

No. 10-08.35

INFORMATION TECHNOLOGY SECURITY POLICY AND PROCEDURES MANUAL



Department of the Treasury

BUREAU OF ENGRAVING AND PRINTING

MANUAL

No. 10-08.35

DATE August 1, 2005

INFORMATION TECHNOLOGY SECURITY POLICY AND PROCEDURES MANUAL

The Bureau of Engraving and Printing (BEP) Information Technology (IT) Security Program has been established to ensure protection of the information and information systems that support the operations and assets of the Bureau (BEP IT systems) and to manage risk throughout the information system lifecycle.

This manual establishes a uniform set of security policies, standards, and procedures for all BEP IT systems and the personnel and contractors who use, maintain, and develop them. Management, operational, and technical controls outlined in this manual, provide the foundation to ensure that BEP IT systems and resources are implemented, operated, and maintained with required security planning, risk management, training, controls, technical standards, periodic security evaluation and testing, certification, and accreditation.

This manual implements Department of the Treasury IT security policies at the Bureau level; and is consistent with Federal laws and regulations, and policies, standards and procedures issued by the Office of Management and Budget (OMB) and the Department of Commerce National Institute of Standards and Technology (NIST).

<SIGNED>

Thomas A. Ferguson
Director

Distribution – E

CONTENTS**Information Technology Security General Policy**

1. Purpose and Scope	1
2. Policy	1
3. References	1
4. Supersession	3
5. Responsibilities	3
6. Sanctions for Non-Compliance	10
7. Office of Primary Responsibility	10

Section 1 – Management Controls

<u>Ch.</u>	<u>Date</u>	<u>Title</u>	<u>Page</u>
1-1		Capital Planning and Investment	
1-2		System Development Life Cycle	
1-3		Contractors and Outsourced Operations	
1-4		Performance Measures and Metrics	
1-5		Critical Infrastructure Protection (CIP)	
1-6		Security Change Management	
1-6-1	5/21/2001	IT Configuration Control Board	1-6-1(1)
1-7		Security Architecture	
1-8		Risk Management	
1-9	1/4/2005	Certification and Accreditation	1-9(1)
1-10		IT Security Review/Assistance Program	
1-11		Security Working Groups and Forums	
1-12	3/31/2005	Disciplinary Action Guidance	1-12(1)
1-13	3/31/2005	Waivers and Exception Guidance	1-13(1)

Section 2 – Operational Controls

<u>Ch.</u>	<u>Date</u>	<u>Title</u>	<u>Page</u>
2-1		Personnel Security	
2-1-1	7/31/2002	IT Security Awareness and Training	2-1-1(1)
2-2	1/22/2007	Protecting Sensitive & PII	2-2(1)
2-2-1	5/21/2001	Electronic Mail	2-2-1(1)
2-2-2	6/6/2001	Internet	2-2-2(1)
2-3		Physical Security	
2-3-1	3/2/1998	Access to the BEP Computer Facility	2-3-1(1)
2-4	5/4/2007	IT Storage Media Controls	2-4(1)
2-5		Communication Security	
2-5-1		Voice Communication Security	
2-5-2		Data Communications Security	
2-5-3	1/7/2007	Wireless Communications Security	2-5-3 (1)
2-5-4		Overseas Communications Security	
2-6		Equipment	
2-6-1		Servers	
2-6-3		Laptop Computers	
2-6-4	7/6/2001	Personal Digital Assistant (PDA)	2-6-4(1)
2-6-5		Converging Technologies	
2-6-6		Privately Owned Equipment and Software	
2-6-7	9/21/2006	USB Storage Devices	2-6-7 (1)
2-7	5/15/2007	Computer Security Incident Response Capability (CSIRC)	2-7(1)
2-8		Contingency Planning	
2-9		System Maintenance	
2-10		Access to Sensitive Information	
2-11	1/21/2004	Protecting IT Resources	2-11(1)

Section 3 – Technical Controls

<u>Ch.</u>	<u>Date</u>	<u>Title</u>	<u>Page</u>
3-1	3/31/2005	Identification and Authentication	3-1(1)
3-1-1	3/31/2005	Passwords	3-1-1(1)
3-1-2		Smart Cards	
3-1-3		Biometrics	
3-2	10/27/2005	Information Technology Access Controls	3-2(1)
3-2-1	12/18/1986	ADP Security Matrices	3-2-1(1)
3-2-2	5/22/1997	Management Information System Security Profiles	3-2-2(1)
3-2-3	7/30/1987	Mainframe Security Software Policy	3-2-3(1)
3-3	5/21/2001	Remote Access to Computer Systems	3-3(1)
3-4		Warning Banner	
3-5		Network Connectivity	
3-6		Network Monitoring	
3-7	6/27/2001	Gateways/Firewalls	3-7(1)
3-8		Electronic Mail	
3-9		Internet Security	
3-10		Mobile Code	
3-11	3/1/1993	Protecting Bureau Computers from Computer Viruses	3-11(1)
3-12		Penetration Testing and Vulnerability Assessment	
3-13		Audit, Audit Reduction, and Audit Review	
3-14	1/22/2007	Encryption	3-14(1)
3-15		IT Product Assurance	

Section 4 – Appendices

<u>Ch.</u>	<u>Date</u>	<u>Title</u>	<u>Page</u>
A	10/6/2005	Glossary	A (1)
B	3/31/2005	Supersession	B (1)

INFORMATION TECHNOLOGY SECURITY GENERAL POLICY

1. PURPOSE AND SCOPE. This manual delineates policies, procedures, roles, and responsibilities for ensuring adequate security to protect the availability, integrity and confidentiality of information and information systems that support the operations and assets of the Bureau, including those provided or managed by another agency, contractor, or other source.

2. POLICY. The Bureau's Information Technology Security Program provides for the management of risk throughout the information systems lifecycle. Periodic assessments are conducted to evaluate the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Bureau of Engraving and Printing (Bureau/BEP). These assessments provide the basis for cost-effective policies, procedures, plans, and controls to reduce risk to an acceptable level.

Bureau policy requires compliance with the Federal Information Security Management Act (FISMA); OMB Circular A-130; Treasury Directive Publication (TD P) 85-01, "Treasury Information Technology Security Program;" and other applicable legislation and implementing guidance.

3. REFERENCES.

- a. [TD P 85-01](#), "Treasury Information Technology Security Program," current version.
- b. Public Law 107-347, "E-Government Act of 2002," Title III, Federal Information Security Management Act (FISMA) of 2002, December 17, 2002. (This is an authority.)
- c. OMB Circular No. A-130, "Management of Federal Information Resources," Appendix III (Rev), November 2000. (This is an authority.)
- d. "Information Technology Management Reform Act of 1996" (Clinger-Cohen Act) (PL 104-106, Div. E). (This is an authority.)
- e. Government Performance and Results Act of 1993 (PL 103-62). (This is an authority.)
- f. Privacy Act of 1974, (5 U.S.C. 552a). (This is an authority.)
- g. Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure

Identification, Prioritization, and Protection,” December 17, 2003. (This is an authority.)

- h. 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. NIST publications are available at <http://csrc.nist.gov/publications>. Some of these are:
1. “Standards for Security Categorization of Federal Information and Information Systems,” FIPS Publication 199, February 2004;
 2. “Guidelines for Security of Computer Applications,” FIPS Publication 73, June 1980;
 3. “Security Considerations in the Information System Development Life Cycle,” SP 800-64 Revision 1, June 2004;
 4. “Guide for Mapping Types of Information and Information Systems to Security Categories,” SP 800-60, June 2004;
 5. “Security Guide for Interconnecting Information Technology Systems,” SP 800-47, September 2002;
 6. “Guide for the Security Certification and Accreditation of Federal Information Systems,” SP 800-37, May 2004;
 7. “Security Self-Assessment Guide for Information Technology Systems,” SP 800-26, November 2001;
 8. “Contingency Planning Guide for Information Technology Systems,” SP 800-34, June 2002;
 9. “Risk Management Guide for Information Technology Systems,” SP 800-30, July 2002;
 10. “Guide for Developing Security Plans for Information Technology Systems,” SP 800-18, December 1998; and
 11. “An Introduction to Computer Security: the NIST Handbook,” SP 800-12, October 1995;

4. SUPERSESSION. BEP Circular No. 10-08.30, “Information Technology Security General Policy,” dated October 18, 2004 is superseded.

5. RESPONSIBILITIES. FISMA and OMB Circular A-130 specifically assign responsibility for information technology (IT) security to the Director of the Bureau. The Director may delegate responsibility to business process owners (the Associate Directors) in some cases. Under FISMA, the Associate Director (Chief Information Officer) has responsibility for developing and maintaining a Bureau-wide information security program and for monitoring compliance across the organization. Treasury Information Technology Security Program Policy TD P 85-01 also defines specific roles and responsibilities.

a. The Director:

1. Establishes a Bureau-wide IT Security Program to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information collected and maintained by BEP and information systems operated by BEP or by a contractor or other organization on behalf of the Bureau;
2. Certifies that adequate security exists for Bureau systems and describes security and other material weaknesses in these systems in the Bureau Head's annual report to the Secretary under TD 40-04, "Treasury Internal (Management) Control Board";
3. Ensures compliance with FISMA, and other applicable Executive, legislative, Treasury, and Bureau IT security policy, regulation, and guidance;
4. Ensures that information security management processes are integrated with the Bureau's strategic and operational planning processes;
5. Ensures that senior Bureau officials provide security for the information and information systems that support the operations and assets under their control;
6. Appoints Authorizing Officials, also referred to as Designated Accrediting Authorities (DAA), and delegates to them the responsibility for accrediting the IT systems that support their business units;
7. Delegates to the Associate Director, Chief Information Officer (AD (CIO)) the authority and responsibility to manage the Bureau-wide IT Security Program and to ensure compliance with Executive, legislative, Treasury, and Bureau IT security policy, regulation, and implementing guidance;
8. Ensures that the Bureau-wide IT security program is adequately resourced and that the Bureau has trained personnel sufficient to assist the Bureau in

- complying with the requirements of FISMA and other applicable IT security policy and implementing guidance; and
9. Ensures that the AD (CIO), in coordination with other senior Bureau officials, reports annually to the Director on the effectiveness of the Bureau information security program, including progress of remedial actions as required by FISMA.
- b. The Associate Director (CIO):
1. Develops and maintains the Bureau-wide information security program, polices, procedures, and control techniques to address all applicable requirements of Executive, legislative, and Treasury policy, regulation, and guidance;
 2. Trains and oversees personnel with significant responsibilities for information security with respect to those responsibilities;
 3. Administers an IT security awareness and training program for Bureau and contractor personnel, and other users of Bureau information systems;
 4. Assists senior agency officials and DAAs concerning their IT security responsibilities;
 5. Ensures that Bureau major information systems and their interdependencies with other systems and networks are identified, risks are assessed and mitigated, and the systems are authorized to operate by the Designated Accrediting Authority;
 6. Evaluates the security of, and approves or disapproves all Interconnection Security Agreements (ISAs) for connections between Bureau and external systems;
 7. Designates the Chief, Office of Critical Infrastructure and IT Security as the Information Systems Security Manager (ISSM) responsible for managing and overseeing the bureau IT security program and for carrying out the CIO's IT security and information protection responsibilities in order to comply with Executive, legislative, Treasury, and Bureau IT security policy, regulation, and guidance; The ISSM must be a Bureau employee;
 8. Appoints a Bureau Information System Security Officer (ISSO) for each system; Bureau ISSOs are OCIITS employees;
 9. Appoints Bureau certification agents and ensures the independent certification of information systems; Bureau certification agents are OCIITS

employees or contractors; and

10. Coordinates with other senior Bureau officials, to report annually to the Director on the effectiveness of the Bureau information security program, including progress of remedial actions as required by FISMA.

