

## 44 USCS § 3552

Current through Public Law 118-62, approved May 13, 2024.

*United States Code Service* > **TITLE 44. PUBLIC PRINTING AND DOCUMENTS (§§ 101 — 4104)** > **CHAPTER 35. Coordination of Federal Information Policy (Subchs. I — III)** > **Subchapter II. Information Security (§§ 3551 — 3559)**

### § 3552. Definitions

---

**(a) In general.** Except as provided under subsection (b), the definitions under section 3502 [44 USCS § 3502] shall apply to this subchapter [44 USCS §§ 3551 et seq.].

**(b) Additional definitions.** As used in this subchapter [44 USCS §§ 3551 et seq.]:

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**(C)** may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.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

## § 3552. Definitions

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

## History

---

### HISTORY:

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

United States Code Service  
Copyright © 2024 All rights reserved.