Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—

The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

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.

Sec. 3. *Modernizing Federal Government Cybersecurity.* (a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

(b) Within 60 days of the date of this order, the head of each agency shall:

(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them; and

(iii) provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to subsection (b)(i) and (ii) of this section.

(c) As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with Zero Trust Architecture. The Secretary of Homeland Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

(i) Within 90 days of the date of this order, the Director of OMB, in consultation with the Secretary of Homeland Security acting through the Director of CISA, and the Administrator of General Services acting through FedRAMP, shall develop a Federal cloud-security strategy and provide guidance to agencies accordingly. Such guidance shall seek to ensure that risks to the FCEB from using cloud-based services are broadly understood and effectively addressed, and that FCEB Agencies move closer to Zero Trust Architecture.

(ii) Within 90 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 and the Administrator of General Services acting through FedRAMP, shall develop and issue, for the FCEB, cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.

(iii) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall develop and issue, for FCEB Agencies, a cloud-service governance framework. That framework shall identify a range of services and protections available to agencies based on incident severity. That framework shall also identify data and processing activities associated with those services and protections.

(iv) Within 90 days of the date of this order, the heads of FCEB Agencies, in consultation with the Secretary of Homeland Security acting through the Director of CISA, shall evaluate the types and sensitivity of their respective agency's unclassified data, and shall provide to the Secretary of Homeland Security through the Director of CISA and to the Director of OMB a report based on such evaluation. The evaluation shall prioritize identification of the unclassified data considered by the agency to be the most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data.

(d) Within 180 days of the date of this order, agencies shall adopt multifactor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. To that end:

(i) Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB,

and the APNSA on their respective agency's progress in adopting multi-factor authentication and encryption of data at rest and in transit. Such agencies shall provide such reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication and data encryption.

(ii) Based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB Agencies of technologies and processes to implement multifactor authentication and encryption for data at rest and in transit.

(iii) Heads of FCEB Agencies that are unable to fully adopt multi-factor authentication and data encryption within 180 days of the date of this order shall, at the end of the 180-day period, provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

(e) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Attorney General, the Director of the FBI, and the Administrator of General Services acting through the Director of FedRAMP, shall establish a framework to collaborate on cybersecurity and incident response activities related to FCEB cloud technology, in order to ensure effective information sharing among agencies and between agencies and CSPs.

(f) Within 60 days of the date of this order, the Administrator of General Services, in consultation with the Director of OMB and the heads of other agencies as the Administrator of General Services deems appropriate, shall begin modernizing FedRAMP by:

(i) establishing a training program to ensure agencies are effectively trained and equipped to manage FedRAMP requests, and providing access to training materials, including videos-on-demand;

(ii) improving communication with CSPs through automation and standardization of messages at each stage of authorization. These communications may include status updates, requirements to complete a vendor's current stage, next steps, and points of contact for questions;

(iii) incorporating automation throughout the lifecycle of FedRAMP, including assessment, authorization, continuous monitoring, and compliance;

(iv) digitizing and streamlining documentation that vendors are required to complete, including through online accessibility and pre-populated forms; and

(v) identifying relevant compliance frameworks, mapping those frameworks onto requirements in the FedRAMP authorization process, and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process, as appropriate.

Sec. 4. *Enhancing Software Supply Chain Security.* (a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of ''critical software''—software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)—is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.

(b) Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria in subsection (e) of this section.

The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions as:

(A) using administratively separate build environments;

(B) auditing trust relationships;

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

(E) employing encryption for data; and

(F) monitoring operations and alerts and responding to attempted and actual cyber incidents;

(ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section;

(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (*i.e.,* origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

(f) Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

(g) Within 45 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, the Secretary of Homeland Security acting through the Director of CISA, the Director of OMB, and the Director of National Intelligence, shall publish a definition of the term ''critical software'' for inclusion in the guidance issued pursuant to subsection (e) of this section. That definition shall reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

(h) Within 30 days of the publication of the definition required by subsection (g) of this section, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Commerce acting through the Director of NIST, shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software issued pursuant to subsection (g) of this section.