c. Senior Bureau officials and Designated Accrediting Authorities:

1. Identify systems under their control and ensure security for the information and information systems that support their operations; and ensure that these information systems are certified and accredited;

2. Coordinate with Office of Critical Infrastructure and IT Security to determine the sensitivity of information, assess risk, determine the appropriate level of security, and implement policies, procedures, and safeguards to cost effectively reduce risk to an appropriate level;

3. Periodically test and evaluate information security controls to ensure that they are effectively implemented; and

4. Establish and test plans and procedures to ensure continuity of operations for information systems that support the operations and assets under their control.

d. The DAAs for the Bureau are senior Bureau officials appointed by the Director, who manage, or are principal business owners of a BEP function supported by an information system. The DAA may also appoint an Authorizing Official Designated Representative to carry out DAA duties. The only duty that cannot be delegated by the DAA is the accreditation decision and signing of the accreditation letter. The DAA shall:

1. Authorize processing of information prior to system implementation by accepting the level of risk which has been identified through the certification process;

2. Implement all applicable protection policies prescribed by the Treasury and BEP CIOs;

3. Ensure that structured and disciplined configuration management procedures are followed;

4. Ensure that periodic testing and evaluation of security policies, procedures and controls for authorized systems is conducted with a frequency based on risk, but no less than annually;

5. Ensure that systems are re-certified and re-accredited every 3 years and whenever there is a significant change to the system or its operational environment; and
 6. Ensure that, for risks that require remediation, a Plan of Action and Milestones (POAM) is prepared, monitored, and reported upon.
- e. Authorizing Official's Designated Representative (DAA's Representative). The DAA may designate a representative to act on the DAAs behalf during the certification and accreditation process. The DAA's Representative may:
1. Develop or review and accept security plans;
 2. Determine risk to Bureau operations, assets, and resources; and
 3. Participate in periodic risk assessments, monitor and report on risk mitigation activities, and participate in or lead other certification and accreditation activities.
- f. Certification Agent shall:
1. Coordinate certification and accreditation activities;
 2. Conduct and prepare a formal report documenting the results of a comprehensive evaluation of the management, operational and technical security controls in the information system;
 3. Certify the effectiveness of those controls in the specific environment of operation, and document vulnerabilities in the system after the implementation of such controls;
 4. Recommend corrective actions to reduce or eliminate vulnerabilities in the information system; and
 5. Perform periodic reviews to validate the certification and accreditation.
- g. The Chief, Office of Critical Infrastructure and IT Security (OCIITS) is the Senior Information Security Officer for the Bureau and serves as the Information Systems Security Manager (ISSM). The ISSM is the AD (CIO)'s principal advisor on IT security matters and is responsible for developing and overseeing the Bureau's IT security program. The Chief OCIITS:
1. Develops, documents, implements, manages, and evaluates the effectiveness of the Bureau-wide information security program, and ensures compliance with law, regulation, and policy. This includes:

- a) Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
 - b) Development and promulgation of policies and procedures that cost-effectively reduce information security risks to an acceptable level, ensure that information security is addressed throughout the life cycle of a system, and ensure compliance with Executive, legislative, and Treasury policy and guidance;
 - c) Evaluation, design and implementation of technologies and controls to ensure the appropriate level of security;
 - d) IT security technical assistance;
 - e) Establishment of and compliance oversight of minimally acceptable system configuration requirements and plans for providing adequate information security for networks, facilities, and systems;
 - f) IT security awareness training to inform personnel, including contractors and other users of information systems, of information security risks associated with their activities, and their responsibilities in complying with Treasury and Bureau policies and procedures designed to reduce these risks;
 - g) Oversight for periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually;
 - h) Establishment and maintenance of a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices;
 - i) Establishment and maintenance of procedures for detecting, reporting, and responding to security incidents, consistent with federal and Treasury standards and guidelines, including mitigating risks associated with such incidents before substantial damage is done; and
 - j) Oversight of plans, procedures and tests to ensure continuity of operations for information systems that support the operations and assets of the Bureau;
2. Serves on the Bureau's IT Configuration Control Board and co-chairs the

- Architecture and Security Subcommittee of the IT Capital Investment Review Committee. Evaluates the impact of changes on the security posture of the Bureau's IT systems;
3. Evaluates and approves or disapproves exceptions to IT security policies, procedures, controls, or configurations; and maintains records of all approved IT security related exceptions;
 4. Evaluates and makes recommendations to the CIO regarding the approval of Interconnection Security Agreements;
 5. Oversees the activities of the Bureau ISSOs and certifiers; and
 6. Coordinates the planning, implementation, and monitoring of Critical Infrastructure Protection (CIP) requirements, and ensures the identification of CIP functions and assets Bureau-wide.
- h. The Information Systems Security Officer (ISSO):
1. Ensures the implementation of all Bureau information system security policies and guidelines;
 2. Implements and ensures compliance with, security requirements for all Bureau information systems;
 3. Oversees security testing of hardware and software for certification purposes, and evaluates technical, operational, and management controls related to IT security for all Bureau systems to ensure they are operating as intended;
 4. Serves on the Bureau's Configuration Control Board;
 5. Evaluates the impact of changes on the security posture of the Bureau's IT systems;
 6. Coordinates system, hardware, software, or procedural changes that have an impact on IT security;
 7. Evaluates interfaces with external systems to ensure compliance with security requirements and appropriate security of those systems and integrity of Bureau information; and
 8. Provides technical and policy advice to information system owners, program officials, Designated 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.

- i. The Information System Owner is the program manager responsible for ensuring that the IT system meets program area functional requirements. The Information System Owner:
 - 1. Approves system requirements and modifications, and ensures that structured configuration management procedures are followed;
 - 2. Ensures system requirements and modifications are tested, and evaluates and approves system tests and test results, prior to system modification or implementation;
 - 3. Develops and maintains the system security plan;
 - 4. Periodically reviews and re-validates system access permissions;
 - 5. Ensures the system is deployed and operated according to the security requirements documented in the IT security plan; and
 - 6. Prepares a written recommendation for the DAA or DAA's Representative concerning the acceptance of and justification for accepting residual risk to the program of operating the IT system.

- j. System administrators, developers, and system support personnel:
 - 1. Are responsible for developing, operating, maintaining, and disposing of systems in compliance with Bureau information security policies and procedures;
 - 2. Perform functions for which they have been authorized, and only on the systems for which the individual is assigned;
 - 3. Follow structured configuration management procedures, and implement only those systems, modifications, configurations and controls approved by the Bureau's Configuration Control Board;
 - 4. Shall not probe or attempt to gain unauthorized access to any computer system;
 - 5. Shall not attempt to test or strain any security mechanisms or conduct security monitoring or investigation without authorization from the Chief, OCIITS; and
 - 6. Ensure that IT security is integrated into the information systems lifecycle.

- k. Employees, contractors, and users of BEP information systems.
 - 1. Must comply with the “BEP Information Technology Rules of Acceptable Use” and all information security policies and procedures;
 - 2. Are required to complete IT security training specified by the OCIITS at least annually;
 - 3. Are accountable for all activity performed under their accounts; and
 - 4. Are required to report all actual, suspected, or potential information security violations and incidents to the Manager, Information Technology Security Division (ITSD).

6. SANCTIONS FOR NON-COMPLIANCE. Failure to comply with the provisions of the Bureau IT Security Program policy may result in suspension of privileges, disciplinary action (up to and including removal), and/or criminal prosecution, depending on the nature or severity of the violation.

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

MANUAL

DATE May 21, 2001

1-6-1 IT CONFIGURATION CONTROL BOARD

1. PURPOSE AND SCOPE. This section establishes a Bureau of Engraving and Printing (Bureau/BEP) Configuration Control Board to coordinate the management of changes made to automated information systems hardware, software, firmware, communications, and operating procedures throughout the development and operational systems lifecycle. Configuration management is necessary to ensure the effective use of funds, the efficient use of information resources, and the maintenance of the integrity of BEP's automated information systems. This policy applies to all Bureau automated information systems and information processing hardware and software.

2. POLICY. It is the policy of the Bureau to integrate security into the information technology hardware and software development lifecycle. This ensures that security elements of a system are thoroughly documented and included as part of a routine development process. Configuration control is essential for preserving the integrity of the Bureau's Enterprise Architecture. The resulting coordination of business, technical and security requirements throughout the systems lifecycle is more cost effective than adding unidentified requirements later in the planning, development or implementation process.

A Configuration Control Board is created which will include representation from system design, operational administration, procurement and budgeting, and security components. The Board will develop configuration management policy, coordinate the planning for and implementation of new hardware and software acquisitions, and review and coordinate the acquisition and installation of software modifications, hardware additions, and changes to hardware and software. This review is intended for all significant changes, whether procured from commercial or Government sources or developed in-house.

3. REFERENCES.

Guidelines for Security of Computer Applications, Federal Information Processing (FIPS) Publication 73, June 1980.

Computer Security Act of 1987 (PL 100-235).

OMB Circular No. A-130, Management of Federal Information Resources, (Rev), November 2000.

Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) (PL 104-106, Div. E).

MANUAL

DATE May 21, 2001

Government Performance and Results Act of 1993 (PL 103-62).

“Government Information Security Reform Act,” 44 USC Sections 3531-3536 (PL 106-398, Title X, Subtitle G).

4. RESPONSIBILITIES. Most components within the organization of the Associate Director (Chief Information Officer) have some role in ensuring the integration of security into Bureau systems and processes. In addition, user components (such as Office of Currency Production, Office of Management Control, Office of Financial Management, etc.) frequently will have an interest in ensuring adequate controls exist for systems they develop or use. Therefore, this Circular establishes a “team approach” that crosses organizational lines for managing security.

a. A Configuration Control Board is established which will consist of the following members. Additional members may be added on an ad hoc basis, depending upon the system being reviewed.

- (1) Manager, Information Technology Security Division
- (2) Manager, Systems Support Division
- (3) Manager, Enterprise Systems Division
- (4) Assistant Chief Information Officer (WCF)
- (5) Manager, Web Development Division
- (6) Manager, Customer Support Division

b. The Configuration Control Board will meet as necessary to accomplish its responsibilities. These meetings will occur during the initial stages of planning and budgeting process, during the process of system review and modification, and in the close-out and final audit phase of a system.

c. The Configuration Control Board will ensure that the requirements of the user community and the interrelationship among the operational, programming, database, and web components of the Associate Director (CIO) are coordinated for proposed, planned, or substantially modified hardware and software, including new applications. Designation of responsibility for implementation of change, access, and functional interrelationships is critical to developing logical and non-intrusive security controls.

d. This Board shall develop basic “models” or “maps” of Bureau systems to use as baselines for system definition and to assess configuration change requirements. A basic configuration model includes:

- (1) System description and descriptor method for logically identifying associated modifications and additions.
 - (a) system documentation, diagrams or maps

MANUAL

DATE May 21, 2001

- (b) communications
- (c) access map/discussion of privileges
- (2) Procedures for
 - (a) allowing access and change
 - software
 - hardware
 - firmware
 - (b) system rules
 - internet
 - intranet
 - remote access
 - workstation
 - virus protection
- (3) Software licenses
 - (a) owners
 - (b) procedures
- (4) Future requirements
 - (a) planned upgrades
 - (b) proposed upgrades
- (5) Hardware procedures
 - (a) assignment
 - (b) relocation
 - (c) disposal
- (6) Security features
 - (a) physical protection/controls
 - (b) audit trails
 - (c) software
 - vulnerability (scanning)
 - protection (firewalls, etc.)
 - (d) hardware
 - locks, alarms
 - inventory management

e. Integrating security into the hardware/software change process requires system wide coordination, and is dependent upon the cooperative effort of all members of the Configuration Control Board, plus management and user groups. These efforts are intimate parts of system lifecycle planning. Justification and approval of configuration changes at each stage of the lifecycle will be contingent upon satisfying cost, operational, and security requirements during the various lifecycle stages of IT projects or proposals.

