THE WHITE HOUSE
WASHINGTON

**FOR IMMEDIATE RELEASE**
July 13, 2023

**FACT SHEET:**
**Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan**

*Read the full Implementation Plan here*

President Biden has made clear that all Americans deserve the full benefits and potential of our digital future. The Biden-Harris Administration's recently released National Cybersecurity Strategy calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace:

1. Ensuring that the biggest, most capable, and best-positioned entities – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk

2. Increasing incentives to favor long-term investments into cybersecurity

Today, the Administration is announcing a roadmap to realize this bold, affirmative vision. It is taking the novel step of publishing the National Cybersecurity Strategy Implementation Plan (NCSIP) to ensure transparency and a continued path for coordination. This plan details more than 65 high-impact Federal initiatives, from protecting American jobs by combatting cybercrimes to building a skilled cyber workforce equipped to excel in our increasingly digital economy. The NCSIP, along with the Bipartisan Infrastructure Law, CHIPS and Science Act, Inflation Reduction Act, and other

major Administration initiatives, will protect our investments in rebuilding America's infrastructure, developing our clean energy sector, and re-shoring America's technology and manufacturing base.

Each NCSIP initiative is assigned to a responsible agency and has a timeline for completion. Some initiatives, such as the issuance of the Administration's Cybersecurity Priorities for the Fiscal Year 2025 Budget, have been completed ahead of schedule. Other completed activities, such as the transmittal of the May 26th Department of Defense 2023 Cyber Strategy to Congress, and the June 20th creation of a new National Security Cyber Section by the Justice Department, are key milestones in completing initiatives. This is the first iteration of the plan, which is a living document that will be updated annually.

Eighteen agencies are leading initiatives in this whole-of-government plan demonstrating the Administration's deep commitment to a more resilient, equitable, and defensible cyberspace. The Office of the National Cyber Director (ONCD) will coordinate activities under the plan, including an annual report to the President and Congress on the status of implementation, and partner with the Office of Management and Budget (OMB) to ensure funding proposals in the President's Budget Request are aligned with NCSIP initiatives. The Administration looks forward to implementing this plan in continued collaboration with the private sector, civil society, international partners, Congress, and state, local, Tribal, and territorial governments. As an example of the Administration's commitment to public-private collaboration, ONCD is also working on a request for information regarding cybersecurity regulatory harmonization that will be published in the near future. The

NCSIP is not intended to capture all Federal agency activities in support of the NCS. The following are sample initiatives from the plan, which is organized by the NCS pillars and strategic objectives.

**Pillar One | Defending Critical Infrastructure**

- Update the National Cyber Incident Response Plan (1.4.1): During a cyber incident, it is critical that the government acts in a coordinated manner and that private sector and SLTT partners know how to get help. The Cybersecurity and

Infrastructure Security Agency (CISA) will lead a process to update the National Cyber Incident Response Plan to more fully realize the policy that “a call to one is a call to all.” The update will also include clear guidance to external partners on the roles and capabilities of Federal agencies in incident response and recovery.

**Pillar Two | Disrupting and Dismantling Threat Actors**

- Combat Ransomware (2.5.2 and 2.5.4): Through the Joint Ransomware Task Force, which is co-chaired by CISA and the FBI, the Administration will continue its campaign to combat the scourge of ransomware and other cybercrime. The FBI will work with Federal, international, and private sector partners to carry out disruption operations against the ransomware ecosystem, including virtual asset providers that enable laundering of ransomware proceeds and web fora offering initial access credentials or other material support for ransomware activities. A complementary initiative, led by CISA, will include offering resources such as training, cybersecurity services, technical assessments, pre-attack planning, and incident response to high-risk targets of ransomware, like hospitals and schools, to make them less likely to be affected and to reduce the scale and duration of impacts if they are attacked.

**Pillar Three | Shaping Market Forces and Driving Security and Resilience**

- Software Bill of Materials (3.3.2): Increasing software transparency allows market actors to better understand their supply chain risk and to hold their vendors accountable for secure development practices. CISA continues to lead work with key stakeholders to identify and reduce gaps in software bill of materials (SBOM) scale and implementation. CISA will also explore requirements for a globally-accessible database for end of life/end of support software and convene an international staff-level working group on SBOM.

**Pillar Four | Investing in a Resilient Future**

- Drive Key Cybersecurity Standards (4.1.3, 4.3.3): Technical standards are foundational to the Internet, and U.S. leadership in this area is essential to the

vibrancy and security of cyberspace. Consistent with the National Standards Strategy, the National Institute of Standards and Technology (NIST) will convene the Interagency International Cybersecurity Standardization Working Group to coordinate major issues in international cybersecurity standardization and enhance U.S. federal agency participation in the process. NIST will also finish standardization of one or more quantum-resistant publickey cryptographic algorithms.

**Pillar Five | Forging International Partnerships to Pursue Shared Goals**

- International Cyberspace and Digital Policy Strategy (5.1.1 and 5.1.2): Cyberspace is inherently global, and policy solutions must reflect close collaboration with our partners and allies. The Department of State will publish an International Cyberspace and Digital Policy Strategy that incorporates bilateral and multilateral activities. State will also work to catalyze the development of staff knowledge and skills related to cyberspace and digital policy that can be used to establish and strengthen country and regional interagency cyber teams to facilitate coordination with partner nations.

###