Erik C. Sorto

CYSE 425W

February 7, 2026

**Policy Analysis Paper 1: U.S. National Cybersecurity Strategy**

The Cybersecurity policy I selected for analysis is the United States National Cybersecurity Strategy, released by the White House in 2023. This strategy fits the current national approach towards cybersecurity and is in line with my experience during my time as a Cyber Risk intern at COVA CCI's Cyber Clinic internship here at ODU. Through that internship I saw how cybersecurity challenges have more governance, risk management and organizational decision-making roots than technical failures. Its national Cybersecurity Strategy reflects these realities by promoting shared responsibility, systemic resilience and coordinated National action.

This policy was strategically developed due to a response from a series of high profile cyber national cyber incidents which exposed structural weakness in both the public and private sector. Notable instances, like the company SolarWinds and it's supply chain being compromised by ransomware attacks and the company Log4j which faced colossal-scale vulnerabilities that only demonstrated how vulnerable a critical infrastructure could become, especially with fragmented cybersecurity practices. These incidents along with other proved how drastic and catastrophic cyber incidents can become regarding to public safety and national security. Therefore, as a result framed cybersecurity collectively as a risk management issue that had to be solved through a strategic policy that addressed it through policy, governance, and long-term investment rather than utilizing isolated technical solutions. (White House, 2023).

During my experience in my internship I worked with a small team that conducted vulnerability assessments for a municipality which only enforced the importance of being able to reference policies and standards. Smaller organizations struggle not only due to be poorly equipped with the right technology but more so due to having unclear accountability, inconsistent risk prioritization, and limited organizational readiness. The National Cybersecurity Strategy policy shifts the responsibility toward organizations that not only maintain digital systems but also deploy and design them. What would normally be placing the burdens on the users individually, the National Cybersecurity Strategy makes the argument that cybersecurity should be built into systems by

default which is an approach that aligns with risk-based assessments and governance recommendations found through clinic engagements.

The National Cybersecurity Strategy is based on five key pillars:

- Pillar One: Defend Critical Infrastructure
- Pillar Two: Disrupt and Dismantle Threat Actors
- Pillar Three: Shape Market Forces to Drive Security and Resilience
- Pillar Four: Invest in a Resilient Future
- Pillar Five: Forge International Partnerships to Pursue Shared Goals

Notably, this represents a shift in U.S. cybersecurity governance which recognizes people and small organizations can indeed handle complex cyber threats on their own accord (Dunn Cavelty & Wenger, 2022). This strategy not only encourages baseline security requirements, accountability for software vendors but most importantly it seeks to reduce systematic vulnerabilities widely spread across whole sectors rather than responding to incidents after the fact they occurred.

In practice, that National Cybersecurity Strategy is carried out by federal agencies, regulatory bodies and public/private partnerships. Organizational risk assessments, incident reporting and information sharing are critical agencies supporting the operationalization of the strategy, including agencies such as CISA. The strategy supports also existing frameworks such as the NIST Cybersecurity Framework that organizations use to identify, manage and communicate cyber risk. This flexible, consistent approach allows the strategy to be applied across environments including municipalities and public-sector organizations like those supported by COVA CCI (Shackelford et al., 2023).

Another strength is that the national cybersecurity Strategy recognizes Cybersecurity as a National risk that transcends organizations. Cyber threats increasingly operate below the threshold of traditional warfare but deliver strategic results. Such "gray zone" cyber activities, Kello (2017) argues require coordinated national responses instead of isolated technical defenses. That understanding reflects in the national cybersecurity Strategy which integrates Cybersecurity into National security planning and stresses resilience, continuity and governance.

Finally, the strategy is integrated within an overall national and international cybersecurity policy context. At the national level it primarily supplements, executive orders, as well as specific regulations and notably cybersecurity mandates. At an international level, it emphasizes the

benefit of working with allies to establish common grounds which also enhance the collective defense to counter malicious cyber activity by both state and non-state actors. By viewing cyberspace worldwide, it demonstrates how everyone is connected and the importance of following cybersecurity policy and how necessary it is to be transnational in nature. The U.S. National Cybersecurity Strategy is a strong and relevant policy as it provides a modern and realistic framework for addressing cyber threats.

**References:**

Dunn Cavelty, M., & Wenger, A. (2022). *Cybersecurity and the politics of security governance*. *Journal of Strategic Studies, 45*(4), 1–20.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Shackelford, S. J., Raymond, A., & Brady, J. (2023). *Cybersecurity governance and critical infrastructure protection*. *Journal of Cybersecurity, 9*(1), 1–14.

White House. (2023). *National cybersecurity strategy of the United States*. https://www.whitehouse.gov/briefing-room/strategic-communications/2023/03/02/national-cybersecurity-strategy/