Information & Security: An International Journal

Raymond Collier, v.34:2, 2016, 105-120 http://dx.doi.org/10.11610/isij.3408

THE OBAMA ADMINISTRATION AND INCIDENT RESPONSE: A REPORT

Raymond COLLIER

Abstract: This article takes an in-depth look at the Obama Administration's incident response plan and its utilization in regard to cyber security throughout their Presidential and Executive-Administrative terms. A focal point and outlining the tool used in the report is the National Cyber Incident Response Plan (Interim Version), released in September 2010 by the Department of Homeland Security. Contents of the response plan are analyzed through brief descriptions, government reports, supportive literature, and comparison of actual efforts conducted by the Administration that reflect sections of the plan. A brief review of legislature that could directly affect the process, assurance, or future of incident response and cyber security proposed by the Administration is included. Discussion of the current presiding President, Barack Obama, and his mannerisms in the wake of incidents, thoughts and views on the nature of the subject, actions planned as well as taken to secure the United States' technological realm, that is the internet, from digital terrorism are micro-scoped and provide a real-time wealth of how incident response is being handled in the U.S.; the past struggles appertained and a glimpse into its architectural future. The report collectively parallels the Administration's formulated incident response plan with their actual actions on real-life incidents in an attempt to provide present-day documentation of resolutions pertaining to incidents and cyber security in the U.S.

Keywords: Barack Obama, Obama Administration, incident response, cybersecurity, NCIRP, proposals, legislature, law.

Introduction

President Barack Hussein Obama II is the first African-American, 44th elected and currently presiding President of the United States of America. President Obama was elected on November 4, 2008 for his first presidency term lasting four years, then re-elected on November 6, 2012 for his second term. The administration for the presi-

dent includes the president himself and the positions held by Vice-President Joe Biden, First Lady Michelle Obama, Dr. Jill Biden, the Cabinet, White House Staff, Executive Office of the President, and other Advisory Boards. The President's duties enforce a multitude of powers entailing Article II of the US Constitution as well as executive, legislation, appointment, foreign affairs, and emergency powers in relation to incident response. His responsibilities come from the power vested in the Executive Branch which gives authority for implementation and enforcement of law adopted by Congress. The vice-president—a member of the Executive Branch—acts as a back-up for the president that must be readily equipped to assume Presidency at any given moment. The rest of the administration such as the Cabinet and other government branches hold the weight of daily administration and enforcement of federal law.[1]

Incident Response Plans (IRPs) are essential and a major priority as well as a need for the majority of organizations. An IRP can be described as a document or policy that an organization uses in the midst or aftermath of an incident that addresses phases or steps to be taken concerning personnel responsibility, organization strategy, incident assessments, information retrieval or access and other issues that may be affected in the wake of an incident. An IRP is often linked to management of security breaches or attacks within an organization but can be related to the management of various issues that can possibly destroy an organization if not handled properly. There have been six steps notated by a respected institution that are thought to handle an incident effectively: preparation, identification, containment, eradication, recovery, and lessons learned.[2] One, few, or all of the afore-mentioned steps are thought to be relevant for ensuring a successful IRP.

Within the Department of Homeland Security (DHS), the Strategic Plan for Fiscal Years (FY) 2012-2016 elaborates the goals that the Obama Administration have for their IRP. Among the document's fourth mission of safeguarding and securing cyberspace, which is goal 4.1 – to create a safe, secure, and resilient cyber environment, is objective 4.1.4 – to develop a robust public-private cyber incident response capability.[3] The plan includes planned targets for the FYs 2012, 2013, and 2016. Performance measures reflect percentages of satisfactory or higher rated intelligence reports from customers managing risks to cyberspace, percent of external traffic monitored for cyber intrusions at Civilian Federal Executive Branch agencies, financial crime loss prevented by the Secret Service Electronic Crimes Task Forces, percent of unique vulnerabilities detected during cyber incidents where mitigation strategies were provided by DHS, and the average amount of time required for initial response to a request for assistance from public and private sector partners to prevent or respond to major cyber incidents.[3] The Administration in lieu of Homeland Security also has a National Cyber Incident Response Plan (NCIRP), the interim version of

which was published in September 2010 and describes its purpose as establishing a "…strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident." The NCIRP has a scope that reaches federal, state, local, tribal, and territorial governments.[4] The scope for the NCIRP is one of five major topics to be discussed throughout this report concerning the Obama Administration's IRP being accompanied by the national concept of operations, organization of the National Cyber security and Communications Integration Center, actions of the incident response cycle, as well as its universal role and responsibilities to convey proposed management of incident response and cyber security.

