MEMORANDUM

From: MIDN 3/C KIM DO, UNITED STATES NAVY
      MIDN 3/C JOSEPH YATES, UNITED STATES NAVY

To: PRESIDENT BARACK OBAMA, COMMANDER-IN-CHIEF
      ASSISTANT SECRETARY DR. ANDY OZMENT, OFFICE OF CYBERSECURITY AND
      COMMUNICATIONS
      BRIGADIER GENERAL GREG TOUHILL, DEPUTING ASST. SECRETARY OFFICE OF CYBERSECURITY
      AND COMMUNICATIONS

Via: CHAIN-OF-COMMAND

Table of Contents:

   Introduction: 2-4
   Past Precedence’s: 4-6
   Basic Budget: 10-11
   Results: 11-13
   Implementation: 13-14
   Incentives: 14-15
   Conclusion: 15
Introduction

In essence, cyber law is an endeavor to amalgamate the challenges presented by the exploitation of internet capable devices with the system of laws applicable to the physical world. The growth of electronic commerce has propelled the need for vivacious and effective regulatory mechanisms to further strengthen the infrastructure inclusive from the national level to the consumer level. This is crucial to the prosperity of electronic commerce as well as defense against future cyber threats. All these regulatory mechanisms and legal infrastructures come within the domain of cyber law. This paper intends to offset the drastic and immensely growing problem of cybercrimes by proposing universal essentials and statures and underscore their preclusions.

The present day sphere of concern within the cyber domain correlates to the ontogenesis of embedded systems invoked as the otherwise referred to as the 'Internet of things' (Iot). Iot is used to describe embedded devices with Internet connectivity granting interaction with other devices, services, and people often on a wide spread scale. This level of connectivity can augment reliability, sustainability, and efficiency by improved access and transfer of information. Due to the burgeoning amount of applications the IoT has provided, there is a common concern that the IoT will replace humans as the largest consumer and producer of information on the Internet. IPv6 over low-powered wireless area networks commonly known as (6LoWPAN) drives these wireless devices and allows the devices to emulate an Internet connected device. With these new IoT advancements, the interconnection of unique embedded devices has eminently become a playground for cyber criminals who seek to take advantage of the consumers who utilize the devices. Specifically, the general masses of consumers who purchase these devices for personal usage. In

2 Ibid
2020, it is estimated for every one person in the world, there will be over 50.1 billion devices.\(^3\)

Despite the convenience for the mass population, IoT provides a new dimension of threat into the cyber realm. With consumers using products that are not securely manufactured with the ample amount of penetration testing, security modes, and additionally safe usage training, the consumers, government and corporates will be at the mercy of crime groups. Criminals seek to exploit these devices through reprehensible means in order to fulfill their economic motives, for example hacking a device and then blackmailing consumers to input their credit card information into an embedded device before relinquishing the device back to the consumer.

The proposed policy to alleviate the detrimental repercussions of these crime ware groups who seek to undermine the fidelity of the relationship between technology and humans in essence is stratified into three parts. The three components are prevention of these offenses, education to the public concerning the dangers of IoT and lastly the response to cyber threats component. These three components combined into a policy referred to as CAPR (Cyber Attacks Prevention and Response). CAPR is intended to embody a “living document,” namely that it can be updated and revised as industry induces such changes on implementation. As the policy is put into practice, lessons learned will be integrated into future versions, ensuring that it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats and menaces. The CAPR policy aims at optimizing and accelerating the recently implemented policies such as the National Cybersecurity and Critical Infrastructure Protection Act of 2014 and the current National Institute of Technology NIST framework. The CAPR policy is not intended to create any new agencies or organizations, rather its purpose is to enhance cyber security for the nation with a focus on leveraging a strong coordination between the government and the private sector to employ prevention, response and

education concerning cybercrimes. The policy is a catalyst that will perpetuate
the recently instilled framework to ensure cyber security within the United
States.

