

DATE August 19, 2002

INFORMATION SECURITY GENERAL POLICY

1. PURPOSE AND SCOPE. This circular delineates roles and responsibilities of system owners, providers, and users of information technology (IT) at the Bureau of Engraving and Printing (BEP/Bureau) for the establishment and maintenance of adequate security to protect the availability, integrity and confidentiality of information.

2. POLICY. It is the policy of the Bureau to integrate security into the lifecycle of general support systems, applications, and the hardware and software that are components of these systems. It is also Bureau policy that security responsibilities are clearly defined and assigned, as appropriate, to business process owners, information systems support staff, information security staff, and system users, including BEP employees and contractors.

3. REFERENCES.

- a. TD P 71-10, "Department of the Treasury Security Manual," Chapter VI;
- b. BEP Circular No. 10-08.8, "Certification and Accreditation of Computer Systems," August 6, 2001;
- c. Computer Security Act of 1987 (PL 100-235);
- d. OMB Circular No. A-130, "Management of Federal Information Resources," Appendix III (Rev), November 2000;
- e. "Information Technology Management Reform Act of 1996" (Clinger-Cohen Act) (PL 104-106, Div. E);
- f. Government Performance and Results Act of 1993 (PL 103-62);
- g. "Government Information Security Reform Act (GISRA)," 44 USC Sections 3531-3536 (PL 106-398, Title X, Subtitle G);
- h. Privacy Act of 1974;
- i. Presidential Decision Directive 63, "Critical Infrastructure Protection," May 1998; and
- j. Various National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SP) for guidance, advice on implementing policy, and best practices. Some of these are:

DATE August 19, 2002

(1) "Guidelines for Security of Computer Applications," FIPS Publication 73, June 1980;

(2) "An Introduction to Computer Security: the NIST Handbook," SP 800-12, October 1995;

(3) "Guide for Developing Security Plans for Information Technology Systems," SP 800-18, December 1998; and

(4) "Risk Management Guide for Information Technology Systems," SP 800-30, January 2002.

4. RESPONSIBILITIES. Responsibility for IT security is specifically assigned to the Director by the Computer Security Act, OMB Circular A-130, and GISRA. The Director may delegate responsibility to business process owners (the Associate Directors) in some cases. Under GISRA, the Associate Director (Chief Information Officer) also has a number of responsibilities for monitoring the efforts of program and information owners across the organization in order to promote IT security and for developing and maintaining a Bureau-wide information security program.

a. The Director is responsible for ensuring the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems. He also has delegated to the AD (CIO) the authority to perform IT security functions to fulfill the requirements of law and regulation. The Director appoints Principal Accrediting Authorities (PAA) and delegates to them the responsibility for accrediting the IT systems or applications that support their business units following certification.

b. The Associate Director (CIO) sets Bureau wide policies to protect information technology, computer systems, data, and telecommunications and issue rules and guidelines for system establishment, access and use. The AD (CIO) ensures an organization wide information security program that meets the requirements of law and regulation. The Associate Director (CIO):

(1) implements a Bureau-wide security program to manage IT security risk based on risk management principles to identify, assess, and understand risk; determines security requirements and implements measures to achieve an acceptable level of risk; and evaluates and monitors to ensure controls are accomplishing their intended purpose. The program includes periodic risk assessments of internal and external threats, and defines roles and responsibilities for Bureau personnel in complying with policies and procedures to reduce identified risks. Ensures the development of a security awareness training program which addresses employee and contractor roles and responsibilities and

DATE August 19, 2002

ensures periodic testing of the effectiveness of information security policies, procedures, and technical and management controls.

(2) ensures that Bureau systems and major applications have been identified, risks to these systems have been assessed and mitigated, and the systems have received authorization to operate from a Principal Accrediting Authority. Ensures that all general support systems and major applications are certified and accredited.

(3) approves all Interconnection Security Agreements for connections between Bureau and external systems.

