FORTIFY U.S. CYBER DEFENSES AND TRUST IN ICT SUPPLY CHAINS

The United States is engaged in an ongoing and escalating struggle against persistent, agile and well-funded cyber adversaries. To succeed in this fight, the federal government needs to improve its defenses against sophisticated and determined cyber threats with a coordinated, multilayered and cutting-edge cyber defense strategy. Significant investments in updating and securing federal government networks to prevent, detect, mitigate and remediate cyber intrusions are a key component of a successful strategy, as well as investments in a robust and active partnership with the private sector to ensure a resilient and adaptive defense of critical infrastructure and government systems.

To that end, the federal government should enhance collaboration between the public and private sectors to detect, deter and respond to malicious activity in cyberspace. The Administration should renew its cyber deterrence frameworks and leadership of global efforts to combat cyber threats.

1. Invest in and modernize U.S. government cyber defenses.

The federal government should make significant investments to secure and modernize its information technology (IT) systems and cyber defense capabilities, particularly across civilian federal government agencies. This work includes taking the following actions:

- **a.** Modernize federal IT systems, with a particular focus on those protecting civilian and regulatory agencies. Additionally, the government should improve efforts to recruit and retain the cybersecurity talent needed to develop and maintain these systems.
- **b.** Increase the use of secure, cloud-based computing architecture among government agencies and their vendors.
- **c.** Partner with state, local, tribal and territorial governments; law enforcement; and citizen services bodies to dramatically improve their cybersecurity posture.
- **d.** Ensure that the Office of National Cyber Director has the resources, the authorities and a clear mandate to lead the federal government's engagement with private industry and coordinate a whole-of-government approach to partnership with critical infrastructure operators.

2. Operationalize cyber defense collaboration between private and government entities.

The federal government should continue to focus on encouraging and amplifying bidirectional communication between the public and private sectors to eliminate cyber threat intelligence silos, particularly given the private sector's role in operating critical infrastructure in the United States. Clear, available fora for public-private information sharing are necessary to ensure that both industry and government have up-to-date information on emerging and increasingly multifaceted threats. The 2015 Cybersecurity Information Sharing Act established a statutory framework around information sharing, but there continue to be gaps

in implementation where information is not shared between agencies, is not shared on a timely basis with the private sector or lacks actionable context. To operationalize public-private cyber defense collaboration between, the federal government should:

a. Enhance existing information-sharing platforms to facilitate the secure exchange of real-time threat data between public and private entities;

b. Systematize a regular process to review cyber intrusions into public and private systems to capture and share lessons learned with the private sector;

c. Expand and build upon the use of mission accelerators to allow the private sector to collaborate with the government on emerging cybersecurity threats;

d. Provide resources and authorities for U.S. agencies with significant cybersecurity capabilities to collaborate actively with the private sector to help reduce systemic cyber risk; and

e. Resource national security agencies to develop programmatic support for critical infrastructure cybersecurity and recognize designated critical infrastructure as intelligence customers.

3. Improve the resiliency and transparency of ICT supply chains.

The federal government should continue to work collaboratively with the private sector to enhance the trust in and security of ICT supply chains. Specifically, the federal government should:

a. Promote the adoption of best practices for secure software development, distribution and testing and support continued development for software assurance programs such as the early-stage National Telecommunications and Information Administration's Software Bill of Materials Project;

b. Combine, streamline and expand on work already underway to enhance supply chain security, such as the Department of Homeland Security ICT Supply Chain Risk Management Task Force and the Department of Defense Cybersecurity Maturity Model Certification program;

c. Partner with critical infrastructure supply chain entities (owners, operators, suppliers and manufacturers) to identify and remediate policy, legal and technical barriers to security testing for critical hardware and software components; and

d. Support the continued advancement of responsible and coordinated approaches to the management and disclosure of security vulnerabilities. The federal government should work with the private sector to update guidance and frameworks for vulnerability management, including disclosure and patching.

4. Invest in building a deeper pool of highly qualified and diverse cybersecurity talent.

Current pathways for training, recruiting and retaining cybersecurity personnel are inadequate to meet the demand for cybersecurity talent. The government should build partnerships with academia and industry to deepen the pool of qualified candidates for critical cybersecurity jobs, including by taking the following actions:

a. Expand current pathways into government cybersecurity roles by utilizing apprenticeship and externship programs, increasing the funding available to the CyberCorps program, and investing in upskilling programs for current federal employees.

b. Work with colleges and universities to fund and develop cybersecurity training programs for high-demand cyber skills, such as secure software development and penetration testing.

5. Promote global cooperation on cyber threat deterrence.

In addition to advancing norms for responsible behavior in cyberspace, the federal government should re-engage with partners and allies and take the lead in building a robust transnational cybersecurity alliance against threat actors that coordinates responses and legal remedies to deter malicious cyber activity.