Sec. 2. Removing Barriers to Sharing Threat Information.

(a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

(b) Within 60 days of the date of this order, the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, shall review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and OT service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. The recommendations shall include descriptions of contractors to be covered by the proposed contract language.

(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:

(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements;

(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;

(iii) service providers collaborate with Federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed; and

(iv) service providers share cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation.

(d) Within 90 days of receipt of the recommendations described in subsection (b) of this section, the FAR Council shall review the proposed contract language and conditions and, as appropriate, shall publish for public comment proposed updates to the FAR.

(e) Within 120 days of the date of this order, the Secretary of Homeland Security and the Director of OMB shall take appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI as may be necessary for the Federal Government to respond to cyber threats, incidents, and risks.

(f) It is the policy of the Federal Government that:

(i) information and communications technology (ICT) service providers entering into contracts with agencies must promptly report to such agencies when they discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies;

(ii) ICT service providers must also directly report to CISA whenever they report under subsection (f)(i) of this section to Federal Civilian Executive Branch (FCEB) Agencies, and CISA must centrally collect and manage such information; and

(iii) reports pertaining to National Security Systems, as defined in section 10(h) of this order, must be received and managed by the appropriate agency as to be determined under subsection (g)(i)(E) of this section.

(g) To implement the policy set forth in subsection (f) of this section:

(i) Within 45 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense acting through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB, shall recommend to the FAR Council contract language that identifies: (A) the nature of cyber incidents that require reporting; (B) the types of information regarding cyber incidents that require reporting to facilitate effective cyber incident response and remediation; (C) appropriate and effective protections for privacy and civil liberties; (D) the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection; (E) National Security Systems reporting requirements; and (F) the type of contractors and associated service providers to be covered by the proposed contract language.

(ii) Within 90 days of receipt of the recommendations described in subsection (g)(i) of this section, the FAR Council shall review the recommendations and publish for public comment proposed updates to the FAR.

(iii) Within 90 days of the date of this order, the Secretary of Defense acting through the Director of the NSA, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies.

(h) Current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government.

(i) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Defense acting through the Director of the NSA,

the Director of OMB, and the Administrator of General Services, shall review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language.

(j) Within 60 days of receiving the recommended contract language developed pursuant to subsection (i) of this section, the FAR Council shall review the recommended contract language and publish for public comment proposed updates to the FAR.

(k) Following any updates to the FAR made by the FAR Council after the public comment period described in subsection (j) of this section, agencies shall update their agency-specific cybersecurity requirements to remove any requirements that are duplicative of such FAR updates.

(l) The Director of OMB shall incorporate into the annual budget process a cost analysis of all recommendations developed under this section.