(4) appoints an Information System Security Officer (ISSO) and a Network Security Officer (NSO) as provided in the Treasury Security Manual, TD P 71-10, Chapter VI, No. 4 B.

c. The Information Systems Security Officer (ISSO):

(1) ensures the implementation of all Bureau information system security policies and guidelines;

(2) implements and monitors security requirements for all Bureau information systems;

(3) coordinates the conduct of certification reviews and the granting of accreditation for Bureau systems and applications and performs periodic reviews to validate the accreditation;

(4) oversees security testing of hardware and software for certification purposes to ensure that products function as intended, in particular, Bureau applications or systems;

(5) evaluates technical, operational, and management controls related to security for all Bureau systems, applications, to ensure they are operating as intended;

(6) ensures compliance with system security requirements and evaluates interfaces with external systems to ensure appropriate security of those systems and integrity of Bureau information;

(7) provides technical and policy advice to system owners, information owners, program officials, Principal Accrediting Authorities, and others in order to assist them in identifying risks, vulnerabilities, and in identifying and applying policy, procedures, and technology in order to mitigate the risks; and

DATE August 19, 2002

(8) fulfills ISSO duties as described in paragraph 4.a. of TD P 71-10, Chapter VI-4.B.

d. The Network Security Officer (NSO):

(1) ensures the implementation of all Bureau network security policies and guidelines;

(2) implements and monitors security requirements for all Bureau networks and telecommunication systems;

(3) coordinates the conduct of certification reviews and the granting of accreditation for Bureau networks and telecommunications systems and performs periodic reviews to validate the accreditation;

(4) oversees security testing of Bureau networks and telecommunications for certification purposes to ensure adequate level of security;

(5) evaluates technical, operational, and management controls related to security for all Bureau networks to ensure they are operating as intended;

(6) ensures compliance with network security requirements and evaluates connectivity with external systems to ensure appropriate security of those systems and integrity of Bureau information;

(7) provides technical and policy advice to system owners, information owners, program officials, Principal Accrediting Authorities, and others in order to assist them in identifying risks, vulnerabilities, and in identifying and applying policy, procedures, and technology in order to mitigate the risks; and

(8) fulfills NSO duties as described in paragraph 4.b. of TD P 71-10, Chapter VI-4.B.

e. The Manager, Information Technology Security Division (ITSD), has responsibility for the implementation of the Bureau information security program and is the Bureau's authority on technical, operational, and management controls and compliance with security policies and procedures. The Manager (ITSD):

(1) manages the information security program throughout the Bureau and ensures the implementation of policies and procedures to comply with all laws and regulations;

DATE August 19, 2002

(2) directs the development and implementation of policies and procedures governing the implementation of IT security measures and directs the design and implementation of technologies and controls to ensure the appropriate level of security;

(3) monitors compliance with, and evaluates effectiveness of, information security program policies, procedures, and controls;

(4) evaluates system certifications and makes recommendations to the PAA regarding system accreditation;

(5) approves access to Bureau systems and monitors access, authorizations within systems or applications, and monitors access logs and user activities within Bureau systems. Denies or revokes access when necessary to ensure system security or integrity;

(6) evaluates and makes recommendations to the CIO regarding the approval of Interconnection Security Agreements;

(7) coordinates the Bureau's Computer Security Incident Response Capability (CSIRC) to ensure adequate response to security incidents, containment of the damage from these incidents or restoration of critical and non-critical functions, and timely reporting of incidents to appropriate parties;

(8) coordinates the information technology security awareness and training program; and

(9) oversees the activities of the Bureau ISSO and NSO.

f. The Principal Accrediting Authorities (PAA) for the Bureau are individuals who manage, or are principal business owners of, a BEP function supported by an information system. PAAs:

(1) determine the sensitivity of information in their system or application;

(2) coordinate with the AD (CIO) on the security requirements for their information and assist in the assessment of risk to this information;

(3) authorize processing of information on their system or application by accepting the level of risk which has been identified through the certification and accreditation process; and

(4) implement all policies, procedures, and safeguards necessary to mitigate risks sufficiently to allow processing.

CIRCULAR

DATE August 19, 2002

g. System Administrators are responsible for operating, maintaining, and disposing of systems in compliance with Bureau information security policies and procedures. System Administrators shall not:

(1) perform security administration functions on the systems for which the individual is assigned system administrator duties;

(2) probe or attempt to gain unauthorized access to any computer system; or

(3) attempt to test or strain any security mechanisms or security monitoring without authorization from the Manager, ITSD.

h. System Developers and Support Staff are responsible for developing, maintaining and supporting systems in compliance with Bureau information security policies and procedures.

i. Users are responsible for complying with all information security policies and procedures. Users:

(1) are accountable for all activity performed under their accounts (User Id and password);

(2) must report all actual, suspected, or potential information security violations and incidents to the Manager, ITSD; and

(3) must adhere to the "BEP Information Technology Rules of Acceptable Use."

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

<SIGNED>

Ronald W. Falter

Associate Director (Chief Information Officer)

DISTRIBUTION - E