

DATE January 21, 2004

---

**PROTECTING INFORMATION TECHNOLOGY RESOURCES**

---

**1. PURPOSE AND SCOPE.** This circular establishes policy and defines responsibilities and procedures for the management, use and protection of the Bureau of Engraving and Printing's (BEP/Bureau) data and supporting information technology (IT) systems on which the data is processed, stored or transmitted. It applies to all Bureau employees, contractors and others who use information technology to process, store or transmit Bureau information.

**2. POLICY.** It is the policy of the Bureau to protect the confidentiality, integrity, and availability of sensitive information and the information technology systems on which it is processed, stored and transmitted. The Bureau complies with the Treasury Information Security Program Policy, Treasury Department Publication (TD P) 85-01 and other Department of the Treasury and Federal policies and regulations.

Bureau systems are for official and limited personal use and are subject to monitoring. All data contained on Bureau systems is considered the property of the Bureau; thus, there can be no expectation of personal privacy on Bureau IT systems.

Bureau IT systems shall not be used to store, process, or transmit classified information. Unless the Office of Critical Infrastructure and Information Technology Security has provided a written determination that specific information is not sensitive, all Bureau data must, at a minimum, be provided the same level of protection afforded sensitive data. Safeguards are designed and implemented based upon the sensitivity of data and the level of acceptable risk.

**3. REFERENCES.**

a. "Treasury Information Technology Security Program," Treasury Directive Publication (TD P) 85-01, Volume I Policy, Part 1 Sensitive Systems dated August 15, 2003.

b. Public Law 107-347, "E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) of 2002," dated December 17, 2002.

c. Office of Management and Budget (OMB) Circular No. A-130 (Rev), Part III, "Management of Federal Information Resources," dated November 2000.

d. BEP Manual No. 71-00.42, "Information Security Manual," dated March 16, 2000.

e. BEP Circular No. 10-08.8, "Certification and Accreditation of Computer Systems," dated August 6, 2001.

DATE January 21, 2004

---

- f. BEP Circular No. 10-08.21, "IT Configuration Control Board," dated May 21, 2001.
- g. BEP Circular No. 10-08.17, "Protecting Bureau Computers from Computer Viruses," dated March 1, 1993.
- h. BEP Circular No. 40-00.6, "Record Systems Subject to the Privacy Act," dated February 20, 2003.
- i. BEP Circular No. 10-08.18, "Computer Access Control Policy," dated May 31, 2002.
- j. Executive Order 12958, "Classified National Security Information," dated April 17, 1995.
- k. Privacy Act of 1974, 5 United States Code (USC) Section 552a

**4. SUPERSESSION.** This circular supersedes BEP Circular No. 10.08-12, "Microcomputer Security Policy," dated January 25, 1989.

**5. DEFINITIONS.**

a. Accreditation. The official management authorization to operate an IT system 1) in a particular security mode; 2) with a prescribed set of administrative, environmental, and technical security safeguards; 3) against a defined threat and with stated vulnerabilities and countermeasures; 4) in a given operational environment; 5) under a stated operational concept; 6) with stated interconnections to other IT systems; and 7) at an acceptable level of risk for which the Designated Accrediting Authority (DAA) has formally assumed responsibility. The DAA formally accepts security responsibility for the operation of an IT system and officially declares that a specified IT system will adequately protect sensitive information against compromise, destruction, or unauthorized alteration through the continuous employment of safeguards, including administrative, procedural, physical, personnel, communications security, emissions security, and computer-based (e.g., hardware, firmware, software) controls. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

b. Authentication. A security measure designed to establish the validity of a transmission, message, or originator; or a means of verifying a user's or entity's identification. For example, a user may be identified by a particular sign-on ID and then authenticated by providing the correct password.