MANUAL

DATE May 21, 2001

Lifecycle Stages of IT Projects or Proposals

- (1) Systems Planning and Design Process Phase
 - (a) security plan
 - (b) feasibility review
 - (c) cost-effectiveness analysis

- (2) Development Phase
 - (a) software development controls (peer review, source data accuracy, etc.)
 - (b) personnel controls (restricted interface, separation of duties, etc.)
 - (c) for a new major system or application, an overall system security plan shall be developed (this will include contingency plans)

- (3) Operational Phase
 - (a) test and evaluation (static review, dynamic testing)
 - (b) enforcement of operational controls (audit logs, physical security reviews, etc.)
 - (c) contingency plan tests

f. Training is one of the most important components of successful system implementation and also of a successful security program. Therefore the Configuration Control Board shall ensure that satisfactory training plans are in place for all project phases. Training shall include both:

- (1) Technical/system administrator training – this includes security system administrator training in system functionality, controls, and procedures, and
- (2) User awareness training.

g. The Configuration Control Board shall develop detailed procedures to comply with the requirements of this policy. These shall include procedures on system or software development projects as well as revisions to procedures for approving individual configuration changes, such as the introduction of new hardware or requests for programming changes or software application procurement. If required, the Board will issue additional policy guidance to ensure full and effective implementation.

MANUAL

DATE January 4, 2005

1-9 CERTIFICATION AND ACCREDITATION OF INFORMATION SYSTEMS

1. PURPOSE AND SCOPE. This section establishes policy and defines responsibilities for ensuring that information systems are certified and accredited (authorized) for operation by the appropriate Designated Accrediting Authority (DAA).

2. POLICY. All major applications and general support systems shall be certified and accredited prior to implementation. Security requirements for other systems shall be documented, and the systems shall be certified and accredited under the general support system on which they operate. Certification and accreditation will be conducted following procedures documented in National Institute of Standards and Technology (NIST) Special Publication 800-37, "Guide for the Certification and Accreditation of Federal Information Systems," May 2004. All interconnections between BEP systems and external systems shall be assessed, documented and authorized by the DAA and the Chief Information Officer (CIO) following procedures specified by NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," September 2002.

Systems must be re-accredited at least every three years, or more often, if there is high risk or potential magnitude of harm. Re-accreditation must also occur prior to a significant change to the system or its operational environment. Periodic reviews will be conducted to ensure that security plans, risk assessments, contingency plans and other security documentation are kept current and reflect current conditions and risks.

3. BACKGROUND. Certification and accreditation are essential activities required by OMB Circular A-130 that support the risk management process and are an integral part of the information technology security program. The objectives of certification and accreditation are to ensure that:

- a. Security is designed into systems and maintained throughout the life cycle of those systems;
- b. A risk management program is in place;
- c. Management has the tools to understand, measure, and make decisions about information technology (IT) resources based on acceptable levels of risk;
- d. Security policy is available and is translated into usable guidelines for managers and employees; and
- e. The Bureau complies with Department of the Treasury and other Federal policies and regulations.

The certification and accreditation process is central to many other IT program requirements, as it ties together all of the elements of a good security program, including risk assessment, security planning, training, development of rules for system use, capital and operational planning.

MANUAL

DATE January 4, 2005

4. REFERENCES.

- a. Treasury Directive Publication (TD P) 85-01, "Treasury Information Technology Security Program," Volume I Policy, Part 1 Sensitive Systems and Part 2 Classified Systems, June 12, 2003.
- b. TD P 85-01, "Treasury Information Technology Security Program," Volume II Handbook, Part 1 Sensitive Systems and Part 2 Classified Systems, June 12, 2003.
- c. Public Law 107-347, "E-Government Act of 2002," Title III, Federal Information Security Management Act (FISMA) of 2002, December 17, 2002. (This is an authority.)
- d. OMB Circular No. A-130, "Management of Federal Information Resources," Appendix III (Rev), November 2000. (This is an authority.)
- e. NIST Federal Information Processing Standard 199, "Standards for Security Categorization of Federal Information and Information Systems," December 2003.
- f. NIST Special Publication 800-37, "Guide for the Certification and Accreditation of Federal Information Systems," May 2004.
- g. NIST Special Publication 800-26, "Self-Assessment Guide for Information Technology Systems," November 2001.
- h. NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.
- i. NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems," July 2002.
- j. NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.
- k. NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," September 2002.

MANUAL

DATE January 4, 2005

5. RESPONSIBILITIES.

- a. The Director appoints Authorizing Officials, also referred to as Designated Accrediting Authorities (DAA), and delegates to them the responsibility for accrediting the IT systems that support their business units.
- b. The Associate Director, Chief Information Officer (CIO), is responsible for:
 1. Ensuring that Bureau information systems and their interdependencies with other systems and networks are identified, risks are assessed and mitigated, and the systems are authorized to operate by the Designated Accrediting Authority;
 2. Evaluating the security of connections between Bureau and external systems, and approving or disapproving all Interconnection Security Agreements (ISAs);
 3. Incorporating summary information on system security plans in the Bureau's Strategic Plan, annual budget submissions, and capital planning documents; and
 4. Carrying out the responsibilities of program official for Bureau general support systems, including accrediting those systems and ensuring that security reviews and periodic independent assessments are performed.
- c. The Chief, Office of Critical Infrastructure and Information Technology Security (OCIITS), is responsible for:
 1. Establishing and maintaining the certification and accreditation program in compliance with law and regulation;
 2. Establishing standards and standard methodologies for the certification and accreditation process;
 3. Reviewing capital requirements and IT system or resource procurements, and system development projects to assure adequacy of security and contingency planning; This includes projects and procurements for systems or equipment which contain embedded IT elements;
 4. Assisting program officials in identifying systems which require accreditation;
 5. Providing technical assistance and administrative guidance for information security planning, implementation, and certification and accreditation;
 6. Evaluating the security of interconnections between Bureau and external systems, and preparing Interconnection Security Agreements;
 7. Conducting risk and vulnerability assessments, monitoring and reporting mitigation efforts for vulnerabilities, coordinating the preparation of IT security plans Bureau-wide, and evaluating and testing management, operational, and technical security controls;
 8. Providing guidance and assistance to program officials for the preparation of

MANUAL

DATE January 4, 2005

- security reviews as required by law or regulation;
 - 9. Maintaining an inventory of major applications and general support systems in compliance with the Federal Information Security Management Act and Treasury policy;
 - 10. Establishing a records retention schedule for accreditation packages;
 - 11. Retaining the official file copy of all accreditation packages; and
 - 12. Reporting to the Department of the Treasury, or other Federal Agencies.
- d. Designated Accrediting Authorities (DAAs) are responsible for:
- 1. Authorizing a system to begin processing based on an evaluation and acceptance of the risk of operations;
 - 2. Ensuring that all information systems and processes are identified to OCIITS, and that the criticality of the system and the sensitivity of the information processed are defined;
 - 3. Ensuring that systems are certified and accredited (authorized to operate, authorized to process information) prior to initial system implementation: For operational systems that have not been accredited, the DAA should ensure that the C&A process is initiated expeditiously;
 - 4. Ensuring that the security of connections between the Bureau and external systems have been evaluated, and approving or disapproving Interconnection Security Agreements (ISAs); and
 - 5. Performing annual program reviews, as required by law or regulation, on major applications and general support systems providing results of reviews to the Chief, OCIITS, for compilation and reporting.
- e. Authorizing Official's Designated Representative (DAA's Representative). The DAA may designate a representative to act on the DAAs behalf during the certification and accreditation process. The DAA's Representative may not authorize system processing (accreditation) but may:
- 1. Develop or review and accept security plans;
 - 2. Determine risk to Bureau operations, assets, and resources; and
 - 3. Participate in periodic risk assessments, monitor and report to OCIITS on risk mitigation activities, and participate in or lead other certification and accreditation activities.
- f. Program Officials may have several systems that support their program area requirements and are responsible for:
- 1. Ensuring that all information systems and processes are identified to OCIITS, and that the criticality of the system and the sensitivity of the information processed are defined;

MANUAL

DATE January 4, 2005

2. Ensuring that systems are certified and authorized for processing (accredit system) prior to initial system implementation; For systems that are operational systems, but have not been accredited, ensure C&A process is initiated expeditiously; and
 3. Ensuring employees and contractors receive information security training.
- g. The Information Systems Security Officer (ISSO) is responsible for:
1. Overseeing security testing of hardware and software for certification purposes, and evaluating technical, operational, and management controls related to IT security for all Bureau systems to ensure they are operating as intended;
 2. Evaluating interfaces with external systems to ensure security requirements are met and the security of those systems is sufficient to protect Bureau information; and
 3. Providing technical and policy advice to information system owners, program officials, Designated 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.
- h. The Information System Owner may be a program or project manager, and must ensure that the IT system meets functional requirements of his/her program area. The Information System Owner is responsible for:
1. Developing and maintaining the system security plan; and
 2. Approving system requirements and modifications, and ensuring that structured configuration management procedures are followed to document system components and baseline configurations and to manage change.
- i. The Certification Agent performs the evaluative and analytic activities necessary prior to accreditation. The Certification Agent is responsible for:
1. Coordinating certification and accreditation activities;
 2. Conducting activities necessary to document the C&A activities and preparing a formal report which evaluates these activities and presents the results in a comprehensive evaluation of the system management, operational and technical security controls;
 3. Certifying the effectiveness of the controls in the specific environment in which the system will operate and documenting vulnerabilities in the system after the implementation of such controls;
 4. Recommending corrective actions to reduce or eliminate vulnerabilities in the information system; and
 5. Performing periodic reviews to validate the certification and accreditation.

MANUAL

DATE January 4, 2005

6. ELEMENTS OF THE CERTIFICATION AND ACCREDITATION PROCESS. The certification and accreditation process employs various techniques to manage information security risk throughout the system life cycle. Whether the system being certified is a general support system or a major application, the process has a number of common requirements. NIST 800-37, "Guide for the Certification and Accreditation of Federal Information Systems", provides an overview of the Certification and Accreditation process. The table below lists key C&A activities from NIST SP 800-37 and relates them to specific guidelines or procedures.

