EXECUTIVE ORDER

- - - - - - -

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, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data 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 cybersecurity 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 and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

(i) Cybersecurity risk management comprises the full range of activities undertaken to identify and protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of,

respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity 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 IT and data. They will also be held

accountable by the President for ensuring that cybersecurity risk 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, each Agency Head 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 the agency's cybersecurity risk. Each Agency Head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document at a minimum the mitigation and acceptance choices made by each Agency Head as of the date of this order, including:

(1) the strategic, operational, and budgetary considerations that informed those choices; and

(2) any accepted risk, including from unmitigated vulnerabilities; and

(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44,

United States Code, shall assess each agency's risk management report to determine whether the risk management and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (their determination).

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

(A) Their determination; and

(B) A plan to accomplish the following:

(1) Protect adequately the executive branch enterprise, should their determination identify insufficiencies;

(2) Address immediate unmet budgetary needs necessary to manage enterprise risk to the executive branch;

(3) Establish a regular process for reassessing and, if appropriate, reissuing their determination, and addressing future, recurring unmet budgetary needs

necessary to manage enterprise risk to the executive branch;

(4) Clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code**, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order**; and

(5) Align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsections c(ii) and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, 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

Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of IT. The report shall be completed within 60 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, or a subset of agencies, to one or more consolidated network architectures, and any legal, policy, or budgetary considerations relevant to implementing that transition; and

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

(C) In assessing technical feasibility under subsections (c)(vi)(B)(1) and (B)(2) of this section, the report shall consider the impact of transitioning to shared IT services on agency cybersecurity, including by making recommendations to ensure consistency with section 227 of

the Homeland Security Act (6 U.S.C. 148) and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All Agency Heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

(vii) For National Security Systems, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Director of OMB and the Secretary of Homeland Security, 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 National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

Sec. 2. Cybersecurity of Critical Infrastructure.

(a) Policy. It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and

operators of the Nation's critical infrastructure (as **defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities),** as appropriate.

(b) Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector specific agencies), 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 entities 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 (b)(i) of this section

might be employed to support cybersecurity risk management efforts and any obstacles to doing so;

(iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

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

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

(C) Findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

(iv) provide an updated report to the President on an annual basis thereafter.

(c) 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 cybersecurity 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.

(d) Resilience Against Botnets and Other Automated, Distributed Threats. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem 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, and appropriate stakeholders in carrying out this subsection. 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 Incident Response Capabilities. The Secretary of Homeland Security, in

coordination with the Secretary of Energy and in consultation with State, local, tribal, and territorial governments and others as appropriate, shall assess:

(i) the potential scope and duration of a power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), 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, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) Department of Defense Warfighting Capabilities and Industrial Base. Within 90 days of the date of this order, the Secretary of Defense, 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. The report may be classified in full or in part, as appropriate.

Sec. 3. Cybersecurity for the Nation.

(a) Policy. To ensure that the Internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure Internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields, as the foundation for achieving our objectives in cyberspace.

(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, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's

strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) International Cooperation. As a highly connected nation, the United States is especially dependent on a globally secure and resilient Internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 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 and the Director of the Federal Bureau of Investigation, shall report to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the submission of the reports and in coordination with the Agency Heads listed in this subsection and any other Agency Heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, on an engagement strategy for international cooperation in cybersecurity.

(d) Workforce Development. In order to ensure that the United States maintains a long-term cybersecurity advantage:

(i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, Secretary of Education, Secretary of Labor, the Director of the Office of Personnel Management, and other executive branch agencies identified by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(a) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and

(b) within 120 days of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the nation's cybersecurity workforce in both the public and private sectors.

(ii) The Director of National Intelligence, in consultation with the heads of other executive branch agencies identified by the Director of National Intelligence, shall:

(a) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term U.S. cybersecurity competitiveness; and

(b) within 60 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism.

(iii) The Secretary of Defense, in coordination with the Secretary of Homeland Security and the Secretary of Commerce, shall:

(a) assess the scope and sufficiency of U.S. efforts to ensure U.S. national security-related cyber capability advantage; and

(b) within 150 days of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

Sec. 4. Definitions. For the purposes of this order:

(a) The term "appropriate stakeholders" means any non-executive-branch person or entity that elects to participate in an open and transparent process established by the Secretary of Commerce and the Secretary of Homeland Security under section 2(d) of this order.

(b) The term "information technology" (IT) has the meaning given to that term in section 11101(6) of title 40, United States Code, and further includes hardware and software systems

of agencies that monitor and control physical equipment and processes.

(c) The term "IT architecture" refers to the integration and implementation of IT within an agency.

(d) The term "network architecture" refers to the elements of IT architecture that enable or facilitate communications between two or more IT assets.

Sec. 5. 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 or 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.

THE WHITE HOUSE,