

rity 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 [enacting 6 U.S.C. 1500], 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.

J.R. BIDEN, JR.

§ 3552. Definitions

(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

(1) The term “binding operational directive” means a compulsory direction to an agency that—

(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

(2) The term “incident” means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies,

security procedures, or acceptable use policies.

(3) The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(4) The term “information technology” has the meaning given that term in section 11101 of title 40.

(5) The term “intelligence community” has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(6)(A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(7) The term “Secretary” means the Secretary of Homeland Security.

(Added Pub. L. 113-283, §2(a), Dec. 18, 2014, 128 Stat. 3074.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3532 and 3542 of this title prior to repeal by Pub. L. 113-283.

§ 3553. Authority and functions of the Director and the Secretary

(a) DIRECTOR.—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) ensuring that the Secretary carries out the authorities and functions under subsection (b);

(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(5) overseeing agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information resources management policies and procedures.

(b) SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

(1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);

(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

(A) requirements for reporting security incidents to the Federal information security