<u>Certification and Accreditation Element</u>	<u>Procedures</u>
a. Identify the security category based upon information sensitivity and criticality.	Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems"
b. Identify requirements for protecting privacy.	Privacy Impact Assessment
c. Identify and evaluate vulnerabilities, threats, and countermeasures to provide a clear understanding of the risk involved in operating a system.	NIST SP 800-30, "Risk Management Guide for Information Technology Systems", July 2002.
d. Assign responsibility for security. Determine security requirements and plan management, operational, and technical security controls. These include: A set of rules of use which delineate responsibilities and expected behaviors of those with access to the system and state consequences for failure to comply; Periodic security and awareness training for all administrators and users of the system which addresses their security responsibilities, the rules of use, rules on system access and permitted activities, and information on where to get security and other assistance; Personnel security requirements which identify responsibilities of individuals or job categories, separation of duties, and required clearances for various system/application access levels, particularly for individuals who are authorized to bypass technical and operational security controls and;	NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems", December 1998

MANUAL

DATE January 4, 2005

<u>Certification and Accreditation Element</u>		<u>Procedures</u>
Enforcement of the principle of "least privilege", and controls to ensure individual accountability.		
e. Interconnection Security Agreements.		NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems", September 2002
f. Test security controls (Security Test and Evaluation).		NIST SP 800-42, "Guidelines on Network Security Testing," October 2003 NIST SP 800-37, "Guide for the Certification and Accreditation of Federal Information Systems", May 2004
g. Incident response capability which will provide help to users when an incident occurs and will also share information on common vulnerabilities and threats with other organizations.		BEP Manual 10-08.29 Computer Security Incident Response Capability (CSIRC) Procedures
h. Contingency plans and procedures that would permit the organization to continue essential functions if the system operation is disrupted. This requires developing alternative capabilities, resources, or strategies and periodically testing them.		NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems", June 2002
i. Action plan indicating actions taken or planned to reduce or eliminate vulnerabilities.		NIST SP 800-37, "Guide for the Certification and Accreditation of Federal Information Systems", May 2004

MANUAL

DATE January 4, 2005

<u>Certification and Accreditation Element</u>	<u>Procedures</u>
<p>j. Certification, a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements for the system.</p>	<p>NIST SP 800-37, "Guide for the Certification and Accreditation of Federal Information Systems", May 2004</p>
<p>k. Accreditation, the Designated Accrediting Authorities decision to accept the associated risks, authorizing the system to operate based on information and recommendations provided through the certification process.</p>	<p>NIST SP 800-37, "Guide for the Certification and Accreditation of Federal Information Systems", May 2004</p>
<p>l. Maintain and monitor system security (configuration management, security control monitoring, annual security assessment, and status reporting).</p>	<p>NIST SP 800-26, "Self-Assessment Guide for Information Technology Systems", November 2001</p>
<p>Re-accredit the system at least every three years or more often if there is high risk or potential magnitude of harm. Re-accreditation must also occur prior to the implementation of a significant change to the system or its operational environment. Examples of significant changes to an information system that should be reviewed for possible re-accreditation include but are not limited to:</p> <ul style="list-style-type: none"> • Installation of a new or upgraded operating system, middleware component, or application; • Modifications to system ports, protocols, or services; • Installation of a new or upgraded hardware platform or firmware component; or • Modifications to cryptographic modules or services. <p>Changes in laws, directives, policies or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a re-accreditation action.</p>	<p>NIST SP 800-37, "Guide for the Certification and Accreditation of Federal Information Systems", May 2004</p>

MANUAL

DATE January 4, 2005

All systems shall have a certification package consisting, at a minimum, of the following:

- a. Security Category
- b. System Security Plan
- c. Final Risk Assessment
- d. Contingency Plan
- e. Security Test and Evaluation (ST&E) report
- f. Action Plan
- g. Security Assessment Report
- h. Certification Statement

The DAA shall grant one of three types of accreditation: full, interim, or denied.

Full
Accreditation

Full accreditation shall be granted when:

- The certification package is complete.
- No corrective actions are required.
- Residual risks are acceptable to the DAA.

Interim
Authority to
Operate
(IATO)

An IATO is rendered when the identified security vulnerabilities in the information system are significant but can be addressed in a timely manner. The IATO provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the Bureau for a specified period of time. The following documentation, at a minimum, shall be provided for an IATO:

- Security Categorization
- System Security Plan
- Risk Assessment
- Security Test and Evaluation Plan
- Action Plan schedule for correcting the deficiencies to achieve full accreditation. This plan must be mutually acceptable to the Program Official and the DAA.

Denied

If the system cannot meet IATO requirements or the residual risks are considered by the DAA to be too high to accept, the accreditation shall be denied. The system may not be placed into operation until at least an IATO can be granted.

MANUAL

DATE January 4, 2005

The DAA may grant an IATO for a specified period of time based on the security category. For moderate risk category systems, the IATO shall not exceed 6 months. For high risk category systems, the IATO shall not exceed 3 months. No extensions are permitted. If after the specified period of time the security-related deficiencies have not been adequately addressed, the system should be taken out of operation, otherwise operation of the system may be considered a material weakness. If the security-related deficiencies have been adequately addressed the system should be fully accredited.

Accreditation shall be the official management authorization to operate an IT system based on the following:

- a. A particular mode of operation;
- b. A prescribed set of security safeguards as defined in the System Security Plan;
- c. A defined threat, with stated vulnerabilities and safeguards
- d. A given operational environment;
- e. A stated operational concept;
- f. A stated interconnection to other IT;
- g. An operational necessity; and
- h. An acceptable level of risk for which the DAA has formally assumed responsibility.

The accreditation package shall consist of the certification package and the accreditation decision letter.

7. WAIVERS AND EXCEPTIONS. No waivers or exceptions shall be granted for the certification and accreditation process.

MANUAL

DATE March 31, 2005

1-12 DISCIPLINARY ACTION GUIDANCE

1. POLICY. Failure to comply with the provisions of the Bureau of Engraving and Printing (BEP) IT Security Program policy may result in suspension of privileges, disciplinary action (up to and including removal), and/or criminal prosecution, depending on the nature or severity of the violation and the number of prior offenses. Non-BEP federal employees or BEP contractors who fail to comply with Bureau security policy are subject to having their access to BEP IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws to include, but not limited to, the Privacy Act, Trade Secrets Act, and Bank Secrecy Act.

MANUAL

DATE March 31, 2005

1-13 WAIVERS AND EXCEPTION GUIDANCE

1. POLICY. The Bureau of Engraving and Printing's (BEP) IT security policies and procedures are designed to reduce and manage the Bureau's exposure to risk. Therefore, every effort shall be made to avoid waivers or exceptions to established BEP security policies and procedures. The Chief Information Officer (CIO) has final authority to grant waivers and exceptions to established IT security policy or procedures.

2. BACKGROUND. Waivers document exceptions to the established policies or procedures. The purpose of having a waiver and exception policy is to outline a process that ensures decision makers understand and are prepared to manage the additional risks associated with deviation from established security policies or procedures.

The IT security policies and procedures are designed to reduce the Bureau's exposure to risk. Therefore, whenever an exception or waiver is requested, it is incumbent upon the requestor prior to requesting a waiver, to assess the risk incurred as a result of non-compliance with the policy or standard.

3. PROCEDURES.

- a. The Requestor shall:
 - (1) Submit a written request with suitable justification, and a thorough assessment of real and potential risks to the CIO; and
 - (2) Ensure that written CIO approval is received prior to implementing an exception to or waiver of any BEP IT security policy or procedure.
- b. The System Owner shall:
 - (1) Submit, to the Designated Accrediting Authorities (DAA), any request with suitable justification for a waiver or exception to BEP policies or procedures; and
 - (2) Implement the waiver or exception in accordance with the authorization memo.
- c. The Designated Accrediting Authority (DAA) shall:
 - (1) Review the request for a waiver or exception to BEP policies or procedures and determine whether to forward the request to the Office of Critical Information and IT Security (OCIITS) for analysis; and
 - (2) Review OCIITS risk assessment report and recommendations, and decide to either reject the request based on the risk level, or submit the authorization request memo with the OCIITS risk assessment and recommendations to the CIO for approval.

MANUAL

DATE March 31, 2005

- d. The Office of Critical Information and IT Security (OCIITS) shall:
 - (1) Evaluate the request for waiver or exception to BEP policies or procedures, assess the risk(s) to the BEP system or other interconnected systems, and make recommendations for additional safeguards, mitigation strategies, and alternative solutions, as appropriate;
 - (2) Draft an authorization request memo from the DAA to the CIO summarizing the request, the risks, and the recommendations. Include a signature block for CIO approval/disapproval; and
 - (3) Ensure that the waiver or exception, if granted, is properly documented and maintained with the system certification and accreditation package.

- e. The Chief Information Officer (CIO) shall:
 - (1) Review each request for a waiver or exception to BEP policy and procedure and OCIITS' risk assessment and recommendations, and make a determination on whether the waiver or exception may be granted for the policy or procedure; and
 - (2) Approve waivers and exceptions by signing the authorization memo.

MANUAL

DATE July 31, 2002

2-1-1 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. "Security of Federal Automated Information Systems," Office of Management and Budget (OMB) Circular A-130, Appendix III (revised October 2000).
- b. Public Law 107-347, "E-Government Act of 2002," Title III, Federal Information Security Management Act (FISMA) of 2002, December 17, 2002.
- c. Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," National Institute for Standards and Technology (NIST), October 1995.
- d. Special Publication 800-16, "IT Security Training Requirements: A Role- and Performance-Based Model," NIST, April 1998.

MANUAL

DATE July 31, 2002

- e. "Treasury Information Technology Security Program", TD P 85-01, current version.

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;
- (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:

MANUAL

DATE July 31, 2002

- (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.

MANUAL

DATE January 22, 2007

2-2 Protecting Sensitive and Personally Identifiable Information

1. POLICY. This chapter establishes policy and responsibilities for protecting information assets that are accessed remotely or stored on mobile media, and the additional measures required to protect Personally Identifiable Information (PII) in accordance with Office of Management and Budget (OMB) and Treasury policy.

OMB Memorandum 06-19 defines personally identifiable information as:

Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Examples of Personally Identifiable Information (PII) are:

1. Social Security Numbers in any form
2. Place of birth associated with an individual
3. Date of birth associated with an individual
4. Mother's maiden name associated with an individual
5. Biometric record associated with an individual
 - a. Fingerprint
 - b. Iris scan
 - c. DNA
6. Medical history information associated with an individual
 - a. Medical conditions, including history of disease
 - b. Metric information, e.g., weight, height, blood pressure
7. Criminal history associated with an individual
8. Employment history and other employment information associated with an individual
 - a. Ratings
 - b. Disciplinary actions
 - c. Performance elements and standards (or work expectations) are PII when they are so intertwined with performance appraisals that their disclosure would reveal an individual's performance appraisal.
9. Financial information associated with an individual
 - a. Credit card numbers
 - b. Bank account numbers
10. Security clearance history or related information (Not including actual clearances held)

MANUAL

DATE January 22, 2007

a. Identifying and Protecting PII.

(1) Procedures for identifying and protecting personally identifiable information and managing associated risks shall be incorporated into the system certification and accreditation and change management process documentation. PII will be identified and documented in the System Security Plan and Privacy Impact Assessment. An inventory of systems that contain PII will be maintained.