On September 30 of 2014, former National Security Agency Director Keith
Alexander called for more information sharing between companies and government
agencies concerning cyber vulnerabilities, and emboldened legislation that would
incentivize distribution of information by providing liability protection in
exchange for jointly established cybersecurity standards. Alexander asserts that
"we need real-time or near real-time situational awareness, and we have got to
have cyber legislation that allows us to go between industry and government to do
that"\(^4\). The only way to procure a chance to combat the ubiquitous threat from
crime ware groups is to ensure that the United States of America begins to take
the steps in a robust manner.

**Past Precedence**

In 2012, a proposed bill known as the ‘Cybersecurity Act of 2012’ (CSA2012)
was killed in a 52-46 vote on the Senate floor. The act would have incorporated
cyber security standards and grant legal immunity to corporations who would meet
the standards\(^5\). The bill failed due to the concern of infringement upon the
constituents’ personal privacy as shown in the American Civil Liberty Union’s
strong opposition to the bill. In conclusion, the House weighed that the risks of
the implementation of the bill outweighed the benefits is proposed. \(^6\)

In 2013, President Obama issued Executive Order 13636: *Improving Critical
Infrastructure Cybersecurity* which called for the development of a voluntary
Cybersecurity Framework inclusive of a new guidelines, standards and practices to
manage the imminent cyber threats and it specifically targeted the promotion of


information sharing between the government and companies\(^7\). However, the framework ultimately received negative feedback because its main contributors of knowledge were industry experts who were professionals in cybersecurity. As a result, bias existed for companies more often than not. The interests of the companies and shareholders were held in higher priority than in standardizing security. However, the framework did raise awareness amongst higher corporate seats such as CEO’s to remain more vigilant concerning the changing cyber domain and the threats it posed.

Finally, two years later in June of 2014, the House passed the National Cybersecurity and Critical Infrastructure Protection Act of 2014, establishing the Department of Homeland Security’s Cybersecurity and Communications Integration Center (NCCIC).\(^8\) The NCCIC and its four groups function as the federal civilian information sharing interface to provide “cyber situational awareness, incident response, and a management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement”\(^9\). Under the bill, federal agencies would be required to notify the NCCIC of data breaches involving personally identifiable information within a timely manner. It also would require the Department of Homeland secretary to establish "cyber incident response teams" to provide technical assistance and recommendations to federal, state, and local government entities, private entities, and critical infrastructure owners. However, the scope of this new bill is constrained\(^10\). The act provides services preferable to the federal government and their agencies. As it stands, the act lacks the capability to establish permanent public-private alliances to jointly combat cyber threats such as those posed by the IoT crime ware groups which target consumer products manufactured by private corporations. Additionally, the new act lacks the incentivize course of actions to


properly integrate the government and private industry. And lastly, the current framework does not provide a means to vivaciously standardize a minimum secure mode for consumer products. A previous successful electronic protection acts such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which included provisions that required Department of Health and Human Services to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that “advances in electronic technology could erode the privacy of health information”\textsuperscript{11}. As a result Congress incorporated into HIPAA provisions the adoption of Federal privacy protections for individually identifiable health information. In 2003, HHS published a final security rule. The rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005.\textsuperscript{12}

The CAPR policy will embody Former NSA Director Alexander’s vision in that it will mandate the cooperation between private sector and the federal government to output a permanent situational cooperation. The policy will delineate the logistics needed to execute a messaging framework that shares information among entities. Additionally, the CAPR policy will allow for a check and balance system between the stakeholders by tasking the Office of Cybersecurity and Communications under the Department of Homeland Security to be the middle-man to regulate the cooperating between civilian sector and the government. All entities have rights to hold the others accountable unceasingly and additionally the policy safeguards their rights from being infringed by another entity. Lastly, the CAPR policy will facilitate the standardization of a consumer product security minimum.

**Consideration of Stakeholders**


\textsuperscript{12} Ibid
The five domains of that the CAPR policy integrates includes the federal government, private corporations developing consumer products, civil liberty groups, the consumers and the Office of Cybersecurity and Communications. The dominant component of the CAPR policy is the Office of Cybersecurity Communications (CS&C) branch under the Department of Homeland Security. Assistant Secretary Dr. Andy Ozment leads the office while Brigadier General Greg Touhill serves as the Deputy Assistant Secretary for Cybersecurity Operations and Programs.