DATE January 21, 2004

---

c. Availability. Timely, reliable access to data and information services for authorized users. This includes the restoration of services after an interruption.

d. Bureau System. An IT system (e.g., telecommunications, networks, computers, and software) that is owned, leased, or operated by the Bureau; or operated by a contractor or another government agency on behalf of the Bureau.

e. Certification. The comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made as part of and in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

f. Classified Information. National security information that has been classified pursuant to Executive Order (E.O.) 12958.

g. Confidentiality. Provides assurance that information is not disclosed to unauthorized persons, processes, or devices.

h. Designated Accrediting Authority (DAA). The official authorized to grant authority to operate a Bureau system. The DAA, in granting authority to operate, determines and accepts the residual risk to Bureau operations and assets. Refer to BEP Circular No. 10-08.8, "Certification and Accreditation of Computer Systems," dated August 6, 2001.

i. Entity. An entity may be a user, system, process or operation.

j. Identification. The process an information system uses to recognize a user or entity.

k. Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

l. Integrity. The quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of data structures and occurrence of stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

m. Limited Personal Use. Limited personal use is permitted, provided that it is infrequent, incurs minimal expense to the Government, and is during non-work time; does not involve sensitive Government information or put Government information or

DATE January 21, 2004

systems at risk; conforms with Bureau and Department of the Treasury policy; and does not interfere with official business or place excessive burden on Bureau systems. Limited personal use must be conducted in a manner that may not be misrepresented as official business. Employees are specifically prohibited from the pursuit of private commercial business activities for profit-making ventures using the Bureau's office equipment. The ban also includes an employee's use of the Bureau's equipment to assist relatives, friends, or other persons in such activities.

n. Minimal Additional Expense. Where the Bureau is already providing equipment or services, employee's use of such equipment or services shall not result in additional expense to the Government; or result only in normal wear and tear and use of minimal amounts of electricity, ink, toner, or paper.

o. Need to Know. The necessity for access to, or knowledge or possession of, specific information required to carry out official business.

p. Official Use. The use of Bureau systems for activities that directly or indirectly support the Bureau's or the Department of the Treasury's mission and the accomplishment of related goals and objectives.

q. Sensitive information. Any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not 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. The terms "loss," "misuse," and "unauthorized access" can involve unauthorized manipulation of data, destruction or loss of data, denial of service, inability to complete or perform a mission, or willful or negligent disclosure of information.

r. System Integrity. Assurance that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

**6. BACKGROUND.** Minimum security requirements for sensitive information include the implementation of:

a. Identification and Authentication. Access shall be controlled and limited based on positive user/entity identification and authentication mechanisms that support minimum requirements for access control, individual accountability, least privilege, and system integrity. Systems shall include a mechanism to require users and entities to uniquely identify and authenticate themselves to the system before performing any actions.

b. Access control. Access control measures limit access to information or resources of an IT system to authorized users, programs, processes, or other

DATE January 21, 2004

---

authorized systems. They shall provide protection from unauthorized alteration, loss, unavailability or disclosure of information. Access controls shall follow the principle of least privilege and separation of duties, and shall require the use of unique identifiers. Systems shall maintain and protect authentication data that contains information for verifying the identity of individual users (e.g., passwords) to prevent access by an unauthorized user.

c. Automatic Account Lockout. Systems will be configured to lock an account after a specified number of consecutive failed logon attempts, in compliance with IT security standards.

d. Automatic Session Lockout. Systems shall enforce threshold limits for the amount of time a session is inactive before the session timeout feature is invoked, in compliance with IT security standards.

e. Individual Accountability. Accountability links actions to the user or entity that performed the action. Accountability means that users can be held responsible for their actions.

f. Least Privilege. Users and entities will be granted the most restrictive set of privileges needed for the performance of authorized tasks. Least privilege limits the damage that can result from accident, error, or unauthorized use of an IT system.

g. Separation of Duties. Duties and responsibilities of critical functions shall be divided and separated among different individuals so that no individual shall have all necessary authority or systems access that could result in fraudulent or criminal activity. Separation of duties shall prevent a single individual from being able to disrupt or corrupt a critical security process.

h. Warning Banner. Systems accessible within the Bureau and Treasury shall display Department of Justice approved sign-on banners where technically practical. Systems accessible to the public shall provide a security and privacy statement at every entry point.

i. Data Integrity. Safeguards shall be in place to detect and minimize the inadvertent modification or destruction of data, and to detect and prevent the malicious destruction or modification of data. Mechanisms that enforce access control and other security functions shall be continuously protected against tampering and/or unauthorized changes.