(2) All PII shall be evaluated for impact of loss or unauthorized disclosure and protected accordingly. Risk assessments shall be conducted and controls shall be implemented to address the risk associated with the download, remote access, or other removal of PII from each system containing PII. Minimum controls shall meet requirements established by [National Institute of Standards and Technology \(NIST\) Federal Information Processing Standard \(FIPS\) 200](#), “Minimum Security Requirements for Federal Information and Information Systems”; [NIST Special Publication \(SP 800-53\)](#), “Recommended Security Controls for Federal Information Systems,” and the Checklist attachment to OMB Memorandum 06-16, “Protection of Sensitive Agency Information” ([NIST M 06-16 Checklist](#)). The Treasury PII checklist must be completed for each information technology system. The NIST M 06-16 Checklist must also be completed for systems that contain Moderate or High Impact PII that is accessed remotely or physically removed from Bureau facilities.

(3) All PII shall be assigned a High, Moderate, or Low impact category for confidentiality according to [FIPS 199](#) and the definitions established in this policy.

(4) User generation of computer-readable reports and extracts containing FIPS 199 High or Moderate confidentiality information (computer-readable extracts) shall be logged, to the extent technically feasible. Procedures shall be developed to ensure that such extracts are erased within 90 days or that verification is made of the requirement for continued use.

b. Physical Removal of PII.

(1) Physical removal of High Impact PII from BEP premises is discouraged. Except for compelling operational need, any mobile computing device or removable electronic media that processes or stores High impact electronic PII records should not be physically removed from Bureau facilities.

(2) Removal of any mobile computing device or media containing High impact PII is not permitted unless approved in writing by the System Owner or Designated Accrediting Authority (DAA). If removal is permitted, the device/media shall be signed in and out with a supervising official designated by the System Owner or DAA.

MANUAL

DATE January 22, 2007

(3) All Moderate and High Impact PII that is transported, stored, or used outside Bureau facilities shall be encrypted. Controls shall be established to restrict the pickup, receipt, and transfer of Moderate and High Impact PII to authorized personnel.

c. Remote access to PII.

(1) Remote access to High Impact PII is discouraged. Except for compelling operational need, any remote access to High Impact PII shall not be permitted.

(2) The System Owner or DAA shall approve remote access to High Impact PII in writing.

(3) Download and local storage of High Impact PII is discouraged.

d. Loss or Suspected Loss of PII.

(1) Loss or suspected loss of PII shall be reported to the Bureau Help Desk immediately. Help Desk numbers are (202) 874-3010 (DC Facility), and (817) 847-3799 (Western Currency Facility).

(2) The Bureau Help Desk shall in turn notify the Bureau Computer Security Incident Response Capability (CSIRC) immediately of the loss or suspected loss according to established procedures.

(3) The Bureau CSIRC shall report the loss or suspected loss to the Treasury CSIRC within one hour and follow procedures established by the United States Computer Emergency Readiness Team (US-CERT) and Treasury CSIRC.

e. Mandatory Controls for Remote Access and Mobile Media. These controls apply to all remote access and mobile media regardless of whether PII is present.

(1) Only Bureau-issued devices, authorized by Office of Critical Infrastructure and Information Technology Security (OCIITS), shall be used for remote access.

(2) When remote access is allowed, access must be accomplished via an OCIITS-authorized virtual private network (VPN) connection.

(3) All Bureau electronic media that is transported, stored, or used remotely will be encrypted.

(4) All laptop computers will be encrypted.

MANUAL

DATE January 22, 2007

(5) Until such time as encryption is deployed, approval of the Designated Accrediting Authority is required for removal of unencrypted devices/media from approved locations and for the selection and implementation of compensating controls.

(6) Two-factor authentication shall be implemented for all remote access to a Bureau system, with one of the factors provided by a device separate from the computer gaining access, regardless of whether PII is present.

(7) When the user has remote access to information pertaining only to them or their own account (e.g., when the employee's account contains information about family members as designated beneficiaries), then two-factor authentication is not required. Examples of this would be when employees log onto a Treasury system to check their own account or a citizen uses a Treasury website to make a purchase (e.g., numismatic products) or check their account status (e.g., savings bonds holdings). This exception also applies to the applicability of the NIST checklist.

(8) Time-out that requires re-authentication after a specified period of inactivity, not to exceed 30 minutes, shall be implemented for all remote access and mobile devices (e.g., laptops and Personal Digital Assistants (PDAs) regardless of whether PII is present (15 minutes or less is recommended). Multiple levels of time-out are not required (i.e., if a system-level time-out is implemented then another time-out within the application is not also required). Inactivity may apply to users, devices, or application. For a workstation or personal digital assistant accessed applications inactivity is the period of time without a key press or mouse movement, and for remotely accessed applications, it is the period of no application-layer traffic. Standards for allowable periods for specific devices are set by OCIITS.

(9) Appropriate procedures and training will be provided to ensure that remote use of encrypted information does not result in accidentally or purposefully bypassing the protection provided by that encryption.

(10) Users shall sign rules of acceptable use before receiving or using BEP networks, computers, media, personal digital assistants (PDAs), or other devices.

2. DEFINITIONS.

a. Electronic PII. PII that is in electronic format, for example, PII stored, transmitted or processed on computers and networks, or stored on electronic media, diskette, CD-ROM, or USB storage device.

b. High Impact PII. FIPS 199 High Confidentiality PII is PII for which the impact of unauthorized disclosure is expected to have a severe or catastrophic adverse affect on

MANUAL

DATE January 22, 2007

organizational operations, organizational assets, or individuals. Also, it may include any PII identified by the System Owner or DAA as requiring additional protection measures.

c. Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. Corporations, partnerships, sole proprietorships, professional groups, businesses (whether incorporated or unincorporated), and other commercial entities are not individuals.

d. Low Impact PII. FIPS 199 Low Confidentiality PII is limited to PII for which the impact of unauthorized disclosure could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Examples of information in this category include: names, telephone numbers, email addresses, addresses, voter registration information, audit trail data of users of government systems, and other information that is available in public records (e.g., birth and death, property, and court.)

e. Moderate Impact PII. FIPS 199 Moderate Confidentiality PII is PII for which the impact of unauthorized disclosure could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Examples of information in the category include: Social Security Number; an individual's medical or financial records, and credit card numbers.

f. Non-electronic PII. Any PII that is not in electronic format, such as printed reports or hand-written notes.

g. Personally Identifiable Information (PII). OMB M 06-19 defines personally identifiable information as:

Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

h. Physical Removal of PII. PII (except that made available intentionally to the public) that is removed from or stored outside Bureau facilities. For the purpose of this policy, Bureau facilities are defined as any location other than those of:

(1) The Bureau of Engraving and Printing, Department of the Treasury, or other Treasury bureau; or

MANUAL

DATE January 22, 2007

(2) Other U.S. Government agency where the level of physical security is acceptable to the Designated Accrediting Authority (DAA); or

(3) Non-Federal organizations (including contractors) that own or operate systems on behalf of the Bureau where the level of physical security provided is acceptable to the DAA. (These must be within the United States, except those principally supporting overseas Treasury personnel)

For example, PII stored at a private residence, hotel, or vehicle is considered physically removed.

i. Supervising Official. An individual, designated by the System Owner or DAA, responsible for maintaining a sign-in/sign-out log of the removal and return of High impact PII.

3. REFERENCES.

a. [OMB Memorandum 06-16, "Protection of Sensitive Agency Information,"](#) June 23, 2006.

b. [OMB Memorandum 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for in Agency Information Technology Investments,"](#) July 12, 2006.

c. Treasury Chief Information Officer Memorandum, "Implementation of OMB M 06-16 for Non-National Security Systems," July 20, 2006.

d. Treasury Chief Information Officer Memorandum, "Encryption of Mobile User Media," June 16, 2006.

e. [NIST FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems,"](#) February 2004.

f. [NIST FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems,"](#) March 2006.

g. [NIST Special Publication \(SP 800-53\), "Recommended Security Controls for Federal Information Systems,"](#) February 2005.

h. [BEP Manual 10-08.35, "Information Technology Security Policy and Procedures Manual, Chapter 3-14, Encryption."](#)

MANUAL

DATE January 22, 2007

i. [BEP Manual 10-08.29, "Computer Security Incident Response Capability \(CSIRC\) Procedures"](#)

4. RESPONSIBILITES.

a. Users shall:

- (1) Sign rules of acceptable use and comply with policy and procedures established to control and protect PII;
- (2) Notify the Bureau Help Desk of any known or suspected violation of this policy;
- (3) Ensure that all Moderate or High Impact PII that is transported, stored, or used outside Bureau facilities is encrypted;
- (4) Not remove any mobile computing device or media containing High Impact PII unless approved in writing by the System Owner or DAA;
- (5) When removal of High Impact PII is permitted, sign in and out with the supervising official designated by the System Owner or DAA;
- (6) Notify the Bureau Help Desk immediately of known or suspected loss or unauthorized disclosure of electronic PII; and
- (7) Notify the Bureau Privacy Officer immediately of known or suspected loss or unauthorized disclosure of non-electronic PII.

b. Designated Accrediting Authorities shall:

- (1) Evaluate and accept the risk of loss or unauthorized disclosure of PII when making accreditation decisions;
- (2) Approve remote access to High Impact PII; and
- (3) Approve removal of mobile computing device or media containing High Impact PII, and designate a supervising official.

c. System Owners shall:

- (1) Identify and document PII in the System Security Plan and Privacy Impact Assessment;
- (2) Evaluate PII for impact of loss or unauthorized disclosure and assign a High, Moderate or Low impact category for confidentiality according to FIPS 199;
- (3) Complete the Treasury PII checklist;
- (4) Evaluate impact of risks associated with the download, remote access or other removal of PII;
- (5) Ensure that adequate controls are implemented to protect PII;
- (6) Approve remote access to High Impact PII;
- (7) Approve removal of mobile computing device or media containing High

MANUAL

DATE January 22, 2007

Impact PII, and designate a supervising official;

(8) Establish controls to restrict the pickup, receipt, and transfer of Moderate and High Impact PII to authorized personnel;

(9) Ensure that users are provided adequate training on how to protect PII; and

(10) Establish and implement procedures to ensure that computer-readable reports and extracts containing High or Moderate Impact PII information are erased within 90 days or that continued use is still required.

d. Supervising Officials shall maintain records of removal and return of mobile computing devices and media containing PII.

e. Supervisors shall ensure that employees receive adequate training on how to protect PII.

f. Contracting Officers Technical Representatives (COTRs) shall ensure that contractors receive adequate training on how to protect PII.

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

(1) Establish procedures to identify, protect, and manage risk associated with PII;

(2) Conduct assessments to identify risks associated with the download, remote access, or other removal of PII;

(3) Complete the NIST M 06-16 Checklist, when applicable;

(4) Establish policy, procedures, and rules of acceptable use for the protection of electronic PII;

(5) Provide training on how to handle and protect electronic PII;

(6) Ensure that an inventory of systems that contain PII is maintained; and

(7) To the extent technically feasible, develop procedures to log the generation of computer-readable reports and extracts containing High or Moderate Impact PII information.

h. Help Desk shall:

(1) Notify the Bureau CSIRC immediately of any known or suspected loss or unauthorized disclosure of electronic PII; and

(2) Notify the Bureau Privacy Officer immediately of any known or suspected loss or unauthorized disclosure of non-electronic PII.

i. Bureau CSIRC shall notify the Treasury CSIRC within one hour of any known or suspected loss or unauthorized disclosure of electronic PII.

