Sec. 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.

(a) The cybersecurity vulnerability and incident response procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting their systems vary across agencies, hindering the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively across agencies. Standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses.

(b) Within 120 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB, the Federal Chief Information Officers Council, and the Federal Chief Information Security Council, and in coordination with the Secretary of Defense acting through the Director of the NSA, the Attorney General, and the Director of National Intelligence, shall develop a standard set of operational procedures (playbook) to be used in planning and conducting a cybersecurity vulnerability and incident response activity respecting FCEB Information Systems. The playbook shall:

(i) incorporate all appropriate NIST standards;

(ii) be used by FCEB Agencies; and

(iii) articulate progress and completion through all phases of an incident response, while allowing flexibility so it may be used in support of various response activities.

(c) The Director of OMB shall issue guidance on agency use of the playbook.

(d) Agencies with cybersecurity vulnerability or incident response procedures that deviate from the playbook may use such procedures only after consulting with the Director of OMB and the APNSA and demonstrating that these procedures meet or exceed the standards proposed in the playbook.

(e) The Director of CISA, in consultation with the Director of the NSA, shall review and update the playbook annually, and provide information to the Director of OMB for incorporation in guidance updates.

(f) To ensure comprehensiveness of incident response activities and build confidence that unauthorized cyber actors no longer have access to FCEB Information Systems, the playbook shall establish, consistent with applicable law, a requirement that the Director of CISA review and validate FCEB Agencies' incident response and remediation results upon an agency's completion of its incident response. The Director of CISA may recommend use of another agency or a third-party incident response team as appropriate.

(g) To ensure a common understanding of cyber incidents and the cybersecurity status of an agency, the playbook shall define key terms and use such terms consistently with any statutory definitions of those terms, to the extent practicable, thereby providing a shared lexicon among agencies using the playbook.