National Cybersecurity Strategy Midterm Assignment

Clarrissa Darden

Old Dominion University

CYSE425 Summer

National Cybersecurity Assessment

Upon analyzing the current 2026 National Cybersecurity strategy which is being used by the United States, has changed from the previous administration under Biden. It was determined that while both strategies focus on protecting the country from cyber threats, the 2026 strategy updates national priorities and reflects the current administration's approach. The focus from the Bidens administration which were organized around five pillars: defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces, investing in a resilient future, and forging international partnerships, Has changed to the Trump administration focus on "six pillars" (House, 2026) which are deterring cyber adversaries, reducing unnecessary regulations, protecting critical infrastructure, modernizing federal systems, strengthening the cybersecurity workforce, and maintaining American technological leadership.

Cybersecurity has become more important because every part of daily life depends on technology. This is why Trump's current strategy "calls for unprecedented coordination across government and the private sector to invest in the best technologies and continue world-class innovation, and to make the most of America's cyber capabilities for both offensive and defensive missions" (Trump, 2026). Hospitals, banks, schools, transportation systems, electric utilities, and government agencies all rely on computer networks. If those systems are attacked, millions of people can be affected. The strategy explains that the federal government, private companies, and state and local governments must work together to reduce cyber risks. The six pillars include shaping adversary behavior, promoting common-sense regulation, modernizing and securing federal networks, securing critical infrastructure, achieving American technological

dominance, and building the cyber workforce and operations. Together these pillars provide a roadmap for improving cybersecurity across the country.

One noticeable difference from the previous strategy is the increased emphasis on taking action against cybercriminals before they cause harm. The strategy also focuses on making government systems more secure, encouraging innovation, and ensuring that the United States remains a global technology leader. Although both strategies recognize the importance of partnerships with industry, the current strategy places greater attention on reducing unnecessary regulatory burdens while still improving security.

The new National Cyber Security Strategy is believed by the administration that "President Trump's leadership has created a new era in cyberspace" (House, 2026). I think creating incentives for the detection of threats will heighten awareness. I disagree with the approach on common sense regulations because all people's sense is not common, this changes too many areas and checklist that was established for a reason. Reducing these can and most likely will result in an overlooked threat that could possibly been caught had this not been in place. I do agree with the modernization of federal government networks, however I would not rely too much on AI. We have all seen movies where AI got too smart for its own good and shut down the government. I agree that securing the critical infrastructures is the most important of the pillars to me and must be done and consistently monitored. I also agree on building the talent through education of the next generation this is how we will sustain superiority in critical and emerging technologies.

Pillar Review: Secure Critical Infrastructure

I chose pillar #4 Secure Critical Infrastructure to review because it was one of the closets to the requested assignment that had Defending Critical Infrastructure. I also chose it because "Critical infrastructure remains an attractive target for malicious cyber actors." (Trump, 2026)

Pillar Four focuses on securing the nation's critical infrastructure. Critical infrastructure includes essential services such as electricity, water systems, hospitals, transportation, communications, banking, and emergency services. These systems are important because people rely on them every day. If cybercriminals successfully attack them, the impact could affect public safety, the economy, and national security.

Compared to the 2023 strategy, the current strategy continues to recognize the importance of protecting critical infrastructure but places additional emphasis on working with owners and operators while improving resilience against increasingly sophisticated attacks. The goal is to prevent attacks before they happen and to recover quickly if an attack occurs.

One important part of this pillar is information sharing. Government agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) work closely with private companies to provide threat intelligence, cybersecurity guidance, and incident response assistance “to defend against today’s threats and collaborate to build a more secure and resilient infrastructure for the future.” (Agency, n.d.) The National Institute of Standards and Technology (NIST) also provides cybersecurity best practices that organizations can use to strengthen their defenses (NIST, 2024).

This pillar also encourages organizations to improve network monitoring, regularly update software, use multi-factor authentication, train employees, and prepare incident response plans. These are practical steps that help reduce cyber risk.

I believe this pillar is one of the most important parts of the strategy because everyone depends on critical infrastructure every day. Most people do not think about cybersecurity when they turn on the lights, visit a hospital, or use online banking, but all of those services depend on secure computer systems. Protecting these systems protects the public as well.

In conclusion, the updated strategy builds on previous cybersecurity efforts while reflecting new national priorities. By strengthening partnerships, improving preparedness, and protecting critical infrastructure, the United States is better positioned to respond to modern cyber threats.

References

Agency, C. a. (n.d.). *About CISA*. Retrieved from America's Cyber Defense Agency: https://www.cisa.gov/about

House, T. W. (2026, March 6). *White House Unveils President Trump's Cyber Strategy for America*. Retrieved from The White House: https://www.whitehouse.gov/releases/2026/03/white-house-unveils-president-trumps-cyber-strategy-for-america/

NIST. (2024, February 26). Retrieved from Cybersecurity Framework: https://www.nist.gov/cyberframework/csf-11-five-functions

Trump, D. (2026, March). *President Trump's Cybersecurity Strategy*. Retrieved from The White house : Cybersecurity has become more important because nearly every part of daily life depends on technology. Hospitals, banks, schools, transportation systems, electric utilities, and government agencies all rely on computer networks. If those systems are attac