

**DEPARTMENT OF HOMELAND SECURITY
FEDERAL LAW ENFORCEMENT TRAINING CENTER**

FLETC DIRECTIVE NO:	4300
DIRECTIVE TITLE:	Information Technology Security Program
EFFECTIVE DATE:	09/15/2008

1. POLICY: The Federal Law Enforcement Training Center's (FLETC) Information Technology (IT) security program provides the foundation to assure the confidentiality, integrity, availability, authenticity, and non-repudiation of government data contained in FLETC IT systems.

2. SCOPE: This directive applies to all individual users and administrators of FLETC IT systems — IT systems owned or operated by FLETC and those IT systems maintained or operated on the behalf of FLETC through contracted services. Individual users and administrators include FLETC personnel, detailees, guests/visitors, contractors, FLETC students, student interns, and Partner Organization personnel when using FLETC IT systems. Additional acceptable guidelines for contractors may be specified in individual contract requirements. This directive does not apply to IT systems that are owned and operated by FLETC Partner Organizations or on their behalf through contracted services.

3. REFERENCES:

- a. Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- b. P.L. 104-106, Clinger-Cohen Act of 1996, as amended [formerly, Information Technology Management Reform Act (ITMRA)].
- c. Privacy Act of 1974, as amended, 5 United States Code (U.S.C.) 552a.
- d. 5 CFR § 2635.704, Standards of Ethical Conduct for Employees of the Executive Branch.
- e. Executive Order 13231, Critical Infrastructure Protection in the Information Age.
- f. Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection.
- g. HSPD-12, Common Identification Standard for Federal Employees and Contractors.

- h. National Security Presidential Directive (NSPD) 51/HSPD 20, National Continuity Policy, May 9, 2007.
- i. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources.
- j. OMB Circular A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
- k. OMB Circular A-127, Financial Management Systems, Revised December 1, 2004.
- l. DHS Sensitive Systems Policy 4300A.
- m. DHS Sensitive Systems Handbook 4300A.
- n. Various DHS Management Directives (MD) (e.g., MD 0470.2, MD 4300.1, MD 4400.1, MD 4500.1, MD 4600.1, MD 4900, MD 11042.1, MD 11050.2).
- o. Department of Homeland Security Acquisition Regulation (HSAR), June 2006.
- p. Various NIST SP (e.g., SP 800-16, SP 800-26, SP 800-34, SP 800-37, SP 800-50, SP 800-53, SP 800-64) and FIPS (e.g., FIPS 199).

4. CANCELLATION: None.

5. ADDITIONAL GUIDANCE: [FLETC Manual 4300](#), Information Technology Security Program.

6. OFFICE OF PRIMARY INTEREST: Chief Information Officer Directorate.

[Signature on file](#)

Connie L. Patrick
Director
Director