Critical Infrastructure Cybersecurity in the US: Two Decades of Evolutionary Policy

Author Joshua Marciano

By Joshua Marciano

Beginning with the Clinton administration, the US government has been collaborating with the private sector to develop, test, and improve policies to enhance the cybersecurity of US critical infrastructure. President Bill Clinton and his successors in the White House have each played an important role in the development of current US policy for critical infrastructure cybersecurity. The Clinton administration created the original framework for critical infrastructure cybersecurity, introducing concepts like public-private partnerships for critical infrastructure protection and information sharing and analysis centers (ISACs). The George W. Bush administration built upon this framework by creating the Department of Homeland Security (DHS) as the leading agency for critical infrastructure security (both physical and cyber) and publishing the first National Infrastructure Protection Plan. The subsequent Obama administration has enhanced many of its predecessors' policies to help the United States cope with the increasingly sophisticated and persistent nature of cyberattacks. Most recently, the Obama administration has begun to look to the US private sector to find new ways to enhance US critical infrastructure cybersecurity.

Origins of Critical Infrastructure Cybersecurity in the Clinton Administration

The rise of the Internet and its application to US industry were responsible for the Clinton administration's interest in critical infrastructure cybersecurity. With the beginning of the "Dot Com Boom" in the mid-1990s, it was apparent that a cyberattack on the computer networks of US critical infrastructure, especially those of the telecommunications or electricity sector, could have a devastating impact on US national security, economic prosperity, and public health. Recognizing that the US "is increasingly reliant upon interdependent and cyber-supported infrastructures," the Clinton administration laid the groundwork for US critical infrastructure cybersecurity policy.

Photo: Reuters

US policy for critical infrastructure cybersecurity has evolved under the administrations of presidents Bill Clinton, George W. Bush and Barack Obama.

On July 15, 1996, President Clinton signed Executive Order (EO) 13010, which had three important results. First, it officially recognized eight critical infrastructure sectors in telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, and emergency services. Second, it recognized that these critical infrastructure sectors were susceptible to both physical and cyber threats. Finally, it created a panel called the President's Commission on Critical Infrastructure Protection (PCCIP), which was designed to study and report to the president on the scope and nature of physical and cyber threats to US critical infrastructure.

While the PCCIP found no immediate threat to the nation's critical infrastructure at the time, it correctly predicted that critical infrastructure cybersecurity would become a growing national security threat in the future and called on the US government to take action. Recognizing that the vast majority of US critical infrastructure is owned by the private sector, the PCCIP recommended that the US government facilitate greater cooperation and communication with industry on matters related to critical infrastructure cybersecurity.

In any event, the PCCIP's findings led Clinton to sign Presidential Decision Directive 63 (PDD-63) on May 22, 1998. This directive resulted in four influential concepts that continue to guide thinking on this issue today. First, PDD-63 stressed the importance of using public-private partnerships to address critical infrastructure security (both physical and cyber). Second, it established the concept of lead government agencies — today called Sector-Specific Agencies — for coordinating with critical infrastructure sectors. Third, PDD-63 created a mechanism to facilitate coordination and collaboration on critical infrastructure protection within and between the private and public sectors. Finally, PDD-63 suggested the creation of private sector-led ISACs to gather, analyze, and disseminate threat information amongst industry. ISACs continue to be a key part of the US government's policy for critical infrastructure cybersecurity.

The Clinton administration's policies for critical infrastructure cybersecurity are best remembered for providing the important foundational structure from which subsequent administrations could build and adapt their cybersecurity policies to address the current geopolitical landscape and threat environment. While both the Bush and Obama administrations have made important changes to this initial policy framework, the fact that many of the concepts first introduced in the late 1990s are still evident in current policies is a testament to the foresight of the Clinton administration regarding cyber threats and how the US planned to respond to them.

The Bush Administration & Cybersecurity after 9/11

The critical infrastructure protection policies developed by the Bush administration were largely influenced by the terrorist attacks of Sept. 11, 2001. While these attacks raised fears about the physical security of US critical infrastructure, they also heightened concern about the cybersecurity of US critical infrastructure. These concerns prompted the Bush administration to develop a more centralized organizational structure and a more detailed plan for critical infrastructure protection that would, according to Bush, "gather and focus all our efforts to face the challenges of cyberterrorism, and the even worse danger of nuclear, chemical, and biological terrorism." As the Bush administration worked toward this goal, it continued certain aspects of Clinton-era cybersecurity policies and also introduced entirely new concepts.

For example, less than one month after the 9/11 terrorist attacks, Bush signed EO 13228, which established the Office of Homeland Security and the Homeland Security Council. EO 13228 tasked the Office of Homeland Security to develop and coordinate a national strategy to protect the US from terrorist threats and attacks. The resulting document, the National Strategy for Homeland Security, was released in July 2002 and argued in favor of creating a DHS to unify the US government's efforts to protect the homeland — to include critical infrastructure — from physical and cyber threats. As part of its critical infrastructure responsibilities, the DHS was called on to coordinate the development of a national plan for protecting US critical infrastructure.

Echoing the sentiments of the National Strategy for Homeland Security, Bush signed into law the Homeland Security Act on Nov. 25, 2002. The bill established the DHS as an executive-level department within the US federal government and assigned it the majority of the responsibilities called for in the National Strategy for Homeland Security, including the protection of critical infrastructure from all physical and cyber threats. Among its other activities, the DHS was instructed to develop a comprehensive national plan for securing critical infrastructure, to establish procedures for sharing critical infrastructure information, and to coordinate activities between the Intelligence Community, the private sector, and the various levels of the US government.

A little more than a year after the signing of the Homeland Security Act of 2002, the Bush administration signed Homeland Security Presidential Directive 7 (HSPD-7). This directive replaced PDD-63 as the US's guiding policy document for critical infrastructure cybersecurity and codified many of the roles and responsibilities assigned to the DHS in the National Strategy for Homeland Security and the Homeland Security Act of 2002. HSPD-7 called on the DHS to identify, prioritize, and coordinate critical infrastructure protection activities; create a National Infrastructure Protection Plan; and support the development and maintenance of sector-coordinating mechanisms and sector-specific ISACs. In addition, HSPD-7 increased the number of critical infrastructure sectors first listed in PDD-63 and replaced the concept of "lead agencies" with Sector-Specific Agencies. Each of the Sector-Specific Agencies was in turn instructed to develop a Sector Specific Plan with input from their sector's stakeholders.

With the DHS established as the focal point of the US government's cybersecurity critical infrastructure protection efforts, it began work with its public and private sector partners to develop the first National Infrastructure Protection Plan, which was released to the public in June 2006. The 2006 National Infrastructure Protection Plan delineated roles and responsibilities for the DHS and its security partners related to critical infrastructure protection. In addition, the document created Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and a Critical Infrastructure Protection Advisory Council (CIPAC) as a forum for public and private sector entities to meet and discuss important and evolving cybersecurity policies in the US. The SCCs, GCCs, and CIPAC would later play a key role as each of the Sector-Specific Agencies worked with their public and private sector stakeholders to develop their respective Sector-Specific Plan for critical infrastructure protection. The first Sector-Specific Plans were released to the public in 2007 and have been periodically updated to coincide with updates to the National Infrastructure Protection Plan.

Photo: Andrew Harrer/Bloomberg/Getty Images

The Department of Homeland Security has become the focal point of US critical infrastructure protection efforts.

The Bush administration's policy for critical infrastructure cybersecurity is best remembered for creating a more centralized organizational structure for critical infrastructure protection with the DHS at the center of all efforts in this area and for creating a detailed, national strategy for increasing the cybersecurity of critical infrastructure under the 2006 National Infrastructure Protection Plan. These efforts built upon the framework left behind by the Clinton administration and provided the Obama administration with an important launching point as it tried to address the increasingly sophisticated and persistent nature of cybersecurity threats to US critical infrastructure.

The Obama Administration & Innovation to Address Increasingly Sophisticated Cyber Threats

President Obama began his presidency in 2009 during a period in which cyberattacks were beginning to grow in sophistication and frequency. Russia's use of cyberattacks when invading Georgia in August 2008, the discovery of malware on the Department of Defense's (DOD) classified networks in October 2008, and China's hacking of the Obama and McCain campaigns during the 2008 US presidential election all had an important impact on the Obama administration's cybersecurity policy going forward. These events led Obama to state during his first months in office that US digital infrastructure was a "strategic national asset" and that "protecting this infrastructure will be a national security priority." The critical infrastructure cybersecurity policies developed by the Obama administration — from the 2009 National Infrastructure Protection Plan to current efforts to imitate private sector bug bounty programs — have sought to address the increasingly sophisticated and persistent nature of cyberattacks.

Shortly after coming to office in 2009, the Obama administration released an updated version of the National Infrastructure Protection Plan. Two important changes stand out. First, while the 2006 plan focused almost exclusively on critical infrastructure protection, the 2009 updated version gave equal importance to critical infrastructure resilience. Its emphasis on resiliency recognized the increasingly pervasive nature of cyberattacks, which had transitioned from a *possible* scenario to a *likely* scenario. The increased likelihood of cyberattacks meant that critical infrastructure security partners needed to develop plans for responding to and recovering from a cyberattack. Second, recognizing the interdependencies between critical infrastructure sectors and the importance of sharing information across sectors, the 2009 National Infrastructure Protection Plan also increased the US government's focus on cross-sector coordination. This was achieved by creating four new coordinating mechanisms to complement the SCCs, GCCs and CIPAC — the Critical Infrastructure Cross-Sector Council; the Federal Senior Leadership Council; the State, Local, Tribal, and Territorial Government Coordinating Council; and the Regional Consortium Coordinating Council. These new coordinating mechanisms sought to encourage greater participation by the various public and private sector entities involved in critical infrastructure protection.

Cyber Threat Intelligence Information Sharing & Voluntary Standards for Cybersecurity

From 2009 to 2013, the severity of cyberattacks on US critical infrastructure continued to increase. Most notable among them were Iranian cyberattacks on the US financial sector and Chinese cyberattacks on the US Defense Industrial Base. In light of these events, the Obama administration sought to develop a deeper partnership between industry and government on critical infrastructure cybersecurity. As part of this effort, Obama signed EO 13636 and Presidential Policy Directive 21 (PPD-21) in February 2013. The Obama administration also released the latest version of its National Infrastructure Protection Plan in January 2014.

EO 13636 sought to create deeper partnerships between industry and government in information sharing and standards development for critical infrastructure cybersecurity. It expanded the scope of information sharing to allow for the rapid flow of cyber threat intelligence — to include classified intelligence — from the US government to private industry. In addition, EO 13636 called on the Department of Commerce's National Institute of Standards and Technology (NIST) to work with the public and private sector to create a framework of standards, methodologies, procedures, and processes to help critical infrastructure owners and operators reduce cyber risks. This effort resulted in the NIST Cybersecurity Framework, a voluntary, risk-based framework that is widely-considered flexible, repeatable, and cost-effective.

PPD-21 became the guiding document for critical infrastructure cybersecurity during the Obama administration, replacing HSPD-7 of the Bush Administration. PPD-21 brought three important, new aspects to US policy for critical infrastructure cybersecurity. First, PPD-21 specifically identified the Energy and Communication Sectors as "uniquely critical due to the enabling functions they provide". Second, it expanded the scope of information sharing to include the dissemination of unclassified and classified cyber threat information from the federal government to the private sector. Finally, it called on the DHS to create

Photo: The White House

President Barack Obama tours the National Cybersecurity and Communications Integration Center.

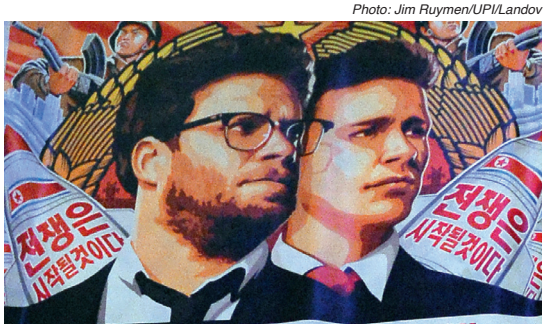
and operate a national center for cyber infrastructure that allows critical infrastructure security partners to obtain cyber threat intelligence and analysis. This ultimately led to the creation of the DHS National Cybersecurity and Communications Integration Center (NCCIC), which would later become the focal point for all critical infrastructure cyber threat information sharing between the US government and the private sector.

The DHS publicly released the 2013 National Infrastructure Protection Plan in January 2014. This newest version of the plan continued to stress the importance of cross-sector coordination and maintained the 2009 version's emphasis on critical infrastructure resiliency. However, it replaced the past two versions' focus on critical infrastructure protection with a new emphasis on critical infrastructure security, both cyber and physical. The 2013 version went further still in recommending new approaches for improving critical infrastructure cybersecurity that align with EO 13636 and PPD-21, such as promoting greater public-private cyber threat information sharing and increased use of the NIST Cybersecurity Framework.

Cross-Sector Information Sharing & Greater Private Sector Participation

From 2013 to 2015, the US experienced numerous sophisticated, high-profile cyberattacks, such as the December 2013 data breach at US retailer Target and the November 2014 cyberattack on Sony Pictures Entertainment. In light of these events, the Obama administration took additional steps to enhance cybersecurity by widening the scope of information-sharing activities and increasing the amount of cross-sector

Photo: Jim Ruymen/UPI/Landov



North Korea hacked Sony Pictures Entertainment to protest the release of the movie "The Interview".

Photo: Jim Wilson/The New York Times

President Barack Obama signs Executive Order 13691 at Stanford University.

collaboration. This was achieved through EO 13691 and the Cybersecurity Act of 2015.