(i) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.

(j) Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.

(k) Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.

(l) Agencies may request an extension for complying with any requirements issued pursuant to subsection (k) of this section. Any such request shall be considered by the Director of OMB on a case-by-case basis, and only if accompanied by a plan for meeting the underlying requirements. The Director of OMB shall on a quarterly basis provide a report to the APNSA identifying and explaining all extensions granted.

(m) Agencies may request a waiver as to any requirements issued pursuant to subsection (k) of this section. Waivers shall be considered by the Director of OMB, in consultation with the APNSA, on a case-by-case basis, and shall be granted only in exceptional circumstances and for limited duration, and only if there is an accompanying plan for mitigating any potential risks.

(n) Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section.

(o) After receiving the recommendations described in subsection (n) of this section, the FAR Council shall review the recommendations and, as appropriate and consistent with applicable law, amend the FAR.

(p) Following the issuance of any final rule amending the FAR as described in subsection (o) of this section, agencies shall, as appropriate and consistent with applicable law, remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.

(q) The Director of OMB, acting through the Administrator of the Office of Electronic Government within OMB, shall require agencies employing software developed and procured prior to the date of this order (legacy software) either to comply with any requirements issued pursuant to subsection (k) of this section or to provide a plan outlining actions to remediate or meet those requirements, and shall further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to subsection (k) of this section, unless an extension or waiver is granted in accordance with subsection (l) or (m) of this section.

(r) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, shall publish guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

(s) The Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.

(t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

(u) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the FTC and representatives from other agencies as the Director of NIST deems appropriate, shall identify secure software development practices or criteria for a consumer software labeling program, and shall consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs, consistent with applicable law. The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone. The Director

of NIST shall examine all relevant information, labeling, and incentive programs, employ best practices, and identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.

(v) These pilot programs shall be conducted in a manner consistent with OMB Circular A–119 and NIST Special Publication 2000–02 (Conformity Assessment Considerations for Federal Agencies).

(w) Within 1 year of the date of this order, the Director of NIST shall conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, determine what improvements can be made going forward, and submit a summary report to the APNSA.

(x) Within 1 year of the date of this order, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide to the President, through the APNSA, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain.

Sec. 5. *Establishing a Cyber Safety Review Board.* (a) The Secretary of Homeland Security, in consultation with the Attorney General, shall establish the Cyber Safety Review Board (Board), pursuant to section 871 of the Homeland Security Act of 2002 (6 U.S.C. 451).

(b) The Board shall review and assess, with respect to significant cyber incidents (as defined under Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination) (PPD–41)) affecting FCEB Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.

(c) The Secretary of Homeland Security shall convene the Board following a significant cyber incident triggering the establishment of a Cyber Unified Coordination Group (UCG) as provided by section V(B)(2) of PPD–41; at any time as directed by the President acting through the APNSA; or at any time the Secretary of Homeland Security deems necessary.

(d) The Board's initial review shall relate to the cyber activities that prompted the establishment of a UCG in December 2020, and the Board shall, within 90 days of the Board's establishment, provide recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices, as outlined in subsection (i) of this section.

(e) The Board's membership shall include Federal officials and representatives from private-sector entities. The Board shall comprise representatives of the Department of Defense, the Department of Justice, CISA, the NSA, and the FBI, as well as representatives from appropriate private-sector cybersecurity or software suppliers as determined by the Secretary of Homeland Security. A representative from OMB shall participate in Board activities when an incident under review involves FCEB Information Systems, as determined by the Secretary of Homeland Security. The Secretary of Homeland Security may invite the participation of others on a case-by-case basis depending on the nature of the incident under review.

(f) The Secretary of Homeland Security shall biennially designate a Chair and Deputy Chair of the Board from among the members of the Board, to include one Federal and one private-sector member.

(g) The Board shall protect sensitive law enforcement, operational, business, and other confidential information that has been shared with it, consistent with applicable law.

(h) The Secretary of Homeland Security shall provide to the President through the APNSA any advice, information, or recommendations of the Board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident.