Additionally, the policy holds the CS&C to be the main adhesion between the federal government and corporations. The office will also be tasked with responding to the threats posed by civil liberty groups when it concerns constitutionals rights. The federal government will be expected to provide a robust authority and the incentives as well as legislations to ensure the CAPR policy is implemented in an efficient manner, specifically in supporting the education of the public as well as incentivizing and supporting corporations and ensuring the foreign community does not interfere with the United States while they increase cyber security on a wide scale. In the modern day United States, whenever the cyber domain comes into play, the question of infringement of civil liberties is instantly attaché as a result of some of the methods to resolve cyber threats. In the world of cyber, real time response is essential to combat malware and threats. However when a cyber team is trying patch and overcome vulnerabilities in an expedient manner but fail to do so because fear of violation civil liberties come into play, the final consequence is deadly to an entire nation. Additionally, the corporations are expected to invest time and money into their products and ensure they are placing the interest of their consumers through the coordination with the CS&C. The consumers are expected to ensure that corporations inform them of security risks of using certain products and to report any violations or egregious actions. Additionally, consumers are expected to be willing to learn and understand the cyber risks that IoT presents and perhaps sign waivers or agreements to ensure this understanding. To safeguard

the standards are being upheld, the main focal point of the CAPR policy is to enhance the flow of information between private sectors and the federal government concerning cyber threats. In the contemporary world, there is often contention between the two parties, but the CAPR policy calls for both the federal government and private sector to utilize resources in order to augment cyber security for the consumers and their products. The main enabler of these goals is the Office of Cybersecurity and Communications’ (CS&C) Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division which is the “DHS primary point of engagement and coordination for national security/emergency preparedness (NS/EP) communications and cybersecurity initiatives for both government and industry partners, and is the Executive Secretariat for the Joint Program Office for the NS/EP Communications Executive Committee.”

The task to maintain this awareness is currently embraced by the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC “is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.” Beyond the money, authority, credibility, resources, or information from any domain, the policy above all calls for coordination between all the stakeholders from the consumers, to federal government, corporations, civil liberty groups and lastly the CS&C. In order to overcome the threats that cybercrime perpetuates, permanent situation awareness must linger in order to prevent and respond to cyber threats.

---


The federal government helps develop the budget for the CS&C and incentivizes corporations through certain tax cuts and leniency in policies. They ensure constitutional rights are upheld and they endorse education in cyber. Additionally, they maintain the international community to ensure U.S.’s cyber domain is protected from foreign threats.

Corporations communicate with the CS&C and federal government when vulnerabilities and threats are posed. They provide annual reports to ensure resources are dedicated to cyber security.

The CS&C facilitates the coordination between the Stakeholders and ensures the standard is upheld by corporations. Their response team provides assistance in cyber research to prevent breaches. The CS&C ensure that corporations are punished appropriately and that the interests of consumers are held in the highest regard.

Consumers demand safe products and education and report violations of compliance act.

The Civil Liberty Groups and ensures that constitutional rights are upheld by all parties.

The U.S. Department of Homeland Security

National Protection & Programs Directorate

Office of Cybersecurity & Communications

Office of Emergency Communications

Stakeholder Engagement and Cyber Infrastructure Resilience

National Cybersecurity and Communications Integration Center

Federal Network Resilience

Network Security Deployment

NCCIC Operations & Integration (MOI)

United States Computer Emergency Readiness Team (US-CERT)

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

National Coordinating Center for Communications (NCC)

Hierarchy of NCCIC

---

Basic Budget

The use of funds within the policy will be distributed for cybersecurity public education as well as implementing the cybersecurity programs for response and prevention. Since the policy will build upon, The National Cybersecurity and Communications Integration Act of 2014, will utilize the funds approved by the Congressional Budget Office this past year. According to statute 2519 of the act, the NCCIC falls under the National Protect and Programs Directorate of the Department of Homeland Security “is funded by appropriations provided to the Infrastructure Protection and Information Security appropriation account.” As of 2014, the account has accumulated $1.2 billion and $800 million has been set aside for cyber security programs. Additionally, according to S. 2519, there will be “no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments”. Furthermore, since the policy requires the joint effort of private sectors, the majority of expenditure will be from companies who yield massive revenue from their products. On June 2014, the Senate released the Fiscal Year 2015 Markup bill which expressed these allotments:

