§ 3552

TITTE 44—PUBLIC PRINTING AND DOCUMENTS

Page 178

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 contain information systems operated or managed by the Department of Defense and agencies in the Intelligence Community.

(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

(i) an information system 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 can be composed of log entries, which 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 detailed 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.

(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 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 user, role, and context.

(l) 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 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 user, role, and context.
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 1101 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.