Issued in February 2015, EO 13691 instructed the DHS to encourage the creation of Information Sharing and Analysis Organizations (ISAOs). Like ISACs, ISAOs are intended to facilitate the sharing of cyber threat information among its members and with the DHS's NCCIC. Unlike ISACs, however, which tend be sector-specific, the ISAO membership base is intended to reach across various sectors of the US economy. Ideally, information sharing between the NCCIC and ISACs and between the NCCIC and ISAOs will create a comprehensive national network of information sharing that enhances cybersecurity for all entities that participate.

To encourage greater cyber threat information sharing between the NCCIC, ISACs, and ISAOs, Obama signed the Cybersecurity Act into law on Dec. 18, 2015. The Cybersecurity Act of 2015 provides legal protection from most civil, regulatory, and antitrust liabilities to private sector companies that share cyber threat information with the US federal government. However, private sector companies must meet a number of criteria to receive these liability protections. For example, the private sector must remove non-relevant, personally identifiable information from the data they share and must use the DHS's NCCIC as the primary gateway for information sharing with the federal government.

Continuous Innovation in Critical Infrastructure Cybersecurity

As the Obama administration approaches its last few months in office, it continues to experiment with innovative ways to improve the cybersecurity of US critical infrastructure, such as the use of vetted, civilian, computer hackers as a low-cost, efficient way to discover and fix vulnerabilities in websites and connected devices.

In May 2016, the Obama administration completed the US government's first "bug bounty" program. Known as "Hack the Pentagon", the program allowed vetted computer hackers (frequently referred to as "white-hat" or "ethical" hackers) to test the DOD's websites for vulnerabilities. The vulnerabilities could then be reported to the DOD in exchange for money. The program is styled after the buy bounty programs of US companies like Yahoo, which pay $15,000 per vulnerability reported. The DOD's three-week program uncovered 138 previously unknown vulnerabilities and the DOD paid approximately $71,000 in total bounties to the ethical hackers participating in the program. Due to the success of this program, DOD and other federal agencies are expected to experiment with similar programs in the future.

Most recently, the Obama administration released Presidential Policy Directive 41 on July 26, 2016 to enhance the manner in which the US federal government responds to cyber incidents. PPD-41 clearly delineates the roles and responsibilities of all relevant government agencies when responding to a cyber incident. Once implemented, it will create a Cyber Response Group (CRG) within the National Security Council to coordinate US government policy and strategy regarding significant cyber incidents or attacks against the US. In turn, the CRG will be able to convene Cyber Unified Coordination Groups on an *ad hoc* basis to oversee the execution of response and recovery efforts.

Outlook for Future of US Cybersecurity Policy

Given the constantly evolving nature of the cyber threat, no single policy document or private sector technology will be able to protect US critical infrastructure from cyberattack. Rather, the various iterations of the National Infrastructure Protection Plan and other policy documents that address critical infrastructure cybersecurity will need to be dynamic in nature. Just as the Bush and Obama administrations made adjustments to the policies of their predecessors, subsequent US administrations will need to amend and build on policies from the past 20 years. Depending on the outcome of the 2016 presidential election, US policy for critical infrastructure cybersecurity will either experience gradual evolution — as it has over the last 20 years — or wholesale change.

Democratic Presidential Candidate Hillary Clinton would likely continue to build on many of the policies developed over the past 20 years given her close links to both the Clinton administration (as First Lady) and the Obama administration (as Secretary of State), as well as her voting history as a US Senator from New York (e.g., she voted in favor of the Homeland Security Act of 2002). While there are very few specifics regarding her cybersecurity platform, she has gone on record to criticize the Cybersecurity Act of 2015 for not doing enough to stop foreign hackers and to promise to make China "play by the rules" in cyberspace, suggesting an approach that would be slightly more aggressive than that of her predecessors.

While Clinton would likely represent a policy of gradual evolution, it is very possible that Donald Trump would take critical infrastructure cybersecurity policy in a totally new direction. Statements made by Trump and the text of the official Republican Party platform suggest that a Trump administration would increase the role of and funding for the DOD in critical infrastructure cybersecurity, explore the possibility of a free market for cyber insurance, pursue a more aggressive deterrence strategy, and even provide critical infrastructure owners and operators the right to self-defense (i.e. the right to "hack back" after a cyberattack).

Regardless of the outcome of the November election, US policy for cybersecurity will see major changes over the coming years as the next administration will likely face an increasing number of sophisticated adversaries in cyberspace. JS

Joshua Marciano is an analyst, Space and Defense, at International Technology and Trade Associates, Inc. (ITTA), a consulting company in Washington, DC.