

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

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. Cybersecurity of Federal Networks.

(a) Policy. The executive branch of the Federal Government operates its networks on behalf of the American people. These networks and the data on them should be secured responsibly using all United States Government capabilities. The President will hold accountable heads of executive departments and agencies (Agency Heads) for managing the risk to their enterprises. In addition, because risk management decisions made by Agency Heads can affect the risk to the executive branch as a whole, it is also the policy of the United States to manage cyber risk as an executive branch enterprise.

(b) Findings.

- (i) Cybersecurity risk management comprises the full range of activities undertaken to identify and protect information and information technology (IT) assets from unauthorized access and other threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT assets, and to mitigate the impact of, respond to, and recover from incidents.
- (ii) The executive branch has for too long accepted antiquated and difficult to defend IT and information systems.
- (iii) Effective risk management involves more than just protecting networks and data currently in place. It also requires planning so that future maintenance, improvements, and modernization occur in a coordinated fashion and with appropriate regularity.
- (iv) Known but unmitigated vulnerabilities are among the highest risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security specific configuration guidance.
- (v) Effective risk management requires Agency Heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

(c) Risk Management.

- (i) Agency Heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems. They shall also be held accountable by the President for ensuring that information security management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.
- (ii) Effective immediately, Agency Heads shall use *The Framework for Improving Critical Infrastructure Cybersecurity* (the Framework), or any successor document, developed by the National Institute of Standards and Technology to manage their agency's cyber risk. Each Agency Head shall provide a risk management report to the Director of the Office of Management and Budget (OMB) and the Secretary of Homeland Security within 90 days of the date of this order describing the agency's implementation of the Framework. The risk management report shall document at a minimum the mitigation and acceptance choices made by each Agency Head. Any accepted risk from unmitigated vulnerabilities

must be explicitly documented in the report. The report described in this paragraph may be classified in full or in part, as appropriate.

(iii) The Director of OMB, with appropriate support from the Secretary of Homeland Security, consistent with Chapter 35, Subchapter II of Title 44, shall assess each agency's risk management report to determine whether, in the aggregate, the risk management choices set forth in the report are appropriate and sufficient to manage the cyber risk to the executive branch enterprise (their determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, their determination and a plan to accomplish the following:

(A) protect adequately the executive branch enterprise should the determination identify insufficiencies;

(B) establish a regular reassessment and determination process;

(C) address unmet budgetary needs necessary to managing risk to the executive branch enterprise resulting from their determination;

(D) clarify, reconcile, and reissue as necessary all policies, standards, and guidelines issued by any agency in furtherance of Chapter 35, Subchapter II of Title 44, United States Code and this order; and

(E) align these policies, standards, and guidelines with the Framework.

(v) Effective immediately, it is the policy of the United States to build a more modern, more secure, and more resilient Executive Branch IT architecture.

(A) Agency Heads shall show preference in their procurement for shared IT services to the extent permitted by law, including email, cloud, and cybersecurity services.

(B) The Assistant to the President for Intragovernmental and Technology Initiatives shall coordinate a report to the President from the Secretary of Commerce, the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services regarding modernization of Federal Government IT. The report shall be completed within 150 days of the date of this order and, at a minimum, describe the following:

(1) The technical feasibility and cost effectiveness, with timelines and milestones, of transitioning all agencies to one or more consolidated network architectures, and any legal, policy, or budgetary considerations to implementing that transition; and

(2) The technical feasibility and cost effectiveness, with timelines and milestones, of transitioning all agencies to shared IT services, including email, cloud services, and cybersecurity services, and any legal, policy, or budgetary considerations to implementing that transition.

In assessing technical feasibility under subsections (1) and (2), the report shall consider the impact of transitioning to shared IT services on agency information security, including by making recommendations to ensure compliance with policies and practices issued in accordance with

44 U.S.C. 3553. All Agency Heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(C) For National Security Systems, the Secretary of Defense and the Director of National Intelligence shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for Homeland Security and

Counterterrorism describing their implementation of this paragraph within 150 days of the date of this order. The report described in this paragraph may be classified in full or in part, as appropriate.

Section 2. Cybersecurity of Critical Infrastructure.

(a) Policy. It is the policy of the United States to ensure that the United States Government is prepared to employ its authorities and capabilities to aid in the protection of the operation of critical infrastructure entities identified by the Secretary of Homeland Security.

(b) Support to Critical Infrastructure. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the Director of National Intelligence, and the heads of appropriate sector specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013, and all other appropriate Agency Heads, as identified by the Secretary of Homeland Security, shall:

(i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure owners and operators identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity) to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

(ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified in subsection (i) of this section might be employed to support their risk management efforts and any obstacles to doing so; and

(iii) deliver a report to the President, with a classified annex as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the signing of this order, that includes the following:

(A) The authorities and capabilities identified pursuant to this paragraph;

(B) The results of the engagement and determination required pursuant to this paragraph; and

(C) Findings and recommendations for better supporting the cybersecurity of section 9 entities.

(b) Supporting Transparency in the Marketplace. The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cyber risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.

(c) Core Communications Infrastructure. The Secretary of Commerce, in coordination with the Secretary of Homeland Security, shall lead an open and transparent process to identify and promote action by owners, operators, and other stakeholders of core communications infrastructure to improve the resilience of such infrastructure and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the

Director of the Federal Bureau of Investigation, the heads of sector specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested Agency Heads, owners and operators of core communications infrastructure, and other stakeholders as appropriate in carrying out this paragraph. Within 240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1 year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) Assessment of Electricity Disruption Response Capabilities. While this order is being implemented to improve the security of critical infrastructure sectors, the Secretary of Homeland Security, in coordination with the Secretary of Energy and in consultation with State, local, tribal and territorial governments and other stakeholders as appropriate, shall assess:

(i) the potential scope and duration of a significant cyber incident against the United States electric subsector;

(ii) the readiness of the United States to manage the consequences of such an incident; and

(iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with a classified annex as appropriate, within 90 days of the date of this order.

(f) Department of Defense Warfighting Capabilities and Industrial Base. The Secretary of Defense and the Secretary of Homeland Security and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks, within 90 days of the date of this order.

Section 3. Cybersecurity for the Nation.

(a) Policy. It is the policy of the United States to promote an open, interoperable, reliable, and secure Internet that fosters efficiency, innovation, communication, and economic prosperity, and respects privacy, while guarding against disruption, fraud, and theft.

(b) Deterrence and Protection. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President on the nation's strategic options for deterring adversaries and better protecting the American people from those who would use networked technology to defeat or undermine this policy.

(c) Internet Freedom and Governance. The Internet is a resource that underpins American power, innovation, and values. Within 180 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General, shall report to the President on continued actions to support the multi-stakeholder process to ensure the Internet remains valuable, reliable, and secure for future generations.

Section 4. General Provisions.

- (a) 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 the head thereof; or
 - (ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.
- (b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.
- (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 construed 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.