National Cybersecurity Strategy Review: Focusing on Defending Critical Infrastructure

Akela Villegas

Old Dominion University School of Cybersecurity

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 28, 2025

Abstract

This paper outlines a proactive plan to strengthen the United States' digital defenses and shift cybersecurity responsibilities towards those who are best equipped to manage the risks. The paper provides a general overview of the strategy's goals, including securing infrastructure, enhancing resilience, and promoting cooperation. It then focuses on the first strategy out of the five pillars, which is defending critical infrastructure. This pillar addresses the urgent need to protect essential sectors like healthcare, transportation, and energy from cyber threats through regulatory standards, public and private collaboration, and effective risk management. The analysis highlights the strategy's strengths, challenges, and potential impact, emphasizing the importance of coordinating implementation to achieve lasting cybersecurity resilience.

General Review

The National Cybersecurity Strategy, released in March 2023 by the Biden Administration, presents a bold and comprehensive plan for securing the United States' digital landscape while also mitigating cyber threats. This strategy recognizes that cybersecurity is not just a technical problem; it is also a national security issue that affects everyone. In today's world, where so much of our daily lives and national systems rely on technology, cyberattacks have become more dangerous and more common. Society is so reliant on technology and critical infrastructure, making this strategy's efforts even more important. It reflects a significant shift and takes a big step forward in making cybersecurity a shared responsibility. It moves the responsibility of cybersecurity away from everyday citizens and small organizations and places it on larger companies and groups that have the tools and resources to better manage cyber risks. In the past, individuals, small businesses, and local governments often had to deal with security

issues on their own. Sadly, many of these groups do not have the resources, expertise, or funding to defend against serious cyber attacks and threats.

The strategy is built around five main pillars:

1. Defend critical infrastructure
2. Disrupt and dismantle cyber threat actors
3. Shape market forces to drive better security
4. Invest in a more secure and resilient future
5. Build international partnerships to pursue shared goals

These pillars work together to ensure that not only are we reacting to cyber threats but also preparing for and preventing them whenever possible.

What's especially important is how this strategy connects cybersecurity to bigger national goals. It is not just about stopping hackers, but also about protecting the progress we have made in rebuilding infrastructure, developing clean energy, and bringing technology manufacturing back to the U.S. (White House, 2023). One of the biggest changes in this strategy is the push to hold software companies accountable when their products are not secure. In the past, users had to take all the responsibility for security. Now, the government is stating that the developers and manufacturers should share the burden, especially if they release products with known flaws (Vijayan, 2023). The strategy also emphasizes the importance of collaborating with international allies. Cyber threats do not stop at borders; therefore, working with other countries will be crucial in keeping systems safe. In short, the 2023 strategy is a strong response to the changing cyber landscape. It looks not only at short-term, but long-term needs as well. If it is implemented effectively, it could lead to a much more secure digital environment for everyone.

Focus on the First Pillar: Defending Critical Infrastructure

Of all the areas the strategy focuses on, the first is the most important. “Critical Infrastructure” refers to systems that we all depend on every day like water, hospitals, electricity, transportation, and communication networks. If these systems are attacked or go down, the consequences would be server, maybe even life-threatening.

This pillar calls for setting minimum cybersecurity requirements across industries that run critical infrastructure. In the past, many of these sectors followed voluntary guidelines, but that is not enough. One example is the Colonial Pipeline ransomware attack on May 7, 2021, which shows how vulnerable these systems can be. The attackers encrypted the data and demanded a ransom for its decryption. In order to prevent further damage and potential compromise, Colonial Pipeline proactively shut down its pipeline operations, which are responsible for transporting nearly half of the fuel used on the East Coast. The shutdown caused fuel shortages and panic buying in several states. Gas prices spiked, and some gas stations ran out of fuel. The pipeline began restarting on May 12, and full operations were restored within a few days. The attack highlighted the vulnerability of critical infrastructure to cyberattacks and underscored the need for improved cybersecurity practices. The government now wants to move forward toward rules and regulations that require companies in these sectors to meet basic cybersecurity standards (Kerner, 2022).

Another part is improving collaboration between the government and private companies. Many critical systems are owned and operated by private businesses, so teamwork is essential. For example, the Cybersecurity and Infrastructure Security Agency (CISA) helps share threat information quickly and responds to incidents. Programs like the Joint Cyber Defense Collaborative (JCDC) are designed to bring experts together to stop attacks before they cause

serious damage (CISA, 2023). The strategy also pushes for the modernization of government systems to lead by example which means using stronger security tools, better monitoring, and building networks that are secure. These changes will aid in reducing the risks and show private companies what strong cybersecurity looks like in action.

Importantly, the strategy talks about resilience, in other words, the ability to bounce back quickly after an attack. Even with strong defenses, some cyberattacks will get through. This is why it is critical to have a response plan in place for continuing operations, backing up data, and restoring services after a disruption.

The way the strategy looks at interconnected systems is very important. A cyberattack on one part of the infrastructure, like the power grid, could then affect other parts, like water systems and hospitals. Therefore, the strategy promotes a big picture view, encouraging different sectors to plan and prepare together; collaboration is key. Of course, putting all this into action will not be easy, especially because many critical infrastructure sectors are privately owned and operate under a tight budget. Some companies may resist stricter rules if compliance is complicated or costly, which is why the government needs to offer support and clear guidance.

References

CISA. (2023). *Cybersecurity and Infrastructure Security Agency Strategic Plan 2023–2025*. https://www.cisa.gov/sites/default/files/2025-01/FY2024 2026_Cybersecurity_Strategic_Plan508.pdf

Kerner, S. M. (2022, April 26). *Colonial pipeline hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained Everything-you-need-to-know

Vijayan, J. (2023, March 2). *Biden's cybersecurity strategy calls for software liability, tighter critical infrastructure security*. Dark Reading. https://www.darkreading.com/ics-ot security/bidens-cybersecurity-strategy-calls-for-software-liability-tighter-critical infastructure-security

White House. (2023). *National Cybersecurity Strategy*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National Cybersecurity-Strategy-2023.pdf