Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities.

(a) Information from network and system logs on Federal Information Systems (for both on□premises systems and connections hosted by third parties, such as CSPs) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide them upon request to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.

(b) Within 14 days of the date of this order, the Secretary of Homeland Security, in consultation with the Attorney General and the Administrator of the Office of Electronic Government within OMB, shall provide to the Director of OMB recommendations on requirements for logging events and retaining other relevant data within an agency's systems and networks. Such recommendations shall include the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. Logs shall be protected by cryptographic methods to ensure integrity once collected and periodically verified against the hashes throughout their retention. Data shall be retained in a manner consistent with all applicable privacy laws and regulations. Such recommendations shall also be considered by the FAR Council when promulgating rules pursuant to section 2 of this order.

(c) Within 90 days of receiving the recommendations described in subsection (b) of this section, the Director of OMB, in consultation with the Secretary of Commerce and the Secretary of Homeland Security, shall formulate policies for agencies to establish requirements for logging, log retention, and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency.

(d) The Director of OMB shall work with agency heads to ensure that agencies have adequate resources to comply with the requirements identified in subsection (c) of this section.

(e) To address cyber risks or incidents, including potential cyber risks or incidents, the proposed recommendations issued pursuant to subsection (b) of this section shall include requirements to ensure that, upon request, agencies provide logs to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law. These requirements should be designed to permit agencies to share log information, as needed and appropriate, with other Federal agencies for cyber risks or incidents.