Proposals, legislature and law are a major factor that goes into the planning and strategy of incident response and cyber security. A main focus of this report is to detail actual events around this subject to relay the work and efforts that have been made by the Administration, whether successful or seen as a failure. Description of bills, addresses, and statements made on behalf of the Administration are reported to enhance the depth of the reader's knowledge on how incident response has and is being managed. The report will exist to provide factual incidents and response to them by the Obama Administration. The research is not to be considered in any way the author's opinion, bias or a reflection of how another organization should deal with incident response and cyber security. The goal has and will always be to provide a report that displays integrity, truth and value based upon researched available documentation of the Obama Administration and its proposition, occurrences and reaction to national incidents and cyber security.

NCIRP – Scope and Purpose

The National Cyber Incident Response Plan promotes clarification and directional strategy in the instance of an incident happening. The document entails the way in which the nation plans to respond in the wake of day-to-day cyber incidents and controls the escalation of operations into coordinated response activities at the national level. These plans place a primary focus on creating the foundation and exploration tools needed to reprimand a significant cyber incident. Significant cyber incidents are described as those conditions that increase the need for national coordination and also trigger the National Cyber Risk Alert Level (NCRAL) system to level 2 in the cyber domain.[4] Recent significant cyber incidents handled by the Obama Administration include the issuance of an Antitrust Policy Statement. The statement includes the U.S. Department of Justice (DoJ) and Federal Trade Commission, reiterating a fourteen-year-old analysis that informs how the design of proper cyber security sharing of threat information most likely will not raise anti-trust concerns. U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE)

issued a National Exam Program Risk Alert (Alert) with purposes of assessing how prepared cyber security is within the securities industries as well as data collection of recent cyber threat experience as a gesture. The questions within the Alert are described as detailed, rigorous, and probing. These questions are thought to set initiatives possible to lead to adoption by critical infrastructures that build their own cyber security intelligence, standards, and correlation between receiving cyber-threat information from disparate sources and maintaining increased focus on resilient ability to respond to their worst possible threat, attack, or scenario.[5]

The NCRAL indicates national cyber risks that account for threats, vulnerabilities, and potential consequences throughout cyber infrastructure and outlines conditions in Homeland Security Presidential Directive 5 (HSPD-5). Focus of the NCRAL is on cyber incidents impacting national security, public health and safety, national economy, and public confidence that includes any combination of the aforementioned categories at the national, regional, or sector level.[4] An example of a NCRAL trigger and response during the Obama Administration is demonstrated when the Division of Corporation Finance of the Securities and Exchange Commission (SEC) issued Disclosure Guidance Topic No. 2 – Cyber-security (CF DG 2) responding to Senate Commerce Committee pressure and public companies that were being publicly attacked in 2011. Ultimately, the CF DG 2 established that of the Securities Acts of 1933 and 1934 requiring companies registered with the SEC to disclose material information, adhering that information related to cyber security is material.[6]

NCIRP – National Concept of Operations

The National Cybersecurity and Communications Integration Center (NCCIC), an organization through DHS, is responsible for coordinating national response in accordance to significant cyber incidents and communicates cross-domain situational awareness that provides updates of a cohesive look at cyber threats, vulnerabilities, and consequences whose awareness can provide warning and support. Pertinent information also known as situational awareness is only provided to certain parties with certain level, detail, classification or appropriation and they are the National Infrastructure Coordinating Center (NICC) and National Operations Center (NOC) which magnify the national operating model for the President, Administrative Staff, and partners.[4] The U.S. operates and uses a centralized coordination and decentralized execution for effective response operations.