(i) Within 30 days of completion of the initial review described in subsection (d) of this section, the Secretary of Homeland Security shall provide to the President through the APNSA the recommendations of the Board based on the initial review. These recommendations shall describe:

(i) identified gaps in, and options for, the Board's composition or authorities;

(ii) the Board's proposed mission, scope, and responsibilities;

(iii) membership eligibility criteria for private-sector representatives;

(iv) Board governance structure including interaction with the executive branch and the Executive Office of the President;

(v) thresholds and criteria for the types of cyber incidents to be evaluated;

(vi) sources of information that should be made available to the Board, consistent with applicable law and policy;

(vii) an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the purpose of the Board's review of incidents; and

(viii) administrative and budgetary considerations required for operation of the Board.

(j) The Secretary of Homeland Security, in consultation with the Attorney General and the APNSA, shall review the recommendations provided to the President through the APNSA pursuant to subsection (i) of this section and take steps to implement them as appropriate.

(k) Unless otherwise directed by the President, the Secretary of Homeland Security shall extend the life of the Board every 2 years as the Secretary of Homeland Security deems appropriate, pursuant to section 871 of the Homeland Security Act of 2002.

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.

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 Secretary, 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.

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.

Sec. 9. *National Security Systems.* (a) Within 60 days of the date of this order, the Secretary of Defense acting through the National Manager, in coordination with the Director of National Intelligence and the CNSS, and in consultation with the APNSA, shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order that are otherwise not applicable to National Security Systems. Such requirements may provide for exceptions in circumstances necessitated by unique mission needs. Such requirements shall be codified in a National Security Memorandum (NSM). Until such time as that NSM is issued, programs, standards, or requirements established pursuant to this order shall not apply with respect to National Security Systems.

(b) Nothing in this order shall alter the authority of the National Manager with respect to National Security Systems as defined in National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) (NSD–42). The FCEB network shall continue to be within the authority of the Secretary of Homeland Security acting through the Director of CISA.

Sec. 10. *Definitions.* For purposes of this order:

(a) the term ''agency'' has the meaning ascribed to it under 44 U.S.C. 3502.

(b) the term ''auditing trust relationship'' means an agreed-upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.

(c) the term ''cyber incident'' has the meaning ascribed to an ''incident'' under 44 U.S.C. 3552(b)(2).

(d) the term ''Federal Civilian Executive Branch Agencies'' or ''FCEB Agencies'' includes all agencies except for the Department of Defense and agencies in the Intelligence Community.

(e) the term ''Federal Civilian Executive Branch Information Systems'' or ''FCEB Information Systems'' means those information systems operated by Federal Civilian Executive Branch Agencies, but excludes National Security Systems.

(f) the term ''Federal Information Systems'' means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency, including FCEB Information Systems and National Security Systems.

(g) the term ''Intelligence Community'' or ''IC'' has the meaning ascribed to it under 50 U.S.C. 3003(4).

(h) the term ''National Security Systems'' means information systems as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3).

(i) the term ''logs'' means records of the events occurring within an organization's systems and networks. Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network.

(j) the term ''Software Bill of Materials'' or ''SBOM'' means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

(k) the term ''Zero Trust Architecture'' means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

Sec. 11. *General Provisions.* (a) Upon the appointment of the National Cyber Director (NCD) and the establishment of the related Office within the Executive Office of the President, pursuant to section 1752 of Public Law 116–283, portions of this order may be modified to enable the NCD to fully execute its duties and responsibilities.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

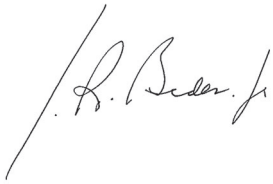
(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) This order shall be implemented in a manner consistent with applicable law and subject to the availability of appropriations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any

party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) Nothing in this order confers authority to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned in the course of a criminal or national security investigation.



THE WHITE HOUSE,
May 12, 2021.

[FR Doc. 2021–10460
Filed 5–14–21; 8:45 am]
Billing code 3295–F1–P