MANUAL

DATE January 22, 2007

j. Privacy Officer shall:

- (1) Notify the Treasury CSIRC within one hour of any known or suspected loss or unauthorized disclosure of non-electronic PII; and
- (2) Provide training on how to identify and protect PII.

MANUAL

DATE May 21, 2001

2-2-1 BUREAU OF ENGRAVING AND PRINTING ELECTRONIC MAIL POLICY

1. PURPOSE. This Policy defines responsibilities and provides guidance for the use of electronic mail (e-mail).

2. SCOPE. This Policy is applicable to all Bureau of Engraving and Printing (Bureau/BEP) employees, contractors and others who use e-mail. It applies to the use of e-mail accessed through Bureau resources or accessed while in a duty status or on Bureau premises. The objective is to ensure economical, effective, efficient and secure use of electronic mail.

3. BACKGROUND. Access to e-mail provides tremendous benefit to Bureau users by enabling instantaneous communication with other employees, Government agencies, and contractors; effective messaging abilities; and efficient use of resources in scheduling meetings. This access also poses significant security risks related to external threats such as viruses, and internal threats, such as compromise of sensitive information.

4. REFERENCES.

Department of the Treasury Information Technology Manual, December 1998.

"Treasury Information Technology (IT) Programs," Treasury Directive TD 81-01.

"Department of the Treasury Electronic Mail Use Policy," Treasury Directive 87-03.

5. DEFINITIONS.

a. Official Use refers to use of resources for activities which directly or indirectly support the Bureau's or the Department of the Treasury's mission and the accomplishment of related goals and objectives.

b. Authorized Use of e-mail includes official use and limited personal use. Limited personal use is permitted, providing that this is infrequent, incurs minimal expense to the Government, is during non-work time; does not involve sensitive Government information or put Government information or systems at risk; conforms with Bureau and Department of the Treasury policy; and does not interfere with official business. Authorized use of e-mail is similar to authorized use of Government telephones and includes activities such as communication with a spouse or children or scheduling a medical appointment.

MANUAL

DATE May 21, 2001

c. Bureau Systems refers to computers, networks, personal electronic devices, cellular telephones with e-mail capability or other devices provided by the Bureau to the user for official business, either at Bureau facilities or from a remote site.

d. Minimal additional expense refers to the use of government equipment where the employee is already provided access for official business and where the additional use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper.

e. Non-work time means when the employee is not otherwise expected to be addressing official business. This could be, for example, during lunch periods, authorized breaks, before or after duty hours.

6. POLICY FOR OFFICIAL AND AUTHORIZED USE. It is the policy of the Bureau to allow the use of electronic mail to support the BEP mission and to accomplish its goals and objectives.

a. Use of BEP e-mail is only for official use and for authorized use as defined in this policy.

b. Access to electronic mail is a privilege and users shall become familiar with Bureau policy and procedures for use. Managers, Office Chiefs, and Associate Directors shall ensure that sufficient information on Bureau policies and procedures is provided to users and that training is provided if required.

c. Use of Government equipment may be monitored and recorded. Anyone using Government equipment consents to such monitoring and shall have no expectation of privacy. If this monitoring reveals possible evidence of criminal activity or violations of policies or security procedures, evidence may be provided to appropriate Bureau management and/or law enforcement officials.

d. Only Bureau issued or specifically authorized equipment may be used for Bureau electronic communications. Personally owned computers, hand-held electronic devices or cell telephones shall not be connected to or used with Bureau communication systems or Bureau devices.

e. Employees, contractors, and other users shall exercise judgment and discretion in their use of e-mail. This includes ensuring that personal use does not interfere with official business and that communications are not disruptive to the work place, do not reflect negatively on the Bureau or the Government, do not have the appearance of inappropriate use of Government resources, and do not violate the Public Trust.

MANUAL

DATE May 21, 2001

f. All users must be aware of the threat of viruses and other malicious code. A user does not need to open an attachment to activate a virus. If there is a suspicion of a virus or other system compromise, the user should stop using the computer immediately and contact the Help Desk.

g. The same coordination and chain-of-command policy and procedures apply to approval and distribution of electronic messages and documents as to physical documents, within the Bureau and between the Bureau and other organizations.

h. Information which is considered "Sensitive But Unclassified", "For Official Use Only", or is otherwise controlled shall be communicated on Bureau e-mail only to authorized parties and in compliance with Department of the Treasury and Bureau Information Security policies and procedures. Questions on the handling of sensitive information should be referred to the Information Technology Security Division.

i. Distribution of chain letters, global (Bureau-wide) distributions of personal items or information, or non-authorized distribution of official communications by individuals is not permitted. However, in some cases, mass distribution of personal information which is of interest to the Bureau workforce may be permitted, but only with the authorization of the appropriate manager. This might include, for example, notices of meetings, parties, funerals, etc. If these distributions are made within an Office, the approval of the appropriate Office Chief (WDC) or Plant Manager (WCF) must be obtained. If they are addressed to one or more Directorates, they must be approved by an Associate Director.

j. Only Microsoft Outlook e-mail is authorized for Bureau users. This means that web browser e-mail, such as Hotmail, may not be used on BEP systems.

k. Limited personal authorized use of e-mail shall be of reasonable duration and frequency and, whenever possible, made during the user's personal time, such as lunch periods or official breaks. Authorized communications shall not:

(1) Adversely affect the performance of official duties.

(2) Place an excessive burden on BEP communications systems or have an adverse impact on the mission or operations of the Bureau.

(3) Involve the use of pornographic, sexually explicit, or obscene language or materials.

(4) Violate any Bureau, Treasury, or Government law or regulation.

MANUAL

DATE May 21, 2001

(5) Involve chain letters, unofficial advertisings or mailings, or the pursuit of private commercial business activities or profit-making activities.

(6) Be used to conduct any activity that would adversely affect the United States Government.

(7) Result in additional expense to the Government, other than normal wear and tear on equipment or the use of small amounts of electricity, ink, toner or paper.

(8) Be used concerning matters directed toward the success or failure of a political party, candidate for partisan office, or partisan political group.

(9) Be used directly or indirectly for purposes of lobbying.

(10) Be used to support outside fund raising activities or endorse a product or service.

(11) Be conducted in a manner that may be misrepresented as official business.

7. RESPONSIBILITIES.

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

(1) ensure that access to computer equipment and authorization to use electronic mail is provided to employees when necessary to accomplish the mission of their organization.

(2) ensure that training is provided users in the appropriate use and security of Bureau computer resources, and accountability and responsibility for electronic data dissemination.

(3) ensure that necessary safeguards are in place to protect the availability, integrity and confidentiality of systems for their operation units.

(4) identify and monitor appropriate management controls and technical safeguards for e-mail assignment and usage.

b. Users shall:

(1) ensure that they understand the policies and rules for use and security of electronic mail.

MANUAL

DATE May 21, 2001

(2) follow the access policies and the use policies to protect Bureau systems and documents and their rights to utilize the systems.

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

MANUAL

DATE June 6, 2001

2-2-2 BUREAU OF ENGRAVING AND PRINTING INTERNET POLICY

1. PURPOSE. This Policy defines responsibilities and provides guidance for the use of the Internet. The objective is to promote economical, effective and efficient research, communication and data gathering, and ensure security of Bureau information technology and communication systems.

2. SCOPE. This Policy is applicable to all Bureau of Engraving and Printing (Bureau/BEP) employees, contractors and others who access the Internet through Bureau devices or while in a duty status or on Bureau premises.

3. BACKGROUND. The Internet is a worldwide alliance of public networks that employ a common set of protocols for communicating information. It provides tremendous benefits to Bureau users by offering increased access to a variety of information resources for official business. This access also poses significant security risks related to a number of external threats, which may result in loss of services, corruption of data, or theft of sensitive information.

4. REFERENCES.

Department of the Treasury Information Technology Manual, December 1998.

“Treasury Information Technology (IT) Programs,” Treasury Directive TD 81-01, April 13, 2000.

Department of the Treasury Security Manual, Chapter VI, October 1992.

“Treasury Internet Use Policy,” Assistant Secretary for Management and CFO, March 11, 1998.

“Personal Use of Government Office Equipment Including Information Technology,” Treasury Directive TD 87-04, May 17, 2001.

5. DEFINITIONS.

a. Official Use refers to use of resources for activities which directly or indirectly support the Bureau’s or the Department of the Treasury’s mission and the accomplishment of related goals and objectives.

b. Authorized Use of the Internet includes official use and limited personal use. Limited personal use is permitted, providing that this is infrequent, incurs minimal expense to the Government, is during non-work time; does not involve sensitive

MANUAL

DATE June 6, 2001

Government information or put Government information or systems at risk; conforms with Bureau and Department of the Treasury policy; and does not interfere with official business.

c. Bureau Systems refers to computers, networks, personal electronic devices, cellular telephones with Internet capability or other devices provided by the Bureau to the user for official business, either at Bureau facilities or from a remote site.

d. Minimal additional expense refers to the use of government equipment where the employee is already provided access for official business and where the additional use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper.

e. Non-work time means when the employee is not otherwise expected to be addressing official business. This could be, for example, during lunch periods, authorized breaks, before or after duty hours.

6. POLICY FOR OFFICIAL AND AUTHORIZED USE. It is the policy of the Bureau to allow the use of the Internet to support the BEP mission and to accomplish its goals and objectives.

a. Internet access may be made available when:

- (1) it contributes to the accomplishment of official duties, including training which is required for job performance or compliance with law or regulation;
- (2) it is technically and financially supportable by the Office and the Bureau; and
- (3) risks to sensitive information are minimized to an acceptable level.

b. Use of the Internet is only for official use and for authorized use as defined in this policy.

c. Access to the Internet is a privilege and users shall become familiar with Bureau policy and procedures for use. Managers, Office Chiefs, and Associate Directors shall ensure that sufficient information on Bureau policies and procedures is provided to users and that training is provided if required.

d. Use of Government equipment may be monitored and recorded. Anyone using Government equipment consents to such monitoring and shall have no expectation of privacy. If this monitoring reveals possible evidence of criminal activity or violations of policies or security procedures, evidence may be provided to appropriate Bureau management and/or law enforcement officials.

e. Any direct connection to Internet services from Bureau computers, networks, or communications services must occur through gateways and firewalls that have been

MANUAL

DATE June 6, 2001

approved by the Associate Director (CIO). Only Bureau issued or specifically authorized equipment may be used for Internet communications. Personally owned computers, hand-held electronic devices or cell telephones shall not be connected to or used with Bureau communication systems or Bureau devices.

f. Employees, contractors, and other users shall exercise judgment and discretion in their use of the Internet. This includes ensuring that personal use does not interfere with official business and that communications are not disruptive to the work place, do not reflect negatively on the Bureau or the Government, do not have the appearance of inappropriate use of Government resources, and do not violate the Public Trust.

g. All users must be aware of the continual threat of compromise to Bureau systems. Unprotected connections to the Internet, unauthorized communication over the Internet, or downloads of unauthorized information may compromise BEP security. If there is a suspicion of a system compromise, the user should stop using the computer immediately and contact the Help Desk.

h. Only Microsoft Outlook e-mail is authorized for Bureau users. This means that web browser e-mail, such as Hotmail, may not be used to send or receive e-mail using BEP systems.

i. There is a great deal of information available through the Internet which can benefit the Bureau and benefit Bureau users in the performance of their duties. However, Bureau users must honor legal protections of the information, such as "intellectual property [rights], copyrights, trademarks, and software licenses."

j. Remote access to Internet services from Bureau provided computers or other devices must employ appropriate security mechanisms which are consistent with the sensitivity of the information at risk, Bureau and Department of the Treasury policy. This includes, at a minimum, only access through encrypted devices such as Virtual Private Networks (VPN) or dial-up access through the Bureau firewall. Computers using VPNs will have a personal firewall installed that is approved by the Information Technology Security Division.

k. Limited personal authorized use of the Internet shall be of reasonable duration and frequency and made during the user's personal time, such as lunch periods or official breaks. Authorized personal use of the Internet shall not:

(1) Adversely affect the performance of official duties.