In 2009, President Obama tasked U.S. Cyber Command (CYBERCOM) with centralized command of U.S. Cyber Operations who since have been responsible for defensive and offensive capabilities as well as a “full spectrum” of operations.[7] The general roles and responsibilities for cyber incidents are shared among a number of government branches, federal departments, private sectors, and non-government organiza-

tions in which the NICC provides the facility and mechanisms needed for coordination of response efforts.[4] Reports show how cyber security, concerning federal securities laws addressing mutual fund board's responsibility on the subject has caught the attention of the SEC and, because there is no discussion of cyber security in the Investment Company Act of 1940, the article suggested looking to general responsibilities under federal securities law or law notions of fiduciary duty. [8]

There are relationships that are birthed at the brink of an incident that will require the support of organizations for other organizations through routine sharing, deconfliction, collaboration, and possible joint action while the nature of the relationship and its support will depend solely on the nature, severity, and scope of an incident.[4] Simultaneous support relationships are needed in certain scenarios and are illustrated when an organization at one level is being supported, yet they are supporting an organization at the same level or another.

NCIRP – Organization of the National Cybersecurity and Communications Integration Center

The National Cybersecurity and Communications Integration Center (NCCIC) can be described as a continuous monitoring system with primary concerns being management of situation awareness and incident response at the national level, as well as point-of-contact and relay of communications for Federal Government, intelligence community, and law enforcement. The NCCIC operates by a mission of reducing probable or critical incidents capable of significantly compromising security and resilience of information technology and communications, with a vision of securing cyber and communications infrastructure whose purpose is to support homeland security, a vibrant economy, as well as health and safety of Americans.[9]

According to the National Cyber Incident Response Plan from the Department of Homeland Security, the NCCIC has two primary phases that it operates in – steady-state response and significant incident response, both of which affect the organization, processes, relationships, and agreements involved with the NCCIC. The steady-state of cyber security operations is the daily response to threats by Federal, State, Local, Tribal, Territorial governments, and the private sector within their networks, systems, and data. When the state shifts to significant incident response, relationships are leveraged through the inclusion of all partners and Cyber Unified Coordination Group (UCG) Senior Officials that may have not been needed during steady-state but are now maximized to execute effective incident response and risk mitigation activities.[4] The organization of operations for the United States has been an ever-growing and internet security altering process since 1988 with the pioneering effects of its national-level cyber security policy making.[7] In 2011, President Obama issued the Cybersecurity Legislative Proposal seeking urgent action for giving private sector and

the government the tools needed to counter against cyber threats which warranted the issue of the international strategy for cyberspace to inform nations of foreign policy cyber security issues. However, when legislation was not passed by Congress, Obama and his Administration issued an Executive Order with the purpose of protecting critical infrastructure through establishment of baseline cyber security standards.

The revised provisions of the 2011 legislature and proposal includes enabling and promoting better cyber security information sharing between the private sector and government. The proposal advocates the private sector sharing appropriate cyber threat information with DHS's NCCIC who will be obligated to share in real-time with relevant federal agencies, private sector-developed and operated information sharing and analysis organizations (ISAOs) as well as encourage their formation, all of which has, is, or possibly will affect the organization of the NCCIC.[1]

NCIRP – Actions of the Incident Response

The Department of Homeland Security lists five phases that make-up the incident response cycle. This cycle forces actions to be taken and coincides with coordination and the common operational picture which are considered fundamental elements and essential developments concerning the phases. Coordination is important for both steady and significant incident response states as different priorities and drivers may be presented for decisions to be made by partner organizations that can affect response at many levels.

Developing a common operational picture supports the information sharing environment among NCCIC partners that can ultimately provide a successful foundation for response efforts placing the NCCIC in a position of readiness to assist with priorities and work with departments and agencies on specific authorities that may have conflict or inabilities concerning operations.[4] The five phases of the incident response cycle include Prevent and Protect which provide the building blocks of the cycle where organizations within the NCCIC ensure the NCCIC and its critical partners receive preventive and protective information they are able to act on throughout all phases of the IR cycle. The Detect phase increases the chance of critical network owners and operators' ability to catch malicious or unauthorized activity. The Analyze phase involves performing an analysis of an incident to discover its intent. The Respond phase is the response process, activity, or assistance given to the incident and the Resolve phase is where the Assistant Secretary for Cybersecurity and Communications (CS&C), Cyber UCG IMT, and NCCIC work together to confirm intended response effort outcomes are met, able to be managed without the help of national coordination, issue appropriate advisories and communications, identify and participate in learned lessons as well as coordinate implementation of long-term corrective actions through monitoring, tracking, and measuring.[4]

