Technology by Policy

CYBERSECURITY

National Cybersecurity Strategy Implementation Plan

July 13, 2023

Summary:

The Biden Administration released the National Cybersecurity Strategy Implementation Plan (NCSIP) on July 13, 2023 as a roadmap to ensure transparency and coordination to implement the NCS. This roadmap outlines 65 high-impact Federal initiatives to implement the five pillars of the National Cybersecurity Strategy, spanning 18 responsible agencies. Each initiative has its own specified completion date, with the latest being Q4 FY26.

The NCSIP is expected to evolve as time goes on.

Overview

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. 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.

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. The plan helps federal agencies coordinate, so they are all moving in the same direction to meet the goals of the NCS. The plan helps agencies understand how to request and allocate their **budget** to achieve the different requirements within the NCS. Walden did not want to create a mandate without funding, which is why the NCS gives agencies the language and tools to receive the required funding for the strategy to succeed.

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.

Number of Initiatives By Pillar

Pillar One: Defend Critical Infrastructure (16 Initiatives)	
Strategic Objectives	**Responsible Agencies**
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 **1.5:** Modernize Federal Defenses	• Office of the National Cyber Director (ONCD) • National Security Council (NSC) • National Institute of Standards and Technology (NIST) • Cybersecurity and Infrastructure Security Agency (CISA) • Department of Homeland Security (DHS) • Office of Management and Budget (OMB) • National Security Agency (NSA)

Pillar Two: Disrupt and Dismantle Threat Actors (11 Initiatives)	
Strategic Objectives	**Responsible Agencies**
2.1: Integrate Federal Disruption Activities **2.2:** Enhance Public-Private Operational Collaboration to Disrupt Adversaries **2.3:** Increase the Speed and Scale of Intelligence Sharing and Victim Notification **2.4:** Prevent Abuse of U.S.-Based Infrastructure **2.5:** Counter Cybercrime, Defeat Ransomware	• Department of Defense (DOD) • Federal Bureau of Investigation (FBI) • Department of Justice (DOJ) • Office of the National Cyber Director (ONCD) • National Security Council (NSC) • Office of the Director of National Intelligence (ODNI) • Department of Commerce • Department of State • Cybersecurity and Infrastructure Security Agency (CISA) • Department of the Treasury

Pillar Three: Shape Market Forces to Drive Security and Resilience (11 Initiatives)	
Strategic Objectives	**Responsible Agencies**
3.1: Hold the Stewards of our Data Accountable **3.2:** Drive the Development of Secure IoT Devices **3.3:** Shift Liability for Insecure Software Products and Services **3.4:** Use Federal Grants and Other Incentives to Build in Security **3.5:** Leverage Federal Procurement to Improve Accountability **3.6:** Explore a Federal Cyber Insurance Backstop	• Office of Management and Budget (OMB) • National Security Council (NSC) • Office of the National Cyber Director (ONCD) • Cybersecurity and Infrastructure Security Agency (CISA) • Office of Science and Technology Policy (OSTP) • National Science Foundation (NSF) • Department of Justice (DOJ) • Department of the Treasury

Pillar Four: Invest in A Resilient Future (13 Initiatives)	
Strategic Objectives	**Responsible Agencies**
4.1: Secure the Technical Foundation of the Internet **4.2:** Reinvigorate Federal Research and Development for Cybersecurity **4.3:** Prepare for Our Post-Quantum Future **4.4:** Secure Our Clean Energy Future **4.5:** Support Development of a Digital Identity Ecosystem **4.6:** Develop a National Strategy to Strengthen Our Cyber Workforce	• Office of Management and Budget (OMB) • Office of the National Cyber Director (ONCD) • National Institute of Standards and Technology (NIST) • Office of Science and Technology Policy (OSTP) • National Security Agency (NSA) • Department of Energy (DOE)

Pillar Five: Forge International Partnerships to Pursue Shared Goals (12 Initiatives)	
Strategic Objectives	**Responsible Agencies**
5.1: Build Coalitions to Counter Threats to Our Digital Ecosystem **5.2:** Strengthen International Partner Capacity **5.3:** Expand U.S. Ability to Assist Allies and Partners **5.4:** Build Coalitions to Reinforce Global Norms of Responsible State Behavior **5.5:** Secure Global Supply Chains for Information, Communication, and Operational Technology Products and Services	• Department of State • Federal Bureau of Investigation (FBI) • Office of the National Cyber Director (ONCD) • Department of Justice (DOJ) • National Telecommunications and Information Administration (NTIA) • National Institute of Standards and Technology (NIST)

For more information on information on the 65 different initiatives, please check out the National Cybersecurity Strategy Implementation Plan.