National Cybersecurity Strategy

March 1, 2023

Summary:

The National Cybersecurity Strategy (NCS), released in March 2023, addressed rebalancing responsibilities to defend cyberspace onto larger industry organizations and realigning incentives to favor long term investments. The cybersecurity strategy wants the following three goals to be met going forward.

- **Defensible: Cybersecurity should become easier, cheaper, and more effective**
- **Resilient: Cyber incidents should have little widespread or lasting impacts**
- **Values-Aligned: Digital world aligns with and reinforces our Nation's values**

The National Cybersecurity Strategy considers the following five "pillars" of cybersecurity essential to protect from constantly evolving threats.

Overview

The strategy was designed to be durable and last for a decade. The intention was to read as a cohesive document and not as a specific applicable section of implementation. The NCS, while it has "national" in its title, was written to be adapted by state and local governments. Cybersecurity can only be achieved with the influence of state and local governments and critical infrastructure. SLG and critical infrastructure can take the pillars and initiatives and apply them to their state or local specific counterpart of the federally responsible agency.

The NCS is accompanied by the National Cybersecurity Strategy Implementation Plan (NCSIP) was published and created to encourage federal cohesion and realizes the NCS. The NCISP is comprised of a list of 65 initiatives with an assigned responsible agency and due date for when the initiative should be complete. Each initiative is designed to help achieve the NCS. The ONCD published version 2 of the NCSIP on May 7, 2024 building the implementation plan following the completion of 33 initiatives. Version 2 displays new initiatives, carryover initiatives, and completed initiatives. The implementation plan is a living document and new initiatives will be added once the original initiatives are completed.

Federal agencies have different cyber strengths, weaknesses, and capabilities, which is why the implementation plan aims for regulatory **harmonization** of requirements to raise the cybersecurity baseline and find **reciprocity** when applicable. While the NCSIP was written for the federal government, it was designed for states to be adapted for their own agencies.

Pillar One: Defend Critical Infrastructure

Critical infrastructure is essential to the safety and security of American's daily lives, yet it is insufficiently protected from cyber threats. Critical infrastructure remains a top target for foreign and domestic threat actors. Loss in service provided or personal information collected from critical infrastructure could have dire consequences, which is why the NCS aims to increase the cyber posture and confidence of the American people in critical infrastructure. The government plans to achieve the goal of pillar one by:

- Expanding the use of minimum cybersecurity requirements in critical sectors
- Harmonizing and simplify regulations
- Enabling public and private collaboration for the defense of critical infrastructure and essential services
- Modernizing and updating Federal incident response policy

Pillar Two: Disrupt and Dismantle Threat Actors

Cyber threat actors threaten diplomatic, information, military, financial, intelligence, and law enforcement capabilities. Pillar 2 aims to stop the threat at the source and render threat actors incapable of conducting campaigns. This requires coordination between Federal and non-Federal actors to strengthen the ability to both disrupt and dismantle cyber threat actors. The government plans to achieve the goal of pillar one by:

- Strategically employing all tools of national power to disrupt adversaries
- Engaging the private sector in disruption activities through scalable mechanisms
- Addressing the ransomware threat through a Federal approach joined with international partners

PILLAR THREE: Shape Market Forces To Drive Security and Resilience

One of the primary goals of the National Cybersecurity Strategy is to create a shift of cyber responsibility away from the individual and small business and place it on the most capable organizations. Assigning the responsibility of protecting the digital ecosystem to industry, it provides the opportunity for garnering trust and increasing the likelihood of a secure and resilient future. Resilience requires protecting against today's threats while simultaneously preparing for the threats of tomorrow. The government plans to achieve the goal of pillar one by:

- Promoting privacy and the security of personal data
- Shifting liability for software products and services to promote secure development practices
- Ensuring that Federal grant programs promote investments in new infrastructure that is secure and resilient

Pillar Four: Invest in Resilient Future

Cyber threats are constantly evolving, especially with increased usage in the internet. Emerging technologies such as internet of things (IoT), quantum computing, and artificial intelligence (AI) demonstrate new and upcoming cyber threats and challenges the government will face in the future. Pillar 4 aims to protect the digital future tomorrow brings by developing resiliency in research and development, clean energy, post-quantum, and cyber workforce. The government plans to achieve the goal of pillar one by:

- Reducing technical vulnerabilities in the foundation of the internet and across the digital ecosystem while making it more resilient against transnational digital repression
- Prioritizing cybersecurity R&D for next generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure
- Developing a diverse and robust national cyber workforce

PILLAR FIVE: Forge International Partnerships To Pursue Shared Goals

Today's current world of globalization and increased threat by foreign adversaries, the importance of forging strong international partnerships is essential. The United States has partnered with governments from Australia, Canada, and the United Kingdom for example to share intelligence, research, and resources to increase our understanding of threat environments, the speed of research and development, and collaboration in the event of an attack.

- Leveraging international coalitions and partnerships among like minded nations to counter threats to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition
- Increasing the capacity of our partners to defend themselves against cyber threats both in peacetime and in crisis
- Working with our allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology and operational technology products and services