In a 2014 review on federal agencies' ability to respond to cyber incidents, results show they did not consistently demonstrate effective cyber incident response practices; did not effectively demonstrate some incident response activities; demonstrated aspects of incident analyses but did not complete others; demonstrated that they contained the majority of incidents; demonstrated that they eradicated most incidents; demonstrated steps to recover systems but did not consistently demonstrate remedial actions to prevent reoccurrence; updated policies or procedures but did not generally capture cost information; selected agencies policies, plans, and procedures did not always include key information or elements; selected agencies did not always develop procedures for incident response; other incident response practices were not implemented; and the Office of Management and Budget (OMB) and DHS have not used the CyberStat Review Process to address agencies' incident response practices. The report continued in the concluding statements to inform of the inconsistent nature that agencies demonstrated regarding their ability to respond to cyber incidents in an effective manner.[10]

In a 2013 review, the challenges that the federal government faced in opposition of addressing a strategic approach to cyber security reported designing and implementing risk-based federal and critical infrastructure programs; the ability to detect, respond to, and mitigate cyber incidents; education, awareness, and workforce promotion; research and development promotion; the ability to address international cyber security challenges; milestones and performance measures; cost and resources; roles and responsibilities; and linkage with other key strategy documents; all issues that remain the federal government's challenge areas. The report continues to conclude the federal government's strategy for cyber security is "poorly articulated and incomplete" with repeated bashing referring to their approach as having "limited value as a tool for mobilizing actions to mitigate the most serious threats facing the nation."[11]

NCIRP – Universal Roles and Responsibilities

The universal roles and responsibility section of the NCIRP explains the general tasks that should be performed by each entity in terms of preparedness, response, and short-term recovery. Preparedness is taken into context as a basic responsibility of all Federal, State, Local, Tribal Territorial, and private sector organizations. Activities that spawn engagement with the NCCIC are maintaining and aligning incident response plans with the most current version of the NCIRP; organizing and developing prescripted cyber incident assignments with periodic updating; being equipped through ensuring facilities, systems, supplies, and personnel are prepared and ready to provide response for an incident; training where individuals, teams, and organizations are taught procedures regarding cyber incident response; exercising response and re-

covery plans; and concluding with evaluation and improvement of lessons learned from experiences.[4]

One of the more familiar common roles is cyber incident response where all partners in the NCIRP have responsibility that calls for distinct missions and different authorities. The next role and responsibility of short-term recovery is summoned immediately after an incident possibly overlapping with response efforts providing restoration to essential services and creating unique roles for all partners in the NCIRP.[4] In a 2010 address on national security strategy, President Barack Obama acknowledges his role and responsibility for incident response through claims of the U.S. digital infrastructure being a strategic national asset and expression of how protecting it is a national security priority, he demands that "[he] will deter, prevent detect, defend against, and quickly recover from cyber intrusions and attacks," seemingly accepting the universal roles and responsibilities as well as guaranteeing to implement the actions of incident response laid out in the NCIRP.[12]

The President lists ways planned to help carry out his esteemed declaration by announcing investment in people and technology. He depicts the investment as a way of advancing goals including investing in research and development, working with government and the private sector to design secure technology, and promotion of cyber security awareness as well as digital literacy within boardrooms and classrooms. Proposal of advancement through strengthening partnerships via expansion of the way in which government and private sector work together as well as strengthening international partnerships is also presented.[12]

However, in a recent publication of the Data Breach Response Guide, an update on roles and responsibilities was addressed. The guide suggests every staff member understand how their roles might change during an incident or breach; how organizations that employ a Chief Information Security Officer (CISO) holding enterprise-wide responsibility may be able to reduce their cost of a data breach by 35 %; that each member of the team must realize their unique responsibility for applying prevention and preparedness best practices to his or her own department; and in regards to successful notification, the responsibility is placed on the organizations themselves or delegated employees for determining deadlines, ac-cording to state law.[13]

The Obama Administration on Proposals, Legislation, and Law Affecting Cybersecurity and Incident Response

There is much that can be taken from the actions of a leader and those that are placed in leadership roles as of managing a country. The act of responding to incidents may and more than likely will depend upon legislature in place that could affect the response. President Obama and his Administration have submitted more than seven

documented pieces of legislation before the United States Congress that are reportedly pending.[14] Listings and brief description of these cyber security policies are as follows and will remain a staple in the "Obama Administration and Incident Response":[14]

1. *Cyber Security and American Cyber Competitiveness Act of 2011* (CSACCA) – The bill is a five-page document that defines the cyber security problem and resembles a call to action. The bill urges Congress to be active in securing the United States against cyber-attacks. Proposals for ways of protecting the U.S. sustain improvement of security, providing incentives for private companies to defend themselves, tech-sector jobs investment, continued defense of critical infrastructure as well as the will and duty of protecting American citizens' civil liberties.