(2) Place an excessive burden on BEP communications systems or have an adverse impact on the mission or operations of the Bureau.

MANUAL

DATE June 6, 2001

(3) Involve the creation, downloading, viewing, storage, copying or transmission of pornographic, sexually oriented, or obscene language or materials.

(4) Violate any Bureau, Treasury, or Government law or regulation.

(5) Involve the pursuit of private commercial business activities or profit-making activities.

(6) Be used to conduct any activity that would adversely affect the United States Government.

(7) Result in more than minimal expense to the Government.

(8) Be used to support outside fund-raising activities; endorse any product or service; participate in any lobbying activity; or engage in any prohibited partisan political activity.

(9) Be conducted in a manner that may be misrepresented as official business.

(10) Be used to access hacker sites or to gain unauthorized access to other systems.

(11) Be used to access sites that promote illegal activities including, but not limited to, illegal gambling, illegal weapons or terrorist activities.

(12) Involve the creation, downloading, viewing, storage, copying or transmission of offensive materials, such as hate speech or material that demeans others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.

(13) Involve the downloading, copying or playing of computer games.

7. RESPONSIBILITIES.

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

(1) ensure that access to computer equipment and authorization to use the Internet is provided to employees when necessary to accomplish the mission of their organization.

(2) ensure that training is provided users in the appropriate use and security of Bureau computer resources, and accountability and responsibility for electronic data downloads and dissemination.

MANUAL

DATE June 6, 2001

(3) ensure that necessary safeguards are in place to protect the availability, integrity and confidentiality of systems for their operation units.

(4) identify and monitor appropriate management controls and technical safeguards for Internet access assignment and usage.

b. Users shall:

(1) ensure that they understand the policies and rules for use and security of the Internet.

(2) follow the access policies and the use policies to protect Bureau systems and documents and their rights to utilize the systems.

(3) read the "Internet Access Agreement" (Attachment 1) and complete the "Internet Access Form" (BEP form 8397) when applying for internet access and agree to comply with the provisions of Bureau policy.

8. SANCTIONS FOR MISUSE. Unauthorized, improper, or insecure use of BEP Internet 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.

MANUAL

DATE June 6, 2001

ATTACHMENT 1

INTERNET ACCESS AGREEMENT

Individuals granted Internet access shall be accountable for following BEP's policies and procedures on Internet use, as well as any and all laws, regulations and rules applicable to Government-owned automated data processing equipment.

The Bureau will be placing a great deal of trust in any employee granted access to the Internet. Therefore, any employee granted this access will be subject to adverse administrative and/or disciplinary action should they violate any part of this policy.

In order to obtain Internet access, the Internet Access Form (BEP form 8387) must be submitted by you through your Office Chief, Plant Manager (Washington or WCF) or Associate Director to the Chief Information Officer, Room 725-A. Both you and the individual it was submitted through should sign this form. In the "Justification" area provided on the form clearly state the reason(s) for Internet access and how this is in support of a BEP mission or need.

In addition to the above rules and regulations an individual obtaining Internet access must also agree to:

- Not divulge to nor let any other individual, under any circumstances, use your Internet user logon and password. If you believe that your user logon has been compromised, IMMEDIATELY contact the Help Desk, Office of IT Operations at (202) 874-3010. Failure to make this notification will constitute a violation of BEP's Internet Access Policy.
- Not download any file from the Internet unless it passes through BEP's standard anti-virus program. If, after downloading a file, you believe it to be corrupted with a virus, IMMEDIATELY stop using the computer and contact the Help Desk, Office of IT Operations, (202) 874-3231, who will then contact the IT Security Division. Failure to make this notification constitutes a violation of BEP's Internet Access Policy, and may result in your computer being infected with a virus along with all other computers on the network.
- Never leave your PC unattended while logged on to the Internet.
- Not divulge to nor let any other individual, under any circumstances, use your IP Address.

Physical connectivity to the Internet will be accomplished following Treasury's connection policy. This will be accomplished by BEP, using a standard desktop configuration employing Microsoft Internet Explorer and firewall (security wall), which in turn connects to the TCS carrier and from there out to the Internet. This connection strategy employs good security for BEP utilizing both a firewall and a security access program.

MANUAL

DATE March 2, 1998

2-3-1 Access to the BEP Computer Facility

1. PURPOSE. Access to the BEP Computer Facility

2. POLICY. The Bureau Computer Facility is designated as a restricted area. Access to this area without an escort is limited to specific personnel. A detailed listing of personnel having access to the facility is maintained by the Manager, Technical Support Service Division (TSSD) and the Contractor Officer Technical Representative (COTR). In general, access is limited in accordance with the following criteria.

- 1) OIS staff whose work requires them to enter the area;
- 2) IBM engineers and maintenance staff (electric shop, etc) who have a work purpose for entering the area:

All other individuals must first be cleared by the Chief, OIS; the Manager, TSSD, or the COTR, who will then notify the Computer Operations Staff of the individual's name, date and time of visit. These individuals must be escorted for the entire period they are in the facility.

The Operations Staff will notify the COTR immediately if any unauthorized personnel enter the area.

3. SCOPE. This circular applies to all components within the Bureau of Engraving and Printing.

MANUAL

DATE May 4, 2007

2-4 INFORMATION TECHNOLOGY STORAGE MEDIA CONTROLS

1. PURPOSE AND SCOPE. This section establishes policy and defines responsibilities for protecting information technology storage media, both paper and digital, containing sensitive but unclassified information. This policy 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 but unclassified information in compliance with the [Treasury Information Security Program Policy, TD P 85-01](#), and other Department of the Treasury and Federal policies and regulations.

3. REFERENCES.

- a) ["Treasury Information Technology Security Program," Treasury Directive Publication \(TD P\) 85-01, Volume I, "Unclassified \(Non-National Security\) Systems,"](#) current version.
- b) ["Department of the Treasury Security Manual," Treasury Directive Publication \(TD P\) 15-71,](#) current version.
- c) [Treasury Chief Information Officer Memorandum, "Implementation of OMB M 06-16 for Non-National Security Systems,"](#) current version.
- d) [Treasury Chief Information Officer Memorandum, "Encryption of Mobile User Media,"](#) current version.
- e) [BEP Manual No. 71-00.42,](#) "Information Security Manual," current version.
- f) [Privacy Act of 1974,](#) 5 United States Code (USC) Section 552a, current version.
- g) [Federal Information Processing Standard Publication 199 \(FIPS Pub 199\) "Standards for Security Categorization of Federal Information and Information Systems,"](#) current version.
- h) [NIST Special Publication \(SP 800-53\), "Recommended Security Controls for Federal Information Systems,"](#) current version.
- i) [NIST Special Publication \(SP 800-88\), "Guidelines for Media Sanitization,"](#) current version.

MANUAL

DATE May 4, 2007

4. SUPERSESION. This chapter supersedes Chapter 2-4, "Information Technology Storage Media Controls," dated March 25, 2004.

5. DEFINITIONS.

- a) **Availability.** Timely, reliable access to data and information services for authorized users. This includes the restoration of services after an interruption.
- b) **Bureau System.** An IT system (including telecommunications, networks, computers, and software programs) that is owned, leased, or operated by the Bureau or is operated by a contractor or another government agency on behalf of the Bureau.
- c) **Confidentiality.** The assurance that information is not disclosed to unauthorized persons, processes, or devices.
- d) **Information Sensitivity.** [FIPS Pub 199](#) defines three levels of potential impact on organizations or individuals should there be a loss of confidentiality, integrity, or availability. Levels of potential impact are low, moderate, or high. Most information is in the low potential impact category. Minimum security measures are designed to protect information at that level. Additional controls may be required for information that requires a higher level of assurance for confidentiality, integrity, or availability.
- e) **Integrity.** Consists of 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. Generally, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
- f) **Media Storage Facilities and Libraries.** Environmentally and physically protected on-site or off-site facilities used to store system backup media and master copies of software.
- g) **Mobile Media.** Mobile media is easily transportable electronic media (e.g., laptop computers, personal digital assistants, diskettes, CDs, DVDs, flash memory devices, and tapes).
- h) **Paper media.** Paper media covered by this policy is limited to information technology paper media that is input to or output from information technology systems.

MANUAL

DATE May 4, 2007

- i) **Records Schedule.** A document that describes agency records, establishes a period for their retention by the agency, and provides mandatory instructions for what to do with them when they are no longer needed for current government business.
- j) **Sanitization.** Elimination of data from storage media so that data cannot be recovered by ordinary means. Examples of sanitization methods are crosscut or strip shredders, degaussing, approved disk-wiping software, and media destruction.
- k) **Sensitive but unclassified 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 USC 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.
- l) **Secure Location.** A physical and/or logical location that provides adequate controls to protect the confidentiality, integrity, and availability of the information. The level of protection required is based upon the sensitivity of the information. Adequate controls result in an acceptable level of risk.
- m) **Storage Media (Media).** Objects used to magnetically, optically, or by other means store data. This includes internal, external, and removable storage devices (e.g., hard drives, tapes, diskettes, compact disks, and removable disk drives), master copies of software, and backup files, data, and programs.
- n) **Unauthorized Disclosure.** Exposure of information to persons, processes, or devices not authorized to receive it.

6. PROCEDURES.

- a) Media Protection.
 - 1) All media and paper-based system input and output containing sensitive but unclassified information shall be stored in a secure location when not in use to prevent unauthorized disclosure, modification, loss, or destruction. Examples of secure locations include a locked desk, bookcase, or room.

MANUAL

DATE May 4, 2007

- 2) Security controls to protect information systems input and output shall be implemented based on [NIST SP 800-53](#) minimum security controls or a system-specific risk assessment to ensure that sensitive but unclassified information cannot be accessed by unauthorized individuals.
- 3) Ensure that only authorized users access, transport, or store media and paper documents that are used as a source of input to or output from information systems. Minimum standards for protection include:
 - (a) Never leaving sensitive but unclassified information unattended at a printer when the printer located in an area that would allow unauthorized disclosure of the information. Printed material (whether sensitive or not) should be picked up from a local or network printer right away.
 - (b) Using locked bins, sealed envelopes, or “in-person” delivery for distribution of paper input and output, “in-person” delivery or use of sealed envelopes to transport media, and use of sealed envelopes when mailing media, or printed input or output.
- 4) Observe special precautions when sensitive but unclassified information is to be faxed by first calling the fax destination to ensure that an authorized person will be available to pick up the fax right away.
- 5) Backup media shall be stored at an off-site location having appropriate security controls in accordance with system security and contingency plans.
- 6) Mobile media shall be encrypted in accordance with BEP encryption policy.
- 7) Logs shall be maintained to track and establish a chain of custody for media deposited into and withdrawn from media storage facilities and libraries.
- 8) Upon the termination or reassignment of an employee, information stored on any media used by this employee shall be transferred to his/her supervisor.
- 9) Upon the termination or reassignment of a contractor, all BEP information shall be transferred to the supervisor and, upon contract termination, all BEP information shall be transferred to the Contract Officer Technical Representative (COTR).

