

DATE July 31, 2002

---

**INFORMATION SECURITY AWARENESS AND TRAINING POLICY**

---

- 1. PURPOSE AND SCOPE.** This policy ensures that the Bureau of Engraving and Printing (BEP/Bureau) complies with all laws and regulations intended to ensure that all employees and contractors are aware of information security principles, risks to information technology (IT) systems, understand their roles and responsibilities related to information security, and are appropriately trained to fulfill them.
- 2. POLICY.** The Bureau will ensure that all users (including contractors) are provided with role-based security awareness training that specifically addresses their information security responsibilities.
- 3. BACKGROUND.** The Bureau, as well as other Government agencies, performs its mission more effectively with ready access to accurate information and access to reliable and secure communications. Information exchange is enhanced through use of the Bureau Local Area/Wide Area Network, including e-mail and In\$ite, and through access to the Internet. However, the greater the access, the more individuals there are using Bureau systems, and the greater the number of interconnections with other systems. This results in greater risk of information compromise, loss of confidentiality, or loss of system capability.

The BEP information security awareness program is designed to provide training for all users which informs them of the risks associated with their activities and the activities of others, and which also informs them of their responsibilities to comply with Bureau and other policies and procedures which are designed to reduce these risks. In addition, the information security training program is targeted to provide specific training to individuals based on their roles and responsibilities in the organization, the level of access to systems and data that they have, the permissions they have to perform activities within a computer system, and the sensitivity of the information to which they have access.

**4. REFERENCES.**

- a. "Protecting America's Critical Infrastructures," Presidential Decision Directive 63, May 1998.
- b. "Security of Federal Automated Information Systems," Office of Management and Budget (OMB) Circular A-130, Appendix III (revised October 2000).
- c. "Government Information Security Reform Act," 44 USC Sections 3531-3536, (PL106-398, Title X, Subtitle G).
- d. "Computer Security Act of 1987," (PL100-235).

DATE July 31, 2002

---

- e. Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," National Institute for Standards and Technology (NIST), October 1995.
- f. Special Publication 800-16, "IT Security Training Requirements: A Role- and Performance-Based Model," NIST, April 1998.
- g. Department of the Treasury Security Manual, TD P 71-10, Chapter VI, Section 8.

## 5. RESPONSIBILITIES.

a. The Associate Director (Chief Information Officer (CIO)) of the Bureau provides oversight of the BEP Information Security Awareness and Training Program. The CIO ensures that programs are in place to inform users of the "Rules of Acceptable Use" which are mandatory for access to systems, and that suitable training is available that is tailored to the roles and responsibilities of those who are involved with the management, use, and operation of information systems within or under the supervision of the Bureau.

b. The Manager, IT Security Division, is responsible for:

- (1) Establishing "Rules of Acceptable Use," which form the basis for information security awareness and training;
- (2) Developing general awareness and role-based computer training and refresher training for all employees and contractors;
- (3) Presenting new employee information security awareness training to all new employees;
- (4) Tracking completion of training to ensure compliance with new employee training, general awareness training, and role-based training goals; and
- (5) Developing performance measures that will indicate the Bureau's progress in meeting Bureau, Departmental, OMB and legislatively mandated training goals.

c. Associate Directors and Office Chiefs are responsible for:

- (1) Ensuring that they are familiar with the requirements for initial and refresher IT security training for their employees;
- (2) Ensuring that their employees and contractors complete required annual training and have signed the "IT Rules of Acceptable Use;"
- (3) Maintaining records of completed training by all employees and contractors;

# CIRCULAR

DATE July 31, 2002

---

- (4) Assisting in the development of training for employees and contractors with specialized roles, responsibilities, and activities; and
- (5) Collecting and maintaining records of training costs and accomplishments for their areas of responsibility.

d. Users are responsible for:

- (1) Reading, understanding, and signing an agreement to abide by the "IT Rules of Acceptable Use" prior to system connection and
- (2) Attending all required training and reporting to supervisors on training completion.

**6. OFFICE OF PRIMARY RESPONSIBILITY.** Associate Director (Chief Information Officer).

**<SIGNED>**

Ronald W. Falter

Associate Director (Chief Information Officer)

DISTRIBUTION - E