2. *Cybersecurity and Internet Safety Standards Act* (CISSA) – The bill calls to action the Secretary of the Department of Homeland Security, proposing specific mechanisms be done for developing and implementing security standards by internet service providers (ISPs).

3. *Cybersecurity Education Enhancement Act of 2011* (CEEA) – The bill proposes a $ 3.7 million grant aimed at creating cyber security programs for universities. The bill includes what is titled *e-Security Fellows Program*, which is described as individuals working in related fields that align directly with the Department of Homeland Security to fight against, improve, and facilitate cyber security issues.

4. *Chief Technology Officer Act* (CTOA) – The bill establishes the new position and Office of the Federal Chief Technology Officer that is within the Executive Office of the President. The President and government would use the Chief as their informer of all things related to cyber security. Responsibility of the Federal Chief Technology Officer would include the design and coordination of policy for federal agencies.

5. *Cybersecurity Public Awareness Act of 2011* (CSPAA) – The bill proposes concerns of Congress gaining access to cyber-attack data that is happening across the nation. The bill demands several reports from different government organizations and titled employees. Reports from the Department of Homeland Security include informing on cyber incidents occurring in military and defense networks as well as the assessment of security risks in regard to the nation's electric grid and technologies previously in possession of foreign countries. The Department of Defense would be called upon to report on the first of two reports to DHS. Industries are desired to provide incident reports. Both the FBI and Attorney General would be charged with providing Congress information and prosecutions related to cyber crimes. The Securities and Exchange Commission would be tasked with reporting the impact of cyber attacks concerning the financial sector. Additional reports would come from the Sec-

retary of Homeland Security to address how assistance can be given to the private sector from federal agencies for attempts at defending information networks, protection methods relating to critical infrastructure and general plans for promoting and improving public awareness of cyber security issues.

6. *Homeland Security Cyber and Physical Infrastructure Protection Act of 2011* (HSCPIPA) – The bill places the Office of Cybersecurity and Communications (OCC) in the Department of Homeland Security charging it with the task of establishing and enforcing cyber security requirements. The cyber security requirements enforced by the OCC would affect civilian non-military and non-intelligence community federal systems. The work group is described as comprising of top technology officials within federal civilian agencies while the legislation pushes the need for information sharing through regulated entities, workforce needs audits to be conducted annually, as well as commitment to research and development.

7. *Executive Cyberspace Coordination Act of 2011* (ECCA) – The bill creates the National Office for Cyberspace within the Executive Office of the President. The office would head the Federal Cybersecurity Practice Board. Through this office, agencies would be tasked with development and implementation of programs that further the goals of the new office and satisfy requirements of cyber security program audits. The bill creates an information clearing house which collects data for analyzation of security incidents and the Office of the Federal Chief Technology Officer while granting power to the Secretary of Commerce for issuance of standards that enhance federal information and private sector systems security. The expansion on a definition of critical information infrastructure is given.

8. *Cybersecurity and Internet Freedom Act of 2011* (CIFA) – The bill originally was proposed in June 2010 as the *Protecting Cyberspace as a National Asset Act* (PCNAA) which would have enabled the President to declare a national cyber emergency causing critics to refer to the bill as an "Internet kill switch." After receiving no votes from Senate, the bill resurfaced in 2011 under the new name with modifications including creating the *Office of Cyberspace Policy* in the Executive Office of the President. The office would be responsible for development of a national strategy increasing cyberspace's security and resilience. Senate is granted confirmation rights and approval for the President's choice as the head of office. The *National Center for Cybersecurity and Communications* (NCCC) is a new department created within the Department of Homeland Security. Provisions include information sharing, private sector assistance, employment, education, and professional development with expansion of research and development. The updated version addresses concerns with the first and informs that the bill grants no authority for a complete shutdown of the internet which critics were afraid of before.