MANUAL

DATE May 4, 2007

b) Media Marking.

- 1) Sensitive but Unclassified information must be marked in compliance with TD P 15-71, "Security Manual", Chapter III, Section 23, "Sensitive But Unclassified Information."
- 2) All removable media containing Sensitive but Unclassified information must have warning labels affixed, the same as those required for diskettes.

c) Media Reuse Within BEP.

- 1) Media that is returned to the surplus pool of equipment, re-deployed, or transferred to another individual within the BEP shall be sanitized using an Office of Critical Infrastructure and Information Technology Security (OCITS) - approved method that prevents the recovery of the information without specialized tools or techniques.
- 2) A written record shall be maintained certifying that sanitization was performed and identifying the media that was sanitized, how it was sanitized, and the final disposition of the media.

d) Paper, Diskette, Compact Disk (CD), and Magnetic Tape Media Not Intended for Reuse within BEP.

- 1) Media shall be destroyed using the physical destruction methods identified in [NIST SP 800-88 "Guidelines for Media Sanitization."](#)
- 2) The following procedures are approved for sanitization prior to disposal in a regular trash container:
 - (a) Diskettes must be shredded or cut into strips, and compact disks must be rendered unreadable by deep scratching on the data side (the shiny side without the label) with a nail, screwdriver, or similar tool. Two deep radial scratches extending from the small inner hole to the outer edge are sufficient.
 - (b) Printed output must be disposed of in a manner that does not allow unauthorized disclosure. Public information and information for which access is not restricted in any way may be recycled or discarded in a regular trash container; all other printed information must be shredded using a crosscut or strip shedder.

MANUAL

DATE May 4, 2007

(c) Magnetic tapes must be shredded or incinerated.

e) Other Storage Media Not Intended for Reuse Within BEP.

- 1) Storage media shall be destroyed using the physical destruction methods identified in [NIST SP 800-88 "Guidelines for Media Sanitization."](#)
- 2) Storage media shall be removed from equipment when feasible and destroyed (e.g., hard drives in laptop, desktop, mainframe computers, and copiers). When not feasible, the entire piece of equipment shall be destroyed (e.g., PDAs).
- 3) Storage media in leased equipment (i.e., copiers) shall not be permitted to be returned to the leaseholder once the equipment has been in use at BEP. If needed, arrangements should be made to purchase the storage component from the leaseholder.
- 4) Sanitize memory components using purge methods identified in [NIST SP 800-88 "Guidelines for Media Sanitization."](#)
- 5) A written record shall be maintained certifying that sanitization was performed, identifying the media that was sanitized, describing how it was sanitized, and listing the final disposition of the media.

f) Unusable Media/Media Repair.

- 1) Storage media, including media in leased equipment, shall not be returned to a manufacturer, leaseholder, or sent outside the BEP for repair or replacement. Unusable storage media shall be treated as media not intended for reuse within BEP.

g) Verification.

- 1) A representative sampling of media shall be tested to ensure that media is properly sanitized.
- 2) Verification shall be conducted by personnel who are not involved in any part of the process. For example, verification would be conducted by someone who is independent of personnel who return media for sanitization, are assigned media for reuse, or who sanitize media.

MANUAL

DATE May 4, 2007

h) Official Records.

- 1) Disposition of official records on storage media shall be handled according to the appropriate Bureau or other Records Schedule.

7. RESPONSIBILITIES.

a) Associate Directors, Designated Accrediting Authorities, and Office Chiefs shall:

- 1) Determine the level of sensitivity of information, ensure that systems meet Federal, Treasury, and Bureau IT security requirements, and ensure 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) Require that all contracts with external companies for repair or recovery of data from systems, hard drives, or media include a nondisclosure statement.

b) Supervisors and COTRs shall:

- 1) Ensure that their employees and contractors are aware of and comply with policy and procedures for protecting sensitive but unclassified information on printed system output and electronic media.
- 2) Ensure that information that has been created and/or maintained by an employee or contractor is transferred to an authorized individual upon the termination or reassignment of the employee or contractor. Submit a Special Access Request ([BEP Form 8393](#)) to the IT Security Division to request the transfer of information that is protected by access controls.
- 3) Ensure that media is sanitized in compliance with approved procedures before the transfer, reuse, surplus, or donation of any equipment or media.

c) System Administrators shall:

- 1) Ensure that system backup media and master copies of software are stored in a secure media storage facility.
- 2) Maintain records to track the deposits and withdrawals from media storage facilities and libraries, and the receipt of media that are transferred to another location by courier or mail. Maintain the official chain of custody for the media

MANUAL

DATE May 4, 2007

- and hold users accountable for media removed from storage. Secure records to prevent unauthorized access and manipulation of log information.
- 3) Comply with procedures for sanitizing all electronic media, hard disks, memory, or other storage devices containing sensitive data or software before the transfer, reuse, dispatch to an external organization for maintenance or replacement, surplus, donation, or disposal of any equipment or media.
 - 4) Comply with procedures to certify that sanitization was performed and maintain and provide records certifying that sanitization was done.
- d) Office of Facilities Support shall:
- 1) Comply with procedures for ensuring that any device containing a hard drive or memory has been sanitized in compliance with this policy before being donated or placed on surplus.
- e) The Office of Information Technology Operations shall:
- 1) Ensure that system backup media and master copies of software are stored in a secure media storage facility.
 - 2) Comply with procedures for sanitizing all electronic media, hard disks, memory, or other storage devices containing sensitive data or software before the transfer or reuse.
 - 3) Sanitize hard media that is intended for reuse within BEP.
 - 4) Sanitize memory components not intended for use within BEP.
 - 5) Remove storage media from equipment when feasible and ensure it's delivery to the Office of Security for destruction.
 - 6) Comply with procedures to certify that sanitization was performed, and maintain and provide records certifying that sanitization was done.
- f) The Office of Critical Infrastructure and Information Technology Security shall:
- 1) Establish policy, procedures, and standards for media controls, media protection, media marking, production input/output controls, sanitization, and disposal to ensure protection of the Bureau's information throughout the system's lifecycle.

MANUAL

DATE May 4, 2007

- 2) Provide oversight to ensure compliance with policy, procedures, and standards for media controls, and verify compliance by testing a sampling of media to ensure that media is properly sanitized.
 - 3) Evaluate sensitive but unclassified information and recommend appropriate media controls.
 - 4) Establish procedures to ensure information stored on any media is transferred to an authorized individual upon the termination or reassignment of an employee or contractor.
- g) The Office of Security shall:
- 1) Destroy media storage devices such as hard drives and PDAs.
 - 2) Comply with procedures to certify that destruction was performed, and maintain and provide records certifying that destruction was done.

8. SANCTIONS FOR MISUSE. Failure to protect the confidentiality, integrity, and availability of sensitive but unclassified information may result in suspension of privileges, disciplinary action (up to and including removal), 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.

MANUAL

DATE January 7, 2007

2-5-3 WIRELESS COMMUNICATIONS SECURITY

1. PURPOSE AND SCOPE. This section establishes policy and defines responsibilities for protecting information technology devices that implement wireless data (wireless LAN) communications capability. This policy 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 in compliance with the [Treasury Information Security Program Policy, TD P 85-01](#), and other Department of the Treasury and Federal policies and regulations.

a. All implementations of wireless data communications shall require written approval in advance from the Chief Information Officer.

b. Where approved, wireless data communications shall implement authentication and [FIPS 140-1](#) or [140-2](#) encryption on the transmission path.

c. To the maximum extent possible, hardware shall be bought without wireless LAN capabilities.

d. Where pre-existing hardware is in place, or where it is impractical to procure hardware without wireless LAN connectivity, the wireless port(s) shall be controllable by the system administrator and will not allow users to turn them on.

e. Wireless access points shall not be installed or activated in BEP without the approval of the CIO.

f. Any authorized BEP computer that is used outside of BEP (i.e., telework) shall not connect to any wireless LAN network unless specifically authorized in writing by the Chief, Office of Critical Infrastructure and Infrastructure (OCITS).

g. System and network scans and sweeps shall be conducted to detect unauthorized wireless access points and other wireless activity inconsistent with BEP and Department of the Treasury policy.

h. Approved wireless data communications shall comply with BEP and Department of the Treasury policy and [NIST SP 800-53](#).

4. REFERENCES. The following section contains the references justifying and explaining this policy.

MANUAL

DATE January 7, 2007

- a. [“Treasury Information Technology Security Program,” Treasury Directive Publication \(TD P\) 85-01, Volume I, “Unclassified \(Non-National Security\) Systems,”](#) current version.
- b. [Federal Information Processing Standard Publication 199 \(FIPS Pub 199\), “Standards for Security Categorization of Federal Information and Information Systems,”](#) current version.
- c. [NIST Special Publication \(SP 800-53\), “Recommended Security Controls for Federal Information Systems,”](#) current version.
- d. [NIST Special Publication \(SP 800-48\), “Wireless Network Security,”](#) current version.
- e. [BEP Manual 10-08.35, Chapter 3-3, “Remote Access to Computer Systems,”](#) current version.

5. DEFINITIONS. The following includes explanations for terms that may be unique to this document.

Wireless Data Communications – Data communications other than those transmitted via wire (e.g., cable, telephone wire) regardless of the technology used for transmission (e.g., infrared (IR), radio frequency (RF)).

5. RESPONSIBILITIES. The following list identifies those in charge of enforcing the policy and what their duties are.

a. The Chief Information Officer shall review risk assessments, security controls, and approve or disapprove the implementation of wireless data communications.

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

- (1) Evaluate risk and develop security controls for implementing wireless data communications.
- (2) Establish policy, procedures, configuration standards, and monitor the use of wireless data communications.
- (3) Approve requests to use approved implementations of wireless data communications.
- (4) Conduct scans to detect unauthorized wireless activity.
- (5) Provide oversight to ensure compliance with policy, procedures, and standards for wireless data communications.

MANUAL

DATE January 7, 2007

c. Users shall not use any wireless data communications unless specifically authorized in writing by OCIITS.

MANUAL

DATE July 6, 2001

2-6-4 SECURITY REQUIREMENTS FOR PERSONAL DIGITAL ASSISTANTS

1. PURPOSE. This policy establishes security requirements related to the introduction and use of personal digital assistants (PDAs) within the Bureau. It provides guidance on the risks involved in using PDAs; the types of information that may be processed and/or stored on them; the approval procedures for procuring them; and the specific, limited user support from the Bureau.

2. SCOPE. This section applies to all PDAs (government and personally owned) and the types of data that may be accessed or stored using these devices. This policy is an extension of several policies in Treasury Department Policy (TDP) 71-10, Chapter 6, Section 4.B., titled "Program for the Protection of Sensitive But Unclassified Information Processed in Automated Information Systems and Networks." Several specific restrictions, as they impact Bureau operations and information systems, are addressed. This policy shall apply to all Bureau employees, Bureau contractors, and other persons visiting or representing other Government agencies while on the Bureau premises. Additionally, it applies to all parties when they