- $378 million for intrusion detection on civilian federal networks;
- $141 million to build on a new monitoring and diagnostics program that began in 2013 to better protect civilian federal networks through real time analysis of day-to-day activity; and
- $15.8 million for cybersecurity education to train future cyber professionals

---


18 Ibid


20 Ibid
More money will be added to the training in fighting cybercrime as a result of its recent success. Last year, $104 million was used for the Secret Service-directed cyber training for state and local law enforcement officials, including judges. In the last four years, Secret Service cyber investigations have affected over 4,900 arrests and prevented approximately $1.37 billion in fraud losses\textsuperscript{21}.

**Results**

The short term vision of this policy is to establish a primary information-sharing infrastructure between companies and the federal agencies with the NCICC mediating the relationship process. This involves promoting leveraging between the government as well as the corporates to obtain cyber security and the need for a regulating standard. To ensure the longevity of the policy, there must be a widespread acceptance for a need to improve the current day approach to cyber security. Even small companies (who are often targeted most by crime groups) should made aware of the push for a full inclusive network that ensures their companies will be provided the information they need to ensure cyber security for their companies and their products. The immediate results should be a relationship that is predominantly focused towards initializing communication in order to coordinate future plans on ensuring cyber security dominance. Another short term goal is to begin the process of standardizing the electronic minimum security guideline which will involve the NIST and NCICC coordinating on a minimum standard for security. In the long run, the CS&C should be a well-tuned and organized agency that provides sustainable and reliable service to not only preventing cyber-attacks but also responding to the threats as they arise. This also includes the coordination of ‘red teams’ of the federal government (ie the US Computer Emergency Readiness Team USCERT component of NCCIC) and private sector penetration

\textsuperscript{21} Ibid
testing teams in order to underscore cyber threats before they surface as well as respond to exploits as they arise.\textsuperscript{22}

Despite being under the DHS umbrella, the CS&C should stand independent of the interests of the government or corporations. This agency is intended to remain an organization that monitors and regulates the cooperation between the federal government and corporations to ensure that consumer products maintain the electronic security standards. Ideally, this policy should facilitate more changes within the government, corporates and the public to ensure all institutions are doing everything possible to combat cybercrime and securing the cyber domain for safe usage. As it stands the NCICC Act of 2014 requires an annual report from the Department of Homeland Security (DHS) on the operation of the Center and a Government Accountability Office (GAO) study on the Center's effectiveness\textsuperscript{23}. Further metrics that will be used in order to track the progression of the policy will be composed of operational reports, annual budget for cyber research and reports concerning the education projects conducted between the government and corporations inclusively or exclusively. These parts include monthly reports submitted that report how many cyber threats were detected or reported the measures taken to resolve them including how much coordination between the government and corporation took place in the process. An example of what these reports should show is the detailed cyber research conducted by a corporation before the development of a product, during its development as well as constant pentesting of the product after its released into the market. Inclusive of these reports would be a consumer incident report in which consumers are allowed to submit failure to comply to electronic security guidance. These consumer reports will be forwarded to the NCICC in order to check as well. Additionally, annual budgeting reports from both the government agencies and corporations will be submitted to the NCCIC to track the amount of resources


\textsuperscript{23} Ibid
allocated towards cyber security. The budgets should have segmentation amongst the areas being spent such as research for future threats, money spent on implementing response to cyber vulnerabilities, money spent on educating the consumers concerning cyber threats, and other areas.

Implementation

As stated above, the CAPR policy will be in accordance to pre-established policies already implemented under the NICCIC Act of 2014. In order for the policy to pass, it must follow the legislative hierarchy of the government which involves approval of the Senate and the House. Consequently, there will inevitably be political motives and agendas which will influence the approval of the policy as a new addition to the Act. Such as the CSA Act of 2012 failed as a result of fear of constitutional violations, this policy also possess a risk of being overturned. However, in order to combat the adversity, the policy itself will underscore the potential dangers that the cyber domain possess towards national security. Since the approval of the NCCIC Act in 2014, this new policy should easily pass as well since it is an addendum to the goals of the original Act. Security incidents in 2014 “rose 48% over the year before to 42.8 million which is equivalent to 117,339 attacks a day and many corporate information security budgets have yet to invest into increasing information security”.