President Barack Obama in the Face of Incident Response and Cybersecurity

When faced with unprecedented accounts of infiltration and cyber security incidents within the massive world of technology and cyber security, President Barack Obama seems to remain proactive, hands-on, and determined to protect, secure, and safeguard the U.S. from security threats. Like the current President's colleagues before him, the Administrations of Clinton and Bush, Obama has issued Directives aiming for the security of the Coalition of Networked Information (CNI), CNI's definition remaining vague, however, reports from a classified White House Staff member bolster "that everything from the electric grid to telecommunications and transportation systems constitute CNI" and how the effect of cyber-attacks directed at more than one network can bring distress to the U.S.[7] During the year of 2009, within a one-year grace period of Obama becoming President, the federal government's cyber security plans and activities were taken under review by him initiating declarations concerning U.S. CNI as well as Cyber Command.[7]

Obama's 2012 presidency year brought with it his legislature in the form of the Cybersecurity Act of 2012 with hopes of granting DHS the powers of overseeing the cyber security government, establishing its performance requirements and creating exchange, as well as the legislation, that is the Secure IT Act, that was to work under the National Security Agency whose approach was more discretionary.[7] The Cybersecurity Act of 2012 would classify industries as "critical" in the event that mistreatment or abuse to "system[s] or asset[s]... – reasonably result[ing] in the interruption of life-sustaining services…, [as] catastrophic economic damages to the United States…, [or] severe degradation of national security." The outcome ended with neither the Cyber-security Act of 2012 nor the Secure IT Act being enacted.[7]

The inabilities to persuade actions of Senate to enact the proposed legislative acts may have sparked the commentary of the President's 2013 State of the Union Address, where he warns, "[we] cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy." The follow-up came with action from the Executive Branch addressing cyber security through an Executive order promoting strength amongst public-private cooperation among concerns with the protection of electronic infrastructure. The failure of legislation on cyber security continued as well as documented disagreements within the U.S. House, the Senate, the White House, privacy advocates, business interests, and security specialists.[6]

More recently, in a 2015 press release, President Obama continued his cyber security efforts in an announcement sincerely concerned for the state of the economy and the cyber world's fate against cyber assaults and hackers where he demands: "our first

order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place…"; pleads that "this is part of the reason why it's going to be so important for Congress to work with us and get an actual bill passed that allows for the kind of information-sharing we need…" and implies that if that does not happen "…this is going to be affecting our entire economy in ways that are extraordinarily significant."[15]

The President continued with his announcement addressing those steps he planned to take next in defense of the nation's systems. Reports reveal that the President's plans include yet another new legislature proposal; the act of building in Congress on important work, continuing his previous long-term goal of solving challenges that involve information-sharing able to deter responses concerning cyber-attacks; revisions of the 2011 provisions legislative proposal still unanswered by Congress today; and if more is needed, the President is ordering the work be done in a bipartisan, bicameral manner attempting to expedite the urgent manner specifically for American people.[15] In addition to speaking on the updated proposals' topics of promoting, enabling, and making cyber security information-sharing better, provisions that modernize law enforcement authorities to combat cybercrime, and the requirements of national data breaching reporting; President Obama also announced the date, purpose and next step in his President's BuySecure initiative being the White House Summit on Cybersecurity and Consumer Protection. He continued to elaborate on his jobs-training initiative that provides grants to historically black colleges for cyber security education with purposes of helping to fill U.S. job markets for skilled cyber security professionals. The program is designed for two-year colleges, four-year colleges, research institutions, and Virgin Islands helping growth in science, technology, engineering, and mathematics (STEM) curricula for HBCUs.[15]

The first quarter of the year 2015 proved busy for President Obama. The President gave his State of the Union Address on January 20, 2015, proposing how he and the administration plan to address protection of networks, trade secrets, and individual policy insisting to Senate government officials and the American people "we are making sure our government integrates intelligence to combat cyber threats…; "…I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber-attacks, combat identity-theft, and protect our children's information" while restating his support for cyber threat information exchange amongst private sector and the government's own Department of Homeland Security through the National Cybersecurity Communications Integration Center.[16]

