

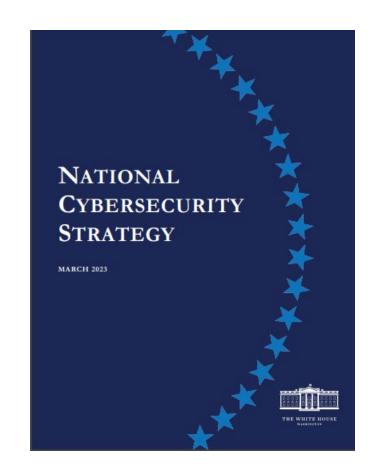
National Cybersecurity Strategy

July 31, 2023
Brian Scott
Deputy Assistant National Cyber Director, Cyber Policy & Programs





- > The President issued the National Cybersecurity Strategy on March 2, 2023
- Establishes an affirmative, values-driven vision for a secure cyberspace that creates opportunities to achieve our collective aspirations.
- Calls for two fundamental shifts:
 - 1. Rebalance the responsibility to defend cyberspace
 - 2. Realign incentives to favor long-term investment
- Advances fundamental shifts across 5 pillars:
 - 1. **Defend** critical infrastructure
 - **2. Disrupt** and dismantle threat actors
 - 3. Shape market forces to drive security and resilience
 - **4. Invest** in a resilient future
 - 5. Forge international partnerships to pursue shared goals



National Cybersecurity Strategy - March 2023

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
Strategic Objective 1.1: Establish Cybersecurity Requirements to Support National Security and Public	Strategic Objective 2.1: Integrate Federal Disruption Activities	Strategic Objective 3.1: Hold the Stewards of Our Data Accountable	Strategic Objective 4.1: Secure the Technical Foundation of the Internet	Strategic Objective 5.1: Build Coalitions to Counter Threats to Our Digital Ecosystem
Safety Strategic Objective 1.2:	Strategic Objective 2.2: Enhance Public-Private Operational Collaboration to	Strategic Objective 3.2: Drive the Development of Secure IoT Devices	Strategic Objective 4.2: Reinvigorate Federal Research and Development	Strategic Objective 5.2: Strengthen International
Scale Public-Private Collaboration	Disrupt Adversaries Strategic Objective 2.3:	Strategic Objective 3.3: Shift Liability for Insecure	for Cybersecurity Strategic Objective 4.3:	Partner Capacity Strategic Objective 5.3:
Strategic Objective 1.3: Integrate Federal Cybersecurity Centers	Increase the Speed and Scale of Intelligence Sharing and Victim Notification	Software Products and Services	Prepare for Our Post-Quantum Future	Expand U.S. Ability to Assist Allies and Partners
Strategic Objective 1.4: Update Federal Incident Response Plans and	Strategic Objective 2.4: Prevent Abuse of U.SBased Infrastructure	Strategic Objective 3.4: Use Federal Grants and Other Incentives to Build in Security	Strategic Objective 4.4: Secure Our Clean Energy Future	Strategic Objective 5.4: Build Coalitions to Reinforce Global Norms of Responsible State Behavior
Processes Strategic Objective 1.5: Modernize Federal Defenses	Strategic Objective 2.5: Defeat Ransomware	Strategic Objective 3.5: Leverage Federal Procurement to Improve Accountability	Strategic Objective 4.5: Support Development of a Digital Identity Ecosystem	Strategic Objective 5.5: Secure Global Supply Chains for Information,
		Strategic Objective 3.6: Explore a Federal Cyber Insurance Backstop	Strategic Objective 4.6: Develop a National Strategy to Strengthen Our Cyber Workforce	Communications, and Operational Technology Products and Services





4.1 Secure the Technical Foundation of the Internet

4.1.5 Collaborate with key stakeholders to drive secure Internet routing

The Office of the National Cyber Director, in conjunction with key stakeholders and appropriate Federal Government entities, will develop a roadmap to increase the adoption of secure internet routing techniques and technology by:

- (1) identifying security challenges;
- (2) exploring approaches and options to address internet routing and BGP security concerns;
- (3) identifying and informing the development of best practices;
- (4) identifying needed research and development; and
- (5) identifying barriers to adoption and alternate mitigation approaches



Brian Scott
Deputy Assistant National Cyber Director, Cyber Policy & Programs
Office of the National Cyber Director
Executive Office of the President