Facilitating the flow of communication between the companies and government is the primary step. Due to the mercurial nature of the cyber domain, the timeline to impose changes must be expedited in order to meet the demands of the consumers as well as the meeting the advances of modern day IoT. A guideline that checks for product security and consumer awareness should be implemented and regulated by the federal government onto the corporates. Additionally, incentives should be initialized and to leverage the relationship. Within ten years, a full-wide national education standard should be imposed. Companies as well as the federal

government are inquired to bridge the gap between the rapid advancements of technology and public understanding. This namely targets the use of the standards which require the private corporations to propagate a methodology of education which perpetuates to consumers explicit information concerning vulnerabilities as well as their solutions to mitigate those dangers for their products. The aim is that consumers are provided as much transparency when it comes of the agenda and methodology for preventing cyber exploitations.

**Timeline of Implementation**

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>The National Cybersecurity and Critical Infrastructure Protection Act of 2014 and the current National Institute of Technology framework is approved and passed by Congress</td>
</tr>
<tr>
<td>2014</td>
<td>The Office of Cybersecurity and Communications is created under the Department of Homeland Security along with branches</td>
</tr>
<tr>
<td>2015</td>
<td>Deadline NIST and NCICC to coordinate an Enforcement Rule for standardization of IoT security</td>
</tr>
<tr>
<td>2016</td>
<td>Deadline for Notification Rule establishment requiring notification of consumers when a breach of their products occur as well as a basic customer education program when consumers purchase the products</td>
</tr>
<tr>
<td>2016</td>
<td>The Enforcement Rule and Notification Rule goes into effect after proper revision</td>
</tr>
<tr>
<td>2016</td>
<td>Deadline for Education plan to be agreed upon</td>
</tr>
</tbody>
</table>
| Dec 
2016 | Deadline for all businesses to comply to the Enforcement Rule |
| Apr 
2016 | Deadline for extensions granted for smaller businesses |
| Dec 
2017 | First submissions of all reports from corporations and agencies to the CS&C |
| Feb 
2018 | Companies and agencies notified of any discrepancies in reports as well ongoing investigations concerning failure to comply |

**Incentives**

Incentivizing the private sector will prove to be a necessary challenge as it will become a driving force into how well companies comply with the standards, but more importantly it influences how well the information sharing between companies and government will be. Incentivizing the private sector also means being able to balance a delicate line that ensures neither side could potentially monopolize the entire endeavor. Therefore, courses of actions such as collaborating with insurance industry to provide cybersecurity insurance, offering federal grants,
and providing legal privileges such as liability limitation are all viable solutions to encourage companies to embrace the policies.

However, besides incentivizing cooperation, a program of consequences must be set in order to correct poor behavior. In the cyber domain, one mistake can have an incorrigible consequence which leads to valuable loss in data and information. Consumers could potentially lose their entire life’s work and information as a result of a breach that otherwise could have been prevented by the corporate or another agency. As a result, certain punishments must be enforced. The NCICC may impose money penalties upon companies and a depending on the egregious consequences, the fine will be determined based by the case. Additionally, the company will be forced to assume full responsibility for the breach and make it up to consumers in whatever fashion that fits the repercussions.

**Conclusion**

The recent innovation of the Internet of Things has connected the people of planet Earth in a scale that humanity has never seen before. With its development, a new domain of cyber threats has become a growing concern. Despite being a highly developed nation, the U.S. will struggle to manage consumer security on these products. To ensure that the consumers are provided adequate protection from crime ware groups and other technological vulnerabilities, the country’s government has enacted the National Cybersecurity and Communications Integration Act this year. However to jumpstart the program, a catalyst such as the CyberAttack Prevention and Response (CAPR) is needed to ensure its success and secure its prosperity.