National Cybersecurity Strategy

Ethan Lasich

Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Professor Bora Aslan

12 October 2025

In March of 2023, the Biden administration and the White House put forth a new plan for how the US should defend and respond to modern cybersecurity threats, called the National Cybersecurity Strategy. As more critical infrastructure becomes digitized and software becomes more complex, cybersecurity has become a more serious issue with new threats emerging every day. The National Cybersecurity strategy aims to promote a secure digital ecosystem by incentivising safer practices in business, and shifting the responsibility of cyber attacks more towards platform owners and threat actors, rather than individuals who don't have the resources to fully protect themselves. The strategy also has an interesting organization structure, focusing on five main pillars, which are defending critical infrastructure, disrupting threat actors, shaping market forces, investing in long term resilience, and finally creating international partnerships. In theory, it will position cybersecurity as a priority in our country and put us on a path to stronger digital security and build more resilience to cyberattacks in a more interconnected world.

One major shift in policy with the new strategy is that it aims to redirect the burden of cyberattacks from individual users onto vendors who sell insecure products. Most large corporations require users to accept licensing agreements before using the products and within these lengthy documents are clauses that protect the companies from legal consequences if the customer suffers any losses or damages, even if it was a result of the product being insecure. With this shift, it means “the administration will work with Congress and the private sector to prevent companies from being shielded from liability claims over the security of their products.” (Forno, 2023). If new laws are passed in accordance with the strategy, not only will this lift the responsibility for cybersecurity from individual consumers, but it will also encourage corporations to invest most in their security as they could be held more accountable to cyber risks in their products.

Another important point in the National Cybersecurity Strategy recognizes that our technological defenses are not enough to protect critical infrastructure and data of corporations and governments, and calls for an increase in education and training to find workers skilled enough to get into the cybersecurity field. On top of growing the cybersecurity workforce, it also focuses on promoting stronger security practices in technical products, and on page 5 of the document, it says to “embrace security and resilience by design,” as opposed to creating a patch every time a vulnerability is found. By finding skilled professionals and incentivising stronger security standards, these initiatives can help to proactively strengthen our nation’s cyber defenses by mitigating risks before they can be exploited.

Finally, the strategy identifies that some foreign countries also pose a major risk to not only cyberspace, but also our national security and economy. The strategy actually lists four governments as direct threats to the nation, those being China, Russia, Iran, and North Korea. It claims these countries are sophisticated enough and are willing to conduct cyber attacks on the United States, and even directly blames Russia for the NotPetya attack in 2017. It makes it clear that state-backed threats pose a significant risk and uses this information as justification to work with international allies in order to share intelligence, promote cyberspace norms, and also disrupt malicious activities from these adversaries.

The National Cybersecurity Strategy organizes its objectives into five pillars and the one that stands out to me the most is the first one, which is to defend critical infrastructure. Critical infrastructure can be defined as any physical or digital systems that are essential to the functioning of society. Our country's infrastructure has been slowly becoming more and more interconnected and digitized, raising the risk of damage if things like water systems, healthcare networks, and power grid are compromised. In fact, one research article found that “even if attackers are only able to control a small fraction of the power connected to the grid, they can still leverage mechanisms inherent to today's large power grids to cause considerable damage." (Krause et al, 2021). Because of these threats, the first pillar puts a heavy emphasis on protecting these systems from cyberthreats and making sure they can still operate in the event that they come under attack.

One thing the administration pushes for in the new strategy is to put new cybersecurity requirements and regulations in place for certain critical sectors, adding more protection against adversaries who wish to disrupt them. The new standards aim to ensure that these sectors have consistent levels of security regardless of their size. They are also promoting collaborative efforts between public and private sectors to protect against adversaries, which will help with coordinating incident response and unifying defense strategies. Also within the goals for this pillar is the advocacy of making the Federal Government's own systems more resilient to cyber attack, citing specific strategies such as implementing a zero trust architecture and modernizing the infrastructure of their IT and OT systems, creating a model for how to properly build secure and resilient systems.

Regarding the establishment of regulations to better secure infrastructure, the strategy recognizes that there are gaps in the authority of the federal government to set minimum requirements and mitigate the failures of certain markets. One of the things the administration wants to do is close those gaps by working with congress, and also push for state governments to also set up cyber requirements. They want new regulations to be based on existing cybersecurity frameworks and guidances, such as CISA's Cybersecurity Performance Goals and also the NIST Framework for Improving Critical Infrastructure Cybersecurity. New regulations should define minimum standards like using secure-by-design principles and implementing fail safes, however it’s also stated that the administration encourages and supports going beyond the minimum requirements to further improve the resilience of our critical infrastructure. For smaller entities that cannot easily afford to implement new regulations, the government encourages regulators to set up incentives for these investments, such as changing tax structures and rate-making processes.

Outside of new regulations and improving collaboration efforts, the 2023 National Cybersecurity Strategy also wishes to update federal incident response plans, making it easier for private sector partners facing security incidents to reach the federal government, and improving what kind of support they can provide. The strategy says the CISA will lead a process to update the National Incident Response Plan, which would strengthen processes and improve coordination between Federal agencies. The document also cites the recent Cyber Incident Reporting for Critical Infrastructure Act of 2022, explaining how it shortened the time frame for reporting incidents, requiring entities within critical infrastructure sectors to report incidents to CISA within hours. These more timely requirements allow information about the breach to be shared faster, enabling quicker coordination between the government and private organizations to contain threats and prevent any further damage.

Finally, the federal government also wants to modernize their own defenses, emphasizing the need to replace any systems that lack defenses for sophisticated cyber attacks, and listing many goals for a zero trust architecture, such as multi-factor authentication, encryption, authorization and access management, and also improving cloud security. With outdated IT and OT systems still in the government, these goals are difficult to achieve, highlighting the urgent need as to why the federal government wants to modernize and reduce any vulnerabilities that can be exploited in their systems. Lastly, the strategy also recognizes the importance of their national security systems and the nation state adversaries that pose a threat to them, and calls for a coordinated plan to be developed by the NSA and OMB to ensure strong cybersecurity requirements for these critical systems.

In conclusion, the 2023 National Cybersecurity Strategy is a major step in how the US government seeks to approach cybersecurity and the nation's digital defenses for the future. By investing in a cyberspace workforce, strengthening the collaboration of public and private sectors, and shifting the responsibility attacks from individual to software vendors, it creates a foundation for a more secure cyber ecosystem. The first pillar’s focus on defending critical infrastructure also demonstrates the importance of cybersecurity within our society and how it’s connected with national security, and the goals it puts forth create a strong path for progress. If the strategy can be carried out successfully, it can help not only the government, but also private business and infrastructure sectors be more prepared to defend and respond to cyber attacks.

References

Forno, R. (2023, March 20). *Thoughts on the Biden national cybersecurity strategy*. Stanford Center for Internet and Society. https://cyberlaw.stanford.edu/blog/2023/03/thoughts-biden-national-cybersecurity-strategy/

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors (Basel, Switzerland), 21(18), 6225. https://doi.org/10.3390/s21186225

U.S. White House. (2023, March 1). *National cybersecurity strategy*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf