Presidential Executive Order on Strengthening the Cybersecurity

of Federal Networks and Critical Infrastructure

Sec. 1 Cybersecurity of Federal Networks.

(a) Policy: The president will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. It is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings
   a. Information sharing facilitates and supports detection, mitigation, response and recovery efforts across the federal networks.
   b. Effective risk management requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.
   c. Agencies have accepted the use of antiquated IT systems. Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies).
      i. 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.
   d. To effectively handle risk management, agencies need senior executives with expertise in IT, security, budgeting, acquisition, law, privacy and human resources.

(c) Risk Management
   a. Agency heads will be held accountable by the president for implementing risk management measures commensurate with the risk and magnitude of the threat and for complying with strategic, operational and budgetary planning processes.
   b. Effective immediately, each agency head shall use the NIST Framework for Improving Critical Infrastructure Cybersecurity, and 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. It will include
      i. Any risk acceptance the agency has chosen
      ii. Agency's plan to implement the NIST Framework
   c. The Secretary of Homeland Security and the Director of OMB shall jointly assess each agency's risk management report to determine whether it is acceptable.
      i. A determination report must be sent to the president 60 days after receiving the agency's report.
   d. The Director of OMB, in coordination with the Secretary of Homeland Security are primarily responsible or submitting a plan on:
      i. Additional ways to adequately protect the executive branch enterprise;
      ii. Address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;
      iii. Establish a regular process for regular continuous evaluation of risk management plans and budgetary needs;

iv. Reissue, clarify and reconcile existing laws, guidance and policy, and align these policies, standards and guidelines with the Framework.

e. The agency reports may be classified, in whole or in part.

f. Effective immediately, the executive branch will build and maintain a modern, secure and more resilient executive branch IT architecture.

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

ii. The Director of the American Technology Council shall coordinate a report to the president from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services which will contain:

1. The relevant legal, policy, and budgetary considerations relevant and technical feasibility and cost effectiveness, of transitioning to:

a. Shared IT services, including email, cloud, and cybersecurity services.

b. A consolidated network architecture.

2. Must be completed within 90 days of this order.

g. For any National Security System, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. They will issue a report within 150 days of the date of this order with justification for any deviation from the reporting requirements outlined above.

Sec. 2 Cybersecurity for Critical Infrastructure.

(a) Policy

a. Executive branch will support the cybersecurity risk management efforts of the owners and operators of the nation's critical infrastructure.

(b) Support to Critical Infrastructure at Greatest Risk.

a. The Secretary of Homeland Security, in coordination with other relevant agencies will:

i. Identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities under greatest threat of catastrophic, regional or national effects on public health or safety, economic security, or national security if compromised.

ii. Write a report within 180 days of the date of this order,

1. identifying enabling authorities and capabilities,

2. identifying results of the engagement and determination as outlined above, and

3. identifying findings and recommendations for better supporting the cybersecurity risk management efforts.

iii. Provide an updated report to the president on an annual basis thereafter.

(c) Supporting Transparency in the Marketplace.

a. The Secretary of Homeland Security, in coordination with other relevant agencies will report on 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.
    a. The Secretary of Commerce and Homeland Security will jointly lead a process to identify and promote action with the goal of dramatically reducing threats perpetrated by automated and distributed attacks.
        i. 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 one 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.
    a. The Secretary of Energy and the Secretary of Homeland Security, in consultation with other relevant agencies will assess:
        i. The potential scope and duration of a prolonged power outage associated with a significant cyber incident;
        ii. The readiness of the United States to manage the consequences of such an incident;
        iii. Any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.
    b. Provide the report to the president 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.
    a. Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and other relevant agencies shall report 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.

Sec. 3 Cybersecurity for the Nation.

(a) Policy
    a. The executive branch promotes 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.
    b. The executive branch also supports the growth and sustainment of a workforce that is skilled in cybersecurity and related fields.

(b) Deterrence and Protection.
    a. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, with other relevant agencies will submit a report on the nation's strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) International Cooperation.
    a. Within 45 days of the executive order, relevant agencies will submit reports to the president on their international cybersecurity priorities, including those concerning

investigation, attribution, cyber threat information sharing, response, capacity building and cooperation.

b. Within 90 days of the submission of the reports, agency heads will submit reports documenting an engagement strategy for international cooperation in cybersecurity.

(d) Workforce Development.

a. The Secretary of Commerce and Secretary of Homeland Security within 120 days of the date of this order, will provide a report 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.

b. The Director of National Intelligence will review the workforce development efforts of foreign talent to help identify foreign workforce development practices and within 60 days of the date of this order, and provide a report for the findings of the review.

c. The Secretary of Defense will:

i. Assess the scope and sufficiency of the United States' efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and

ii. Within 150 days of the date of this order, provide a report to the president, with findings and recommendations.

Sec. 4 Definitions.

Sec. 5 General Provisions.