Liam Clement

Professor Malik Gladden

CYSE 425W, Spring 2024

Old Dominion University

3/17/2024

In 2023, the United States White House released a revision to the National Cybersecurity Strategy. The March 2023 revision to the National Cybersecurity Strategy was precluded by the effects of the 2019 COVID-SARS pandemic. In response to the surge in remote networking for enterprise and personal use as a result of the pandemic, the Biden Administration, through the Bipartisan Infrastructure Law, invested “$65 billion” to ensure consistent and convenient access to stable, reliable, high-speed internet access. In combination with this, the Biden administration revised the United States National Cybersecurity Strategy to better reflect the necessary approach that the administration would need to take to ensure the protection of American citizens and interests in cyberspace in response to the shift caused by the Bipartisan Infrastructure Law.

The Biden administration holds several predictions that drive their decisions within the March 2023 revision, as well as internal policies that drove the signing of the Bipartisan Infrastructure Law. These predictions include a maturing Internet-of-Things (IoT) landscape, “comprising everything from consumer goods to digitized industrial controls to constellations of satellites.” Because of this, the Biden administration expects a significant shift in the potential vulnerable attack surfaces and the expected level of infrastructure critical to the safety of American citizens.

The Biden administration understands and holds that at the time of the writing of the march 2023 revision of the National Cybersecurity Strategy, the proverbial ball is in the court of offensive, malicious actors that current American cyber-defense specialists engage in cyber-conflict with every day. This is partially due to the state of American Cyberdefense and presence in cyberspace being a proverbial chain with far more links than should be necessary, with too much reliance on a vast number of small, local, community, and state level organizations. These small actors are too numerous and often too poorly equipped to counteract against national cyber-attackers, with each individual actor being a potential weakest-link in the chain necessary to ensure that National Cybersecurity Strategy objectives and goals are met. In order to counteract this, and in expectation of the expected shifting priorities and circumstances that define the nature of cyberspace and its actors, the Biden administration intends to create a National Cybersecurity Strategy that shifts the advantage from the attackers to the position of the defenders, partially by shifting the responsibility of cyberdefense of critical assets and infrastructure away from a vast army of individual, small-level agents and small businesses to national-level centralized authorities.

In addition to centralizing and increasing the overall power of authorities within the United States cyberspace environment to defend critical infrastructure, the Biden Administration also intends to focus on a policy of long-term investment within cyber-defense. The Administration holds that, although short-term benefits focused on ensuring continuity of operations and resilience of the defensive landscape are important to ensuring the protection of critical assets and infrastructure, long-term investments must be made for the sake of creating a “future digital ecosystem that is more inherently defensible and resilient.”

Finally, the Biden Administration intends to build the current revision of the United States National Cybersecurity Strategy upon prior-existing infrastructure and laws. To these ends, the United States National Cybersecurity Strategy's March 2023 revision is made up of five pillars; defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals. Each of these five pillars make up a small part of a comprehensive plan to ensure the security of the United States in cyberspace.

The overarching goals of the March 2023 revision of the United States National Cybersecurity Strategy are a highly comprehensive set, but have several caveats that must be considered. First and foremost is the ramifications of the Administration's intent to move the authority of defense from state and local level authorities to centralized, federal level authorities. Although this goal would remedy the danger of incompetent or unprepared low-level authorities endangering critical infrastructure, it calls into question the ability of the Federal government itself to ensure these same protections this act seeks to ensure. In the event that the Federal government finds itself unable to ensure these protections, state and local governments will find their own cybersecurity protections nullified, and their own citizens unprotected. Next, the Administration's goals of establishing long-term investments in cybersecurity infrastructure is a very well-designed policy, but will require a very fine balance of resources to assure protection of currently critical assets. Failing to protect the infrastructure of today could potentially endanger the potential infrastructure of tomorrow. Finally, the intention to establish cybersecurity infrastructure using previously established policy is a comprehensive and well-designed policy. The United States has a longstanding set of policies that have ensured protection against significant cyber-threats in the past, and while these policies are insufficient by themselves to

assure protection in the future, removal of these policies and rebuilding of policy from the ground up endangers the ability of current authorities to quickly respond to imminent threats.

Each pillar of the United States National Cybersecurity Strategy is composed of several sub-goals that contribute to the stated end-goal of the National Cybersecurity Strategy. For the purposes of this paper, this author will focus entirely on the first pillar and its stated sub-goals; defend critical infrastructure. This pillar is a tantamount one in almost every cybersecurity policy and strategy. The Biden Administration holds the ideal that collaboration between powerful, centralized authorities is necessary to defend against advanced persistent threats that are posed by nationally-backed cyber attackers and highly-organized cybercriminals. However, this collaborative effort can only occur if the " owners and operators of critical infrastructure" have cyber-defensive protections implemented to ensure the cyber-environment necessary for this collaboration to occur without disruption. To this end, the Biden Administration has begun to establish new guidelines and requirements for multiple critical sectors to follow for the purpose of cybersecurity. Additionally, the Administration intends to require new authorities to establish similar cybersecurity requirements of their own within other sectors. Furthermore, the Administration has begun to engage with current leaders within specific sectors for dialogues "to construct consistent, predictable regulatory frameworks for cybersecurity," pursuant of the goals the Administration seeks to achieve with the National Cybersecurity Strategy.

The Administration notes that public-private partnerships and collaboration within the field of cybersecurity have ensured significant gains in the past years, notably mentioning the "Shields Up" campaign that preceded the 2022 Russo-Ukrainian invasion. In note of this, the Administration intends to create similar campaigns of even greater scale, as well as foster channels and capabilities by which public, private, federal, and local entities operating within the

United States's cyber-defensive environment may "effectively collaborate with each other at speed and scale."

Finally, the Administration seeks to improve the resilience of American cyber-infrastructure by implementing a "zero trust architecture strategy and [modernizing] IT and OT infrastructure." Through this, the Administration believes that it can create a model for local and state level infrastructure through the method by which it establishes cyber defense within federal level infrastructure.

This pillar of the National Cybersecurity Strategy is a highly comprehensive one. Public-private partnerships and collaborations between the United States Federal Government and the private actors within the cybersecurity sector stands to greatly benefit the ability of the United States to quickly and effectively innovate in the face of new threats and undetected vulnerabilities. By capitalizing on this capability, the Biden Administration stands to have the greatest chance of vastly improving existing architecture and infrastructure in the shortest amount of time. Additionally, by opening channels for rapid collaboration, the United States government may foster similar, rapid developments as the ability to develop them arises, as opposed to only incentivizing them during crises. Finally, the investment into creating more resiliency within currently existing infrastructure is a highly necessary step in ensuring that the current infrastructure of the United States is properly protected.