On February 6, 2015, the 2015 National Security Strategy was released by President Obama displaying various cyber security issues where again he calls on Congress, this time to enact a legislative framework birthed in the U.S. to be shared internationally; upholding regulation of behavior regarding intellectual property, online expres-

sion, and respect for civilian infrastructure.[17] In an attempt to keep the cyber security fever going, President Obama announced on February 10, 2015 the creation of a new government agency, the *Cyber Threat Intelligence Integration Center* (CTIIC) seemingly finally laying a concrete foundation to Obama's war for information-sharing, the new CTIIC will act as the focal point for cyber security threat data sharing across all government agencies giving the President real-time cyberspace actionable intelligence with "the mission of providing an integrated all-source analysis of threats…" connecting the National Security Agency, the Department of Homeland Security, the Federal Bureau of Investigation and the Central Intelligence Agency.[18]

On February 13, 2015, President Obama stood more ground on cyber security at the White House Summit through consistently gauging his war on cyber security and introducing four principles for combating the subject that include having a shared mission between government and industry, focusing on unique strengths, constantly evolving and the ability of protecting the privacy and civil liberty of the American people. In more efforts to continue his information-sharing campaign, the President signed a new executive order promoting the topic in regards to government and private sector and also encouraging companies and industries to share information through the set-up of hubs.[19]

Conclusion

Since the beginning of President Barack Hussein Obama II's reign as President, research and documentation reports that incident response and cyber security has been at the forefront of concerns for him and his administration. The United States has become an internet-driven, technology-transaction dependent and digital business conducting country that the Obama Administration seems to recognize and desperately seeks to protect. Research and documentation as well narrate the tireless efforts of the Administration's pursuit in this protection despite the anguish and opposition that various levels of government have spewed in the midst of their campaign.

Since the Obama Administration's stint as officially managing the country, the United States' stance toward international cyber-arms control has changed. Before, the U.S. feared international cyber-arms control for reasons of the internet being globally regulated, which was thought to undermine the US technological dominance and to create restriction of openness but now, under the command of the current President, has come to the realization of how reliant the U.S. is on cyber-space, yielding awareness of its vulnerability to cyber attacks.[7]

President Obama commissioned the Cyberspace Policy Review, released May 29, 2009 – a year after gaining presidency that served as an additive to the Comprehensive National Cybersecurity Initiative while calling for the development of a cyber

security incident response plan.[4] Within the five, nearing six years that have passed, the Obama Administration consistently remained aggressive towards incident response through the plethora of attempts at improving cyber security. Obviously, the Administration has not run out of fuel as their endeavors continue eagerly in the year of 2015. Within the security section of the National Security Strategy, released February 2015, they acknowledge and interpret the role of the U.S. and internet suggesting that "an open, interoperable and secure internet plays [a role] in economic security of the nation and global community."[17] In another benchmark for the proposal of information-sharing, a meeting was held at Stanford University with the White House and Silicon Valley leaders discussing cyber security and consumer protection. The meeting reports to have caused reflection and pondering of the relation to President Obama signing a second Executive order at the White House Summit calling for Information Sharing and Analysis Organizations (ISOAs) to be established, both happening in February of 2015.[20] Perhaps with the announcement from the Obama Administration on creating the new government agency, *Cyber Threat Intelligence Integration Center*, recognition that legislation years ago possibly could have helped with the many recent cyber attacks on the U.S. may or may-not be acknowledged. However, there will always be interesting insight to gain from writers like Sylvertooth who shares "The center was basically a compromise for both parties and all together presents a win-win situation for the entire United States and our National Security" offering a silver-lining, no pun-intended, for the Obama Administration's past, present, and future of incident response and cyber security in the remainder of their Executive-Administrative term.[18]

Acknowledgements

The research was conceived and inspired by a Disaster, Recovery and Continuity course at Kennesaw State University, instructed by Dr. Michael Whitman. Only the author's views are reflected. Kennesaw State University and Dr. Michael Whitman are not liable for any use of the information within this research. The author thanks his research mentor Dr. Kathaleena Edward-Monds for continued encouragement and mentorship.

Notes:

1 The Executive Branch, The White House, http://www.whitehouse.gov/our-government/executive-branch, accessed: February 5, 2015.

[2] Luis Rocha, "Computer Security Incident Handling – 6 Steps," *Count Upon Security*, 2012, http://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/, accessed February 5, 2015.

[3] "Department of Homeland Security Strategic Plan: Fiscal Years 2012-2016," U.S. Department of Homeland Security (DHS), February 2012, http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf, accessed February 4, 2015.