j. Audit Trail. The audit trail shall be sufficient in detail to reconstruct events, to determine the cause or magnitude of compromise, should a security violation or malfunction occur or be suspected. Audit trails shall be protected from modifications, unauthorized access, or destruction. As a minimum, log files shall show the identity of

DATE January 21, 2004

each person and device, successful and unsuccessful logon attempts, applications and files accessed and time/date stamps. Activities, including security relevant actions associated with processing and administrative actions that might modify, bypass, or negate security controls shall be logged. Administrative actions shall be logged to show time/date, identity, and actions taken (e.g., software changes, add or delete accounts, system time clock changes, etc.). Audit trails will be recorded and retained in accordance with the Bureau's Records Management Program.

k. Configuration Management. New systems, modifications to existing systems and related documentation (hardware, software, firmware, telecommunications, documentation, test environments, and test documentation) shall comply with configuration management policy to ensure the system is protected against unauthorized modifications before, during, and after system implementation.

l. Physical Security. Physical protection measures shall be implemented for all facilities where sensitive information is processed, transmitted, or stored based on the level of risk. Access to equipment and data shall be limited to authorized personnel. Controls shall be based on the level of risk and shall be sufficient to safeguard these assets against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

m. Personnel Security. All personnel (employees and contractors) who have access to any sensitive or classified information must have had the necessary personnel investigation completed, have the required authorizations, and have been granted appropriate security background clearances and have a need to know.

n. Contingency Plan. Systems shall have plans that describe interim measures to recover IT services following an emergency or system disruption. Interim measures may include relocation of IT systems and operations to an alternate site, recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods

## **7. RESPONSIBILITIES.**

a. Associate Directors, Designated Accrediting Authorities, Plant Managers and Office Chiefs shall:

(1) Determine the level of sensitivity of information; ensure that systems meet Federal, Treasury, and Bureau IT security requirements; and that necessary safeguards are in place to adequately protect the availability, integrity and confidentiality of Bureau information and systems that support their program areas.

(2) Ensure a complete understanding of risks, especially increased risks resulting from interconnecting with other programs or systems over which program officials have little control.

DATE January 21, 2004

---

(3) Identify systems used to process highly sensitive information and notify the Office of Critical Infrastructure and IT Security to request assistance in determining the appropriate method for purging data, prior to disposal or redeployment of computer equipment and storage devices.

(4) Ensure all statements of work and contract vehicles identify and document specific IT security requirements for outsourced services and operations that are required of the contractor. Outsourced services and operations shall adhere to the Federal, Treasury, and Bureau's IT security policies.

b. Supervisors shall:

(1) Ensure that users have the proper level of personnel security clearance for the information they will be accessing.

(2) Approve system access based on job requirements and "need-to-know", and ensure that access authorizations maintain appropriate separation of duties.

(3) Update access authorizations when requirements change (e.g. change of duties, job transfer, or termination).

c. Users shall:

(1) Comply with all IT security policies and procedures, and shall not disable or circumvent any IT security features including, but not limited to, antivirus protection, password protected screen-savers, or access controls.

(2) Use only Bureau-approved IT equipment, devices or systems to process, store, or transmit Bureau information. Bureau-approved IT equipment, systems and devices are evaluated by the Office of Critical Infrastructure and IT Security and approved by the Configuration Control Board.

(3) Use only Internet service and e-mail accounts issued by the Bureau. Other Internet Service Provider or e-mail accounts may not be installed or used on Bureau equipment, and may not be used to communicate Bureau information. Transmission of sensitive Bureau information to any privately owned e-mail account, automatic forwarding of Bureau e-mail to any address outside the Bureau, automatic forwarding of personal e-mail to a Bureau e-mail address, instant messaging, storing information on the Internet, and peer-to-peer file sharing are prohibited.

(4) Not install standalone or networked hardware, (e.g., computers, internal components or peripherals, modems, network devices).

DATE January 21, 2004

---

(5) Ensure adequate controls are implemented prior to creating, storing, processing or transmitting sensitive information.

(6) Not connect or synchronize any device that has not been approved to any computer containing Bureau information. Conversely, no Bureau-owned device may be synchronized with or connected to any non-Bureau device.

(7) Use only licensed and approved operating systems and applications on Bureau equipment. Users are prohibited from downloading or installing software.

(8) Not use Bureau computer resources for personal business such as taxes, private commercial business, games, illegal activities, unauthorized access to any computer system, partisan political activity, or sexually-explicit, offensive or discriminatory materials.

(9) Ensure adequate safeguards are in place to protect information stored on removable media, displayed, downloaded, copied, transmitted, or printed from unauthorized access.

(10) Report any occurrence that may affect a Bureau IT system to the Help Desk. For example, suspected virus infections, unusual system activity, or suspected or actual IT security violations.

(11) Ensure that all media, such as diskettes or compact disks (CDs) brought into the Bureau are scanned for viruses prior to use on any Bureau system.

(12) Ensure that computers are logged off, locked, or use a password-protected screen saver when unattended. Computers connected to the network must be left turned on to receive software and antivirus updates, and security patches.

d. The Configuration Control Board shall:

(1) Evaluate and approve new systems and changes to existing systems (hardware, software, and system configurations), and maintain evaluation and approval documentation.

(2) Ensure that the IT security is fully integrated into the systems lifecycle.

e. The CIO Directorate shall:

(1) Ensure that only approved hardware, software, and configurations are installed in the Bureau's IT environment.

DATE January 21, 2004

(2) Install or authorize the installation of all approved computer hardware, software, and telecommunications equipment.

(3) Maintain or authorize the maintenance of computer hardware, software, and telecommunications equipment.

f. The Office of Information Technology Operations shall:

(1) Use approved methods to sanitize computer media prior to disposal, dispatch to external organization for maintenance, or re-assignment to another user; and document, and maintain records certifying that such sanitization was performed.

(2) Ensure that Interconnection Security Agreements are in place prior to connecting Bureau systems to non-Bureau systems.

g. The Office of Critical Infrastructure and Information Technology Security shall:

(1) Ensure that the provisions for confidentiality, integrity, and availability of all information transmitted, stored or processed are in compliance with applicable statutes, regulations, guidelines, and standards.

(2) Establish policy, procedures, and standards to ensure protection of the Bureau's information technology assets throughout the systems lifecycle.

(3) Ensure that IT investment and lifecycle processes identify the system sensitivity, security and privacy requirements, the level of security risk, and include plans to remediate identified security weaknesses.

(4) Ensure and validate that a risk management process is conducted throughout the systems lifecycle.

(5) Evaluate the adequacy of, and sets standards for security controls, including controls for system interconnections, points of entry and methods of access into the Bureau IT environment (e.g. firewalls, modems, virtual private networks), identification and authentication, access controls, encryption, and media sanitization.

(6) Conduct the IT security awareness and role-based training program.

(7) Coordinate the Bureau's Computer Security Incident Response Capability (CSIRC) and conduct internal investigations related to the security or inappropriate use of the Bureau's IT assets.

(8) Audit system records and activities to test for adequacy of technical, operational and management controls, to ensure compliance with established policy,

DATE January 21, 2004

procedures, and standards and to recommend any indicated changes in controls, policy, or procedures.

(9) Ensure that Bureau information is processed, stored, or transmitted by authorized systems; and that unauthorized software and hardware is not present in the Bureau's IT environment.

(10) Authorize the confiscation or removal of any data or IT system suspected to be the object of inappropriate use or violation of Bureau security policy.

(11) Conduct reviews to ensure that security requirements in contracts are implemented and enforced.

(12) Evaluate statements of work, contract proposals, interagency agreements, and interconnection security agreements for compliance with security policies, audit requirements, and controls.

(13) Maintain records of authorized exceptions and waivers to IT security policy, procedures, standards, minimum security controls, and controls documented for system certification and accreditation.

**8. SANCTIONS FOR MISUSE.** Unauthorized, improper, or insecure use of Bureau systems access may result in suspension of privileges, disciplinary action (up to and including termination), and/or criminal prosecution depending on the nature and severity of the misuse.

**9. EXCEPTIONS AND WAIVERS.** Exceptions and waivers to this policy require that a written request be submitted to the Chief, Office of Critical Infrastructure and Information Technology Security. Bureau Chief Information Officer (CIO) approval must be received before implementing an exception to, or waiver of, this policy.

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

<SIGNED>

Ronald W. Falter

Associate Director (Chief Information Officer)

DISTRIBUTION –