JENNER & BLOCK

White House Releases Report on US Cybersecurity Posture

Client Alerts

May 14, 2024
By: Shoba Pillay, Zoë Higgins Reinstein

On May 7, 2024, the White House Office of the National Cyber Director (ONCD) released several reports on the United States' cybersecurity posture and strategic plan. These documents implement the 2023 National Cybersecurity Strategy (NCS), and consist of:

> (1) the 2024 Report on the Cybersecurity Posture of the United States (Posture Report) and fact sheet; and
> (2) Version 2 of the National Cybersecurity Strategy Implementation Plan (NCSIP) and fact sheet.

According to ONCD Director Harry Coker, Jr., the United States' cybersecurity regime is in the midst of "a fundamental transformation," moving from a reactive to a proactive posture in order to keep pace with a fast-evolving cyber threat landscape. These documents provide updates on the US transition, and the steps necessary to implement the NCS.

Key Takeaways

The Posture Report is largely retrospective and serves as an index of the federal cyber initiatives over the past year, listing the various accomplishments of the over 24 federal agencies contributing to this effort. Conversely, the NCSIP is prospective and outlines the 100 initiatives the federal government will take to implement the NCS.

Together, these reports analyze the challenges and opportunities ONCD plans to target in the next year. The benchmarks point toward an increased scrutiny of and reliance on the private sector to reshape the digital ecosystem and enhance the United States' resilience to cyber threats. Private sector organizations often have visibility into certain aspects of malicious activity that the federal government does not and hold much of the power to reverse insecure practices by implementing Secure by Design principles and patching security vulnerabilities. Another trend is an increased focus on developments in advanced computing technologies like quantum computing and AI and preparing for these technologies via cyber workforce training and interagency coordination.

Furthermore, the federal government is looking externally to risks posed by China, Russia, Iran, and North Korea, and non-state criminal organizations. However, these reports stress that many of the solutions to these risks are also external to the United States, based in coalition building and compatible international standards.

2024 Cybersecurity Posture Report

The Posture Report, issued by the ONCD under 6 U.S.C. § 1500(c)(1)(C)(iv), provides a first-of-its-kind update on how the United States is addressing the challenges and opportunities faced in cyberspace, the progress made in realizing a safe, prosperous, and equitable digital future, and remaining threats.

The Posture Report analyzes:

> (1) The **strategic environment**, including emerging trends, threat actor capabilities and intent, and evolving vulnerabilities;

The Posture Report focuses on five trends that transformed the strategic environment in 2023: evolving risks to critical infrastructure, ransomware, supply chain exploitation, commercial spyware, and AI.

> (2) The United States' **current efforts** to bolster domestic cybersecurity;

The Posture Report lists the actions taken by 24 government agencies over the past year to improve cybersecurity policy, in parallel with Versions 1 and 2 of the NCSIP (discussed in more detail below). These actions focus on, among other topics, protecting critical infrastructure, enhancing federal cooperation and partnerships with the private sector and international partners, disrupting adversary activity, strengthening the national cyber workforce, and investing in resilient next-generation technologies.

These initiatives aim to bolster cybersecurity requirements where they are lacking, harmonize and align new and existing regulatory requirements both at home and abroad, aid victims of cyberattacks, and provide tools to potential victims.

> (3) The **future outlook.**

The Posture Report highlights the new technical and governance challenges and opportunities the administration will take over the next year, including aligning resources to support the efforts outlined in greater detail in NCSIP.

2024 NCSIP

Version 2 of the NCSIP complements the findings of the Posture Report and outlines the steps necessary to further improve US cybersecurity posture. Version 1 of the NCSIP, released in July

2023, introduced 69 federal benchmarks intended to achieve the goals of the NCS by 2025. Going forward the NCSIP will be updated annually in coordination with the Office of Management and Budget.

Version 2 provides a status update and complements the goals outlined in the Posture Report by adding 31 new benchmarks, bringing the total to 100. These benchmarks correspond to the five pillars of the NCS:

(1) Defend **critical infrastructure.**

Benchmarks under this pillar stem from the Cybersecurity and Infrastructure Security Agency (CISA) and other sector risk management agencies and focus on enabling and scaling public-private collaboration with critical infrastructure owners and operators. Among the critical infrastructure sectors targeted are healthcare and public health, education, energy, and utilities like water and wastewater systems. Specific initiatives include developing a taxonomy for federal cybersecurity centers, introducing an energy threat and analysis center (ETAC), reinvigorating interagency coordination through issuing the final CIRCIA cyber incident reporting rule, encouraging best practices through implementation of the updated NIST CSF, and developing supply chain risk assessment rules.

(2) Disrupt and dismantle **threat actors.**

This pillar focuses on strengthening collaboration between federal, state, local, tribal, and territorial law enforcement, the private sector, and international partners to prevent, deter, and disrupt cybercrime. Specific benchmarks introduced in Version 2 of the NCSIP focus on deterring cybercrime by juveniles, disrupting safe havens for ransomware crimes, and developing policies that support collaboration with the private sector.

(3) Shape **market forces** to drive security and resilience.

The benchmarks under this pillar focus on placing responsibility for cybersecurity on entities best positioned to reduce risk and generate a more resilient digital ecosystem. These include updating the national privacy research strategy, developing a voluntary labeling program for internet of things (IoT) smart devices (US Cyber Trust Mark), and assessing open-source software security risk.

(4) **Invest** in a resilient future.

In support of this pillar, the NCSIP focuses on accelerating the development and adoption of secure internet standards and technologies, increasing federal involvement in research and development of cybersecurity techniques, pairing decarbonization and cybersecurity for electric distribution operators with the administration's broader cybersecurity goals, preparing for the rise of quantum computing, and expanding access to cyber education and training in support of the national cyber workforce.

(5) Forge **international partnerships** to pursue shared goals.

This pillar emphasizes the importance of building coalitions to develop open and interoperable standards-based networks, providing incident response assistance to allies, improving supply-chain resiliency, implementing the International Cyberspace and Digital Policy Strategy, developing guidance for the secure development and manufacturing of semiconductors, and supporting the development of open and interoperable wireless networks.

Conclusion

The scope of the programs introduced in the Posture Report and Version 2 of the NCSIP are sweeping and indicate a real commitment by the federal government to assessing and improving US cybersecurity resilience. These initiatives continue the trend towards a deeper reliance on the private sector and aspirational coordination between federal agencies in an already crowded space.

Related Attorneys

Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Zoë Higgins Reinstein
Associate
zreinstein@jenner.com
+1 312 840 7420

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →