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 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

- Expand the use of minimum cybersecurity requirements in critical sectors
- Harmonize and simplify regulations
- Enable public and private collaboration for the defnse of critical infrastructure and essential services
- Modernize and update Federal incident response policy

Pillar Two: Disrupt and Dismantle Threat Actors

- Strategically employ all tools of national power to disrupt adversaries
- Engage 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

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

Pillar Four: Invest in Resilient Future

- Reduce technical vulnerabilities in the foundation of the internet and across the digital ecosystem while making it more resilient against transnational digital repression
- Prioritize 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

- 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