Executive Order—Strengthening U.S. Cyber Security and Capabilities

EXECUTIVE ORDER

STRENGTHENING U.S. CYBER SECURITY AND CAPABILITIES

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy.

It is the policy of the United States to defend and enhance the security of the Nation's cyber infrastructure and capabilities. Free and secure use of cyberspace is essential to advancing U.S. national interests. The Internet is a vital national resource. Cyberspace must be an environment that fosters efficiency, innovation, communication, and economic prosperity without disruption, fraud, theft, or invasion of privacy. The United States is committed to: ensuring the long-term strength of the Nation in cyberspace; preserving the ability of the United States to decisively shape cyberspace relative to other international, state, and non-state actors; employing the full spectrum of our capabilities to defend U.S. interests in cyberspace; and identifying, disrupting, and defeating malicious cyber actors.

Sec. 2. Findings.

(a) America's civilian government institutions and critical infrastructure are currently vulnerable to attacks from both state and non-state actors. Criminals, terrorists, and state and non-state actors are engaging in continuous operations that impose significant costs on the U.S. economy and significantly harm vital national interests. These operations may disrupt or disable the functioning of important economic institutions and critical infrastructure, and may potentially cause physical effects that could result in significant property damage and loss of life.

(b) The cyber realm is undergoing constant, rapid change as a result of the pace of technological innovation, the explosive global growth in Internet use, the increasing interdependencies between the networks and the operations of infrastructure and key economic institutions, and the continuously evolving nature of cyberattacks and attackers.

(c) As a result of these changes, cyberspace has emerged as a new domain of engagement, comparable in significance to land, sea, air, and space, and its significance will increase in the years ahead.

(d) The Federal Government has a responsibility to defend America from cyberattacks that could threaten U.S. national interests or cause significant damage to Americans' personal or economic security. That responsibility extends to protecting both privately and publicly operated critical networks and infrastructure. At the same time, the need for dynamism, flexibility, and

innovation in cyber security demands that government exercise its responsibility in close cooperation with private sector entities.

(e) The executive departments and agencies (agencies) tasked with protecting civilian government networks and critical infrastructure are not currently organized to act collectively/ collaboratively, tasked, or resourced, or provided with legal authority adequate to succeed in their missions.

Sec. 3. Definitions. As used in this order:

(a) The term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

(b) The term "national security system" means any telecommunications or information system operated by the Federal Government or any contractor on its behalf, the function, operation, or use of which—

(i) involves intelligence activities;

(ii) involves cryptologic activities related to national security;

(iii) involves command and control of military forces;

(iv) involves equipment that is an integral part of a weapon or weapons system; or

(v) is critical to the direct fulfillment of military or intelligence missions (but does not include a system used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications).

Sec. 4. Policy Coordination.

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned in this order shall be provided through the interagency process established in National Security Presidential Directive – 1 of January 21, 2017 (Organization of the National Security Council and the Homeland Security Council), or any successor.

Sec. 5. Review of Cyber Vulnerabilities.

(a) *Scope and Timing.*

(i) A review of the most critical U.S. cyber vulnerabilities (Vulnerabilities Review) shall commence immediately.

(ii) Within 60 days of the date of this order, initial recommendations for the protection of U.S. national security systems shall be submitted to the President through the Secretary of Defense.

(iii) Within 60 days of the date of this order, initial recommendations for the enhanced protection of the most critical civilian Federal Government, public, and private sector infrastructure, other than U.S. national security systems, shall be submitted to the President through the Secretary of Homeland Security.

(iv) The recommendations shall include steps to ensure that the responsible agencies are appropriately organized, tasked, and resourced, and provided with adequate legal authority necessary to fulfill their missions.

(b) *Review Participants.* The Secretary of Defense shall co-chair the Vulnerabilities Review with the Secretary of Homeland Security, the Director of National Intelligence, the Assistant to the President for National Security Affairs, and the Assistant to the President for Homeland Security and Counterterrorism.

(c) *Operation of the Vulnerabilities Review.* The Co-Chairs of the Vulnerabilities Review shall assemble all information in the possession of the Federal Government that pertains to the most urgent vulnerabilities to national security systems, the most urgent vulnerabilities to civilian Federal Government networks, and the most critical private sector infrastructure. All agencies shall promptly comply with any request of the Co-Chairs to provide information in their possession or control pertaining to U.S. cyber vulnerabilities. The Secretary of Defense, the Secretary of Homeland Security, the Assistant to the President for National Security Affairs, and the Assistant to the President for Homeland Security and Counterterrorism may seek further information relevant to the Vulnerabilities Review from any appropriate source.

Sec. 6. Review of Cyber Adversaries.

(a) *Scope and Timing.*

(i) A review of the principal U.S. cyber adversaries (Adversaries Review) shall commence immediately.

(ii) Within 60 days of the date of this order, a first report on the identities, capabilities, and vulnerabilities of the principal U.S. cyber adversaries shall be submitted to the President through the Director of National Intelligence.

(b) *Review Participants.* The Director of National Intelligence shall co-chair the Adversaries Review with the Secretary of Homeland Security, the Secretary of Defense, the Assistant to the President for National Security Affairs, and the Assistant to the President for Homeland Security and Counterterrorism.

(c) *Operation of the Adversaries Review.* The Co-Chairs of the Adversaries Review shall assemble all information in the possession of the Federal Government that pertains to the identities, capabilities, and vulnerabilities of U.S. cyber adversaries. All agencies shall promptly comply with any request of the Co-Chairs to provide information in their possession or control pertaining to U.S. cyber adversaries. The Co-Chairs may seek further information relevant to the Adversaries Review from any appropriate source.

Sec. 7. U.S. Cyber Capabilities Review.

(a) *Scope and Timing.*

(i) Based on the results of sections 5 and 6 of this order, a review of the relevant cyber capabilities of the Department of Defense, the Department of Homeland Security, and the National Security Agency (Capabilities Review) shall identify an initial set of capabilities needing improvement to adequately protect U.S. critical infrastructure.

(ii) The Capabilities Review's recommendations shall include steps to ensure that the responsible agencies are appropriately organized, tasked, and resourced, and provided with adequate legal authority necessary to fulfill their missions.

(b) *Participants.* The Secretary of Defense shall co-chair the Capabilities Review, with the Secretary of Homeland Security and the Director of the National Security Agency.

(c) *Operation of Capabilities Review.* The Co-Chairs of the Capabilities Review shall assemble all information in the possession of the Federal Government that pertains to relevant cyber capabilities of the Department of Defense, the Department of Homeland Security, and the National Security Agency. All agencies shall promptly comply with any request of the Co-Chairs to provide information in their possession or control pertaining to U.S. cyber capabilities. The Secretary of Defense, the Secretary of Homeland Security, and the Director of the National Security Agency may seek further information relevant to the Capabilities Review from any appropriate source.

(d) *Workforce Development Review.* In order to ensure that the United States has a long-term cyber capability advantage, the Secretary of Defense and Secretary of Homeland Security shall also gather and review information from the Department of Education regarding computer science, mathematics, and cyber security education from primary through higher education to understand the full scope of U.S. efforts to educate and train the workforce of the future. The Secretary of Defense shall make recommendations as he sees fit in order to best position the U.S. educational system to maintain its competitive advantage into the future.

Sec. 8. Private Sector Infrastructure Incentives Report.

(a) *Scope and Timing.*

(i) Preparation of a Report on options to incentivize private sector adoption of effective cyber security measures (Report) shall commence immediately.

(ii) Within 100 days of the date of this order, the Report recommending options shall be submitted to the President through the Secretary of Commerce.

(b) *Participants.* The Secretary of Commerce shall co-chair the group preparing the Report, with the Secretary of the Treasury, the Secretary of Homeland Security, and the Assistant to the President for Economic Affairs. The Secretary of Commerce may also invite the Chair of the Securities and Exchange Commission and the Chair of the Federal Trade Commission to participate.

(c) *Operation of Report.* The Co-Chairs of the group that prepared the Report shall review and expand on existing reports on economic and other incentives to: induce private sector owners and operators of the Nation's critical infrastructure to maximize protective measures; invest in cyber enterprise risk management tools and services; and adopt best practices with respect to processes and technologies necessary for the increased sharing of and response to real-time cyber threat information. All agencies shall promptly comply with any request of the Co-Chairs to identify those economic policies and incentives capable of accelerating investments in cyber security tools, services, and software. The Secretary of the Treasury, the Secretary of Commerce, the Secretary of Homeland Security, and the Assistant to the President for Economic Affairs may seek further information relevant to the Report from any appropriate source.

Sec. 9. General Provisions.

(a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or any head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu