National Cybersecurity Strategy

Branden Barnes

CYSE 525 Cyber Strategy and Policy

Professor Demirel

November 5, 2023

General Review

The United States strives to be the best digitally equipped ecosystem. It fosters inclusivity, equity, prosperity, and security to our nation and its allies. With the imaginative, ever-changing "Internet of Things" (IOT) a balance in dynamics amongst the digital globe, must be defended for the prosperity of a global collaboration for a digital future. Achieving this vision, requires cyber defenders assigned with safeguarding our constitutional values proposed by the Declaration for the Future of the Internet (DFI) and our human rights guarded by the Freedom Online Coalition (FOC). Such safeguard proposes a defensible foundation for which to protect. That denotes, a path to resilience sought out by a "collaboration around five pillars: (1) Defend Critical Infrastructure, (2) Disrupt and Dismantle Threat Actors, (3) Shape Market Forces to Drive Security and Resilience, (4) Invest in a Resilient Future, and (5) Forge International Partnerships to Pursue Shared Goals" (The White House, 2023). This structure only works with a smooth transfer of responsibility between stakeholders, involving the public sector, private industry, civil society, and international allies and partners. Users of this digital ecosystem today should not have to bear an immense responsibility of national security for their resources cannot thwart foreign adversaries. The "government's role is to protect its own systems; to ensure private entities, particularly critical infrastructure, are protecting their systems; and to carry out core governmental functions such as engaging in diplomacy, collecting intelligence, imposing economic costs, enforcing the law, and conducting disruptive actions to counter cyber threats" (The White House, 2023). An important aspect of a maturing defense system is the ability to build upon existing policy. The Biden-Harris administration adopted leadership positions to improve our cybersecurity against Russia. A foundation built by "appointing experienced, senior leaders in new positions at the National Security Council (NSC) and the Office of National

Cyber Director (ONCD) and moved quickly to fold lessons learned from these and other incidents into executive actions" (The White House, 2023). The National Cybersecurity Strategy March 2023 replaces the 2018 National Cyber Strategy, yet it sustains progress on numerous objectives, such as the collective defense of the digital ecosystem. To achieve security of the digital ecosystem, the National Cybersecurity Strategy builds upon and implements many private and civil sectors. The National Security Strategy and National Defense Strategy, implementations are as follows:

> Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," National Security Memorandum (NSM) 5, "Improving Cybersecurity for Critical Infrastructure Control Systems," NSM 8, "Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems,… EO 14017, "America's Supply Chains."… Space Policy Directive 5, "Cybersecurity Principles for Space Systems."… EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," EO 13691, "Promoting Private Sector Cybersecurity Information Sharing," and EO 13636, "Improving Critical Infrastructure Cybersecurity," and fit within the frameworks established by Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," and Presidential Policy Directive 41, "United States Cyber Incident Coordination." (The White House, 2023)

The strategic approach of the five pillars will enable the United States and its allies/partners to collaboratively develop the digital ecosystem, rendering it effortlessly defensible, resilient, and in alignment with our values. By the conclusion of this decade, the aim is to attain such results in the vanguard of technical development. The five pillars empower a bold embracement of a digitally enabled future for all (The White House, 2023).

Pillar One: Defend Critical Infrastructure

Reviewing pillar one from the National Cybersecurity Strategy March 2023, centers on a vital aspect of defense. A robust defense targets our critical infrastructure, ensuring adequate national security, public safety, and economic prosperity. Pillar One's collaborative defense model establishes cybersecurity requirements to support national security and public safety. It scales public and private collaboration, integrates federal cybersecurity centers, updates federal incident response plans and processes, and promotes the modernization of federal defense.

Collaboration being the focal point of this model advocates the sharing of responsibility and an informative synergy between stakeholders, owners and operators of critical infrastructure, and Federal agencies. "When incidents occur, Federal response efforts must be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners" (The White House, 2023). With the support of the Federal Government, our critical infrastructure can become more secure by firstly concentrating on its own systems. To provide a more defensible and resilient environment, "improving Federal cybersecurity through long-term efforts to implement a zero-trust architecture strategy and modernize IT and OT infrastructure. In doing so, Federal cybersecurity can be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems" (The White House, 2023).

Establishing Cybersecurity Requirements

The Federal Government will leverage its existing authorities to establish essential cybersecurity requirements within critical sectors. Regulations will work with proven frameworks like, Cybersecurity and Infrastructure Security Agency (CISA)'s and the National Institute of Standards and Technology (NIST) "to drive the adoption of secure-by-design principles,

prioritize the availability of essential services, and ensure that systems are designed to fail safely and recover quickly" (The White House, 2023). By implementing these regulations effectively, organizations wield an ability to follow compliances whilst integrating standards seamlessly into their cost benefit analysis (CBA). Allowing regulatory harmonization with investing into standards of protection, provides an affordable security that incentivizes infrastructures to develop regulatory frameworks without marginal costs. This in turn, impacts competition of under bidding policies, granting a "level playing field" amongst companies while simultaneously providing proper cybersecurity.

Defense of Critical Infrastructure

The Federal Government must integrate cybersecurity centers to support the defense of critical infrastructure. For example, the Joint Cyber Defense Collaborative (JCDC) program was established to assist cyber defense planning. This allows the National Cyber Investigative Joint Task Force (NCIJTF) to have more focus on law enforcement. Subsequently, the Cyber Threat Intelligence Integration Center's (CTIIC) can then apply more focus on intelligence collection, studies, and partnerships. At the top of the hierarchy, "the Office of the National Cyber Director (ONCD) will lead the Administration's efforts to enhance the integration of centers such as these, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale" (The White House, 2023).

Federal Defenses

Secure and resilient information, communications, operational technology, and services to carry out responsibilities is to be requisite for the Federal Government to wield adequate defense. This administration put forth EO 14028, "Improving the Nation's Cybersecurity" in contingency with

NSM 8, “Improving the Cybersecurity of National Security, the Defense Department, and Intelligence Community Systems” to support the zero-trust strategy. “The OMB zero trust architecture strategy directs FCEB agencies to implement multi-factor authentication, encrypt their data, gain visibility into their entire attack surface, manage authorization and access, and adopt cloud security tools” (The White House, 2023). With the modernization of Federal systems, security and resilience of cybersecurity triumphs the old legacy architecture. Moreover, to uphold the requisite posture of a zero-trust architecture strategy, cloud-based services will be further integrated over outdated functions. This intern provides higher standards of risk mitigation to American national security.

References

The White House. (2023, March). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf