National Cybersecurity Strategy Policy Analysis

Destiny Hale

CYSE 425W

Professor Aslan

March 8, 2026

## Introduction

All over the world, cyberattacks and threats occur, damaging critical infrastructures and digital assets that are crucial to how we operate in our daily lives. To address these growing threats and protect digital assets, governments have implemented policies to enhance cybersecurity resilience across various sectors. The National Cybersecurity Strategy policy serves as a structured blueprint for private sectors and governments to strengthen their cybersecurity practices against digital threats. Its primary goal is to protect various systems and digital infrastructures in sectors for long-term systemic resilience. The objective of this paper is to summarize the National Cybersecurity Strategy, outline its key pillars, and provide an in-depth analysis of the pillar on defending critical infrastructure.

## Policy Overview

According to Wiens (2023), the National Cybersecurity Strategy policy serves as a blueprint for federal governments on how they should respond to cybercrime-related issues and the roles the private sector should play in protecting national cybersecurity. In addition, it is a highly analyzed document that highlights current trends in national cybersecurity and provides guidelines for managing cyber policies across federal agencies and departments (Wiens, 2023). Before this was developed, its predecessors, such as those developed by Presidents Bush, Obama, and Trump, sought to "incentivize adequate and long-term investment in cybersecurity to combat current risks and mitigate future ones" (Jaikaran, 2023). However, this policy, developed by Biden, focuses on understanding threat actors, cybercrime, and reshaping the responsibilities in cyberspace. In order to accomplish these key objectives, this strategic policy is

built on five pillars, each focusing on a specific aspect of cybersecurity and strengthening national security.

The five pillars serve as the foundation of the strategy, establishing numerous approaches to mitigate cyber threats at different levels across sectors. A few approaches include: collaborating between the public and private sectors, harmonizing regulations, disrupting ransomware, etc (Jaikaran, 2023). The first pillar, Defend Critical Infrastructure, focuses on protecting critical systems and vital services from cyber attacks, ensuring they are resilient. The second pillar, Disrupt and Dismantle Threat Actors, involves implementing strategies and collaborating with other departments to fight against adversaries and cybercrime. The third pillar, Shape Market Forces To Drive Security and Resilience, involves implementing privacy requirements for data-driven systems, securing IoT devices, and shifting liability towards entities. The fourth pillar, Invest In A Resilient Future, prioritizes long-term investments and conducts research in securing emerging technology. Lastly, the fifth pillar, Forge International Partnerships To Pursue Shared Goals, focuses on global collaboration to build a "shared digital ecosystem that is more inherently resilient and defensible" (The White House, 2023).

Overall, the application of this policy emphasizes shared responsibilities through the collaboration of the public and private sectors and shifting accountability toward various organizations with critical infrastructures. According to Johnson & McAndrew (2023), this policy seeks to "rebalance responsibility for cybersecurity defense and realign incentives to make long-term investments that increase cyber resiliency". Through its five pillars, this reinforces the responsibilities set, enhancing protection, security, and accountability for the upcoming digital age and digital systems. As cyber threats continuously evolve, the application of this policy plays a huge role in protecting national security and public safety.

# Pillar Analysis: Defend Critical Infrastructure

Critical infrastructures and systems are crucial to how we operate in our daily lives. As the White House (2023) states, people must be able to trust and have confidence in the "availability and resilience of this infrastructure and the essential services it provides". Without the protection of these infrastructures, disruptions can lead to consequential effects, including threats to national security and public safety. Therefore, the defend critical infrastructure pillar is a key part of the National Cybersecurity Strategy, which governs policies and measures to maintain the reliability of these systems. This pillar includes 5 objectives, such as: (1.1) Establish Cybersecurity Requirements To Support National Security and Public Safety, (1.2) Scale Public-Private Collaboration, (1.3) Integrate Federal Cybersecurity Centers, (1.4) Update Federal Incident Response Plans and Processes, and (1.5) Modernize Federal Defense. All of these are essential approaches to guarding systems against cyber threats.

