified to give preferential treatment to organizations that adopt the Framework; third, an information sharing scheme should be established via a public-private partnership headed by DHS and the private sector; and finally, DHS should establish a technical assistance program to assist critical infrastructure organizations in adopting the Framework.

Even if the aforementioned incentives are implemented, their effectiveness at improving critical infrastructure cybersecurity is dependent upon the efficacy of the Framework. Therefore, continued refinement of the Framework is required. Future versions of the Framework should attempt to link the Framework to established and future cybersecurity standards. The Framework should also be modified to help address issues of legal liability. Research also needs to be performed on how critical infrastructure organizations will adapt to changes in the Framework and government's role in assisting organizations in maintaining pace with the Framework. Finally, further action by the Federal Government beyond the scope what is contained in of the Executive Order will need to be pursued in order to improve the cybersecurity stance of the nation's critical infrastructure.

References

[1] Executive Order 13636. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf, Feb 2013. Accessed: 06-18-14.

[2] *At the Nexus of Cybersecurity and Public Policy : Some Basic Concepts and Issues*. National Academy of Sciences, http://www.nap.edu/catalog.php?record_id=18749, 2014. Accessed: 06-18-2014.

[3] Presidential Policy Directive - Critical Infrastructure Security and Resilience. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, Feb 2014. Accessed: 06-18-2014.

[4] J. M. Bauer and M. J. G. van Eeten. Cybersecurity: stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10-11):706–19, Nov-Dec 2009.

[5] Ian Brown, editor. *Research Handbook on Governance of the Internet*. Edward Elgar Publishing, Jun 2013.

[6] Joseph J. Cordes. An Overview of the Economics of Cybersecurity and Cybersecurity Policy. http://www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/2011-6_economics_and_cybersecurity_cordes.pdf, Jun 2011. Accessed: 06-18-2014.

[7] Department of Commerce. Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program. http:

//www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf, Aug 2013. Accessed: 06-18-2014.

[8] Department of Homeland Security. Analytic Report: Executive Order 13636 Cybersecurity Incentives Study. http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf, Jun 2013. Accessed: 06-20-2014.

[9] Department of Homeland Security. Summary Report: Executive Order 13636 Cybersecurity Incentives Study. http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-summary-report-cybersecurity-incentives-study_0.pdf, Jun 2013. Accessed: 06-18-2014.

[10] Department of the Treasury. Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636. http://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf, Aug 2013. Accessed: 06-19-2014.

[11] Department of the Treasury. Treasury Department Summary Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636. http://www.treasury.gov/press-center/Documents/Treasury%20Report%20%28Summary%29%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf, Aug 2013. Accessed: 06-18-2014.

[12] Electronic Frontier Foundation. Computer Fraud and Abuse Act. https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA), Apr 2013. Accessed: 07-02-2014.

[13] Robert McMillan. Security Guard Charged With Hacking Hospital Systems. http://www.pcworld.com/article/167756/article.html, Jul 2009. Accessed: 07-16-2014.

[14] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, Feb 2014. Accessed: 06-18-2014.

[15] Huzaifa Sidhpurwala. A Brief History of Cryptography. https://securityblog.redhat.com/2013/08/14/a-brief-history-of-cryptography/, Aug 2013. Accessed: 07-02-2014.

[16] Tim Starks and CQ Roll Call. Obama Unveils Cybersecurity Executive Order. http://public.cq.com/docs/news/news-000004219300.html, Feb 2013. Accessed: 06-23-2014.

[17] Joe Stuntz. An Analysis of US Government Proposed Cyber Incentives. http://s2erc.georgetown.edu/sites/s2erc/files/Analysis%20of%20Incentives_0.pdf, Feb 2014. Accessed: 06-20-2014.

[18] Rita Tehan. Cybersecurity: Authoritative Reports and Resources. Technical report, Congressional Research Service, http://fpc.state.gov/documents/organization/217486.pdf, Oct 2013. Accessed: 06-17-2014.

[19] The Brookings Institution. Cybersecurity: Incentives and Governance. http://www.brookings.edu/~/media/events/2011/7/21%20cybersecurity/20110721_cybersecurity, Jul 2011. Accessed: 06-27-2014.

[20] Costis Toregas and Nicolas Zahn. Insurance for Cyber Attacks: The Issue of Setting Premiums in Context. http:

//www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/cyberinsurance_paper_pdf.pdf, Jan 2014. Accessed: 06-20-2014.

Appendix

List of Abbreviations and Acronyms

Commerce - U.S. Department of Commerce

DHS - U.S. Department of Homeland Security

the Executive Order - Executive Order 13636

the Framework - Framework for Improving Critical Infrastructure

HVAC - Heating, Ventilation, and Air Condition

ISAC - Information Sharing and Analysis Center

NIST - National Institute of Standards and Technology

the Policy Directive - Presidential Policy Directive 21

the Program - Program to Encourage Framework Adoption

Treasury - U.S. Department of the Treasury