

Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks.

(a) The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks in order to bolster the Federal Government's cybersecurity efforts.

(b) FCEB Agencies shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

(c) Within 30 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall provide to the Director of OMB recommendations on options for implementing an EDR initiative, centrally located to support host-level visibility, attribution, and response regarding FCEB Information Systems.

(d) Within 90 days of receiving the recommendations described in subsection (c) of this section, the Director of OMB, in consultation with Secretary of Homeland Security, shall issue requirements for FCEB Agencies to adopt Federal Government-wide EDR approaches. Those requirements shall support a capability of the Secretary of Homeland Security, acting through the Director of CISA, to engage in cyber hunt, detection, and response activities.

(e) The Director of OMB shall work with the Secretary of Homeland Security and agency heads to ensure that agencies have adequate resources to comply with the requirements issued pursuant to subsection (d) of this section.

(f) Defending FCEB Information Systems requires that the Secretary of Homeland Security acting through the Director of CISA have access to agency data that are relevant to a threat and vulnerability analysis, as well as for assessment and threat-hunting purposes. Within 75 days of the date of this order, agencies shall establish or update Memoranda of Agreement (MOA) with CISA for the Continuous Diagnostics and Mitigation Program to ensure object level data, as defined in the MOA, are available and accessible to CISA, consistent with applicable law.

(g) Within 45 days of the date of this order, the Director of the NSA as the National Manager for National Security Systems (National Manager) shall recommend to the Secretary of Defense, the Director of National Intelligence, and the Committee on National Security Systems (CNSS) appropriate actions for improving detection of cyber incidents affecting National Security Systems, to the extent permitted by applicable law, including recommendations concerning EDR approaches and whether such measures should be operated by agencies or through a centralized service of common concern provided by the National Manager.

(h) Within 90 days of the date of this order, the Secretary of Defense, the Director of National Intelligence, and the CNSS shall review the recommendations submitted under subsection (g) of this section and, as appropriate, establish policies that effectuate those recommendations, consistent with applicable law.

(i) Within 90 days of the date of this order, the Director of CISA shall provide to the Director of OMB and the APNSA a report describing how authorities granted under section 1705 of Public Law 116-283, to conduct threat-hunting activities on FCEB networks without prior authorization from agencies, are being implemented. This report shall also recommend procedures to ensure that mission-critical systems are not disrupted, procedures for notifying system owners of vulnerable government systems, and the range of techniques that can be used during testing of FCEB Information Systems. The Director of CISA shall provide quarterly reports to the APNSA and the Director of OMB regarding actions taken under section 1705 of Public Law 116-283.

(j) To ensure alignment between Department of Defense Information Network (DODIN) directives and FCEB Information Systems directives, the Secretary of Defense and the Secretary of Homeland Security, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, establish procedures for the Department of Defense and the Department of Homeland Security to immediately share with each other Department of Defense Incident Response Orders or Department of Homeland Security Emergency Directives and Binding Operational Directives applying to their respective information networks;

(ii) evaluate whether to adopt any guidance contained in an Order or Directive issued by the other Department, consistent with regulations concerning sharing of classified information; and

(iii) within 7 days of receiving notice of an Order or Directive issued pursuant to the procedures established under subsection (j)(i) of this section, notify the APNSA and Administrator of the Office of Electronic Government within OMB of the evaluation described in subsection (j)(ii) of this section, including a determination whether to adopt guidance issued by the other Department, the rationale for that determination, and a timeline for application of the directive, if applicable.