In the first objective, the White House (2023) highlights the lack of mandatory cybersecurity requirements, leading to inconsistent security outcomes and statutory authority gaps. The administration is aiming to leverage a regulatory shift for critical infrastructure sectors such as oil, natural gas, and aviation. It involves the harmonization of current and new regulations, the minimization of the requirements' burden, and the funding of incentivized investments. This closes the gap between federal expectations and sector execution. By transitioning to a "performance-based" framework, the strategy allows for industries to adapt. The second objective focuses on building "trust-based networks of networks" through collaboration of public and private sectors using enhanced technology to defend against adversaries in real time. For instance, Cybersecurity and Infrastructure Security Agency (CISA) and Sector Risk Management Agencies (SRMA) are collaborating to respond to the needs of

sectors and explore “technical and organizational mechanisms to enhance and evolve machine-to-machine sharing of data” (White House, 2023). Through this collaboration of agencies, this provides a shared vision of the framework and reshapes the digital landscape.

Building on the collaborative framework, the pillar also addresses the need to integrate federal cybersecurity centers (Objective 1.3). According to the White House (2023), these serve as collaborative nodes to bring together capabilities across numerous department missions. By aligning centralized coordination, information sharing, and operational defense planning, the federal government will be able to respond more effectively when cyber threats arise. As of now, the administration has been successful in this by establishing the collaboration of numerous departments, such as the Defense Industrial Base Collaborative Information Sharing Environment (DCISE) and the National Security Agency (NSA). This provides opportunities to enable sharing directly with private sectors in their respective sectors.

Additionally, to promote the growth of this vision, it includes updating federal incident response plans and processes (Objective 1.4). Just like the previous objective, federal departments must be able to present a coordinated response when private sectors need assistance in defending against cyber incidents. This would help them to contact the right agencies, which would lead to gaining support and access to information. To put this in action, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for the revision of the National Cyber Incident Response Plan (NCIRP) to strengthen and enhance information sharing. In addition, the Cyber Safety Review Board (CSRB) gives insight and recommendations for “improving the nation’s cybersecurity posture” (White House, 2023). By updating response plans and processes, this helps defenses and private sectors stay ahead of evolving threats. Lastly, to stay ahead of these threats, the government plans to modernize its defenses (Objective 1.5). The goal is to

implement a zero-trust architecture, which replaces outdated security systems that are incapable of keeping data safe. According to Claro (n.d.), these architectures use multi-factor authentication, data encryption, authentication/access management, and upgrading legacy systems. This sets the example for private sectors to adopt high-standard security measures to protect their systems, the public, and the nation. Overall, the objectives support the pillar's mission to defend the nation's most crucial systems.

## Conclusion

The National Cybersecurity Strategy policy serves as a blueprint and example for private sectors and federal government agencies to adopt cybersecurity practices into their systems and critical infrastructures. This policy emphasizes collaboration among agencies and departments, while maintaining adaptability and dynamic defense. As stated, its primary goal is to strengthen and protect various systems for long-term resilience. To achieve this goal, the five pillars focus on a specific aspect of cybersecurity, establishing numerous approaches to mitigate cyber threats at different levels. The most significant pillar of this strategy, Defend Critical Infrastructure, governs policies and measures to maintain the reliability of these systems. However, to maintain the reliability, its objectives focus on establishing cybersecurity requirements, collaboration among agencies, integrating federal cybersecurity centers, updating incident responses, and modernizing defenses. Overall, these support the mission to defend national infrastructures.

# References

Claro . (n.d.). *The 5 Pillars of the White House's 2023 Cyber Security Strategy*. Claro. Retrieved March 4, 2026, from https://www.usclaro.com/blog/the-5-pillars-of-the-white-houses-2023-cybersecurity-strategy

Jaikaran, C. (2023, July 17). *The National Cybersecurity Strategy—Going Where No Strategy Has Gone Before*. Congress.gov. https://www.congress.gov/crs-product/IN12123

Johnson, J. S., & McAndrew, E. J. (2023, March 10). *Key Takeaways from the US National Cybersecurity Strategy | BakerHostetler*. BakerHostetler. https://www.bakerlaw.com/insights/key-takeaways-from-the-us-national-cybersecurity-strategy/

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

Wiens, C. (2023, April 4). *What is the National Cybersecurity Strategy?* Mixmode. https://www.mixmode.ai/blog/what-is-the-national-cybersecurity-strategy