[4] "National Cyber Incident Response Plan," Interim Version, U.S. Department of Homeland Security (DHS), September 2010, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf, accessed February 4, 2015.

[5] Roland L. Trope and Lixian Loong Hantover, "In the Wake of Cyber Damage: Significant Decisions in Cybersecurity 2013-2014," *The Business Lawyer* 70, no. 1 (Winter 2014–2015): 223-230.

[6] Matthew F. Ferraro, "'Groundbreaking' or Broken? An Analysis of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, and Implications," *Albany Law Review* 77, no.2 (2014): 297-347.

[7] Scott Shackelford And Amanda Craig, "Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity," *Stanford Journal of International Law* 50, no. 1 (2014): 119-184.

[8] Arthur C. Delibert, Marguerite W. Laurent, and Lori L. Schneider, "Cybersecurity: Could Investment Company Directors be Liable for a Breach?" *The Investment Lawyer* 22, no. 2 (2015): 23-36.

[9] "National Cybersecurity and Communications Integration Center," U.S. Department of Homeland Security, 2014, www.dhs.gov/about-national-cybersecurity-communications-integration-center, accessed February 5, 2015.

[10] "Information Security: Agencies Need to Improve Cyber Incident Response Practices," GAO Highlights, GAO-14-354 (Washington, D.C.: United States Government Accountability Office, 2014), http://www.gao.gov/assets/670/662901.pdf, accessed February 4, 2015.

[11] "Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented," GAO Highlights, GAO-13-187, United States Government Accountability Office (GAO), 2013, http://www.gao.gov/assets/660/652170.pdf, accessed February 4, 2015.

[12] President of the United States, "National Security Strategy 2010," White House, 2010, http://nssarchive.us/national-security-strategy-2010/, accessed February 4, 2010.

[13] "Data Breach Response Guide: Experian Data Breach Resolution, 2013-2014," *Experian*, 2013, http://www.experian.com/assets/data-breach/brochures/response-guide.pdf, accessed February 4, 2015.

[14] Karson K. Thompson, "Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate," *Texas Law Review* 90, no. 465 (2012): 465-495.

[15] White House, "Securing Cyberspace – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," 2015, http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat, accessed February 5, 2015.

[16] Kevin Newmeyer, "Cybersecurity and the 2015 State of the Union Address," Cyber Experts Blog at National Cybersecurity Institute, Excelsior College, 2015,

http://www.nationalcybersecurityinstitute.org/cybersecurity-and-the-2015-state-of-the-union-address/, accessed February 10, 2015.

[17] Kevin Newmeyer, "Cybersecurity in the President's National Security Strategy," Cyber Experts Blog at National Cybersecurity Institute, Excelsior College, 2015, https://www.excelsior.edu/article/cybersecurity-in-the-presidents-national-security-strategy/, accessed February 10, 2015.

[18] Randall Sylvertooth, "Government Cyber Agency Will Be Here Shortly!" Cyber Experts Blog at National Cybersecurity Institute, Excelsior College, 2015, www.excelsior.edu/article/government-cyber-agency-will-be-here-shortly/, accessed February 15, 2015.

[19] David Hudson, "President Obama Speaks at the White House Summit on Cybersecurity and Consumer Protection," The White House Blog, 2015, http://www.whitehouse.gov/blog/2015/02/13/president-obama-speaks-white-house-summit-cybersecurity-and-consumer-protection, accessed February 20, 2015.

[20] Kevin Newmeyer, "Executive Order on Cybersecurity: Billion-Dollar Bank Heist," Cyber Experts Blog at National Cybersecurity Institute, Excelsior College, 2015, https://www.excelsior.edu/article/executive-order-on-cybersecurity-billion-dollar-bank-heist/, accessed February 20, 2015.

About the Author

Raymond COLLIER Jr. is currently a full-time graduate-student at Kennesaw State University studying information systems at the master's level. He completed a graduate-level student assistant position in his first semester and anticipates graduation summer 2016. In 2014 and 2013 he gained a contract as a Programmer Analyst with the Computer Science Corporation and completed an internship as a Database Administrator and IT Consultant with Workforce Investment Act. His research interests include virtualization and its deployment into real-life application information systems. He is an author of articles and papers in conferences such as Wearable Technologies for Healthcare Innovation 2015 and the 18th Southern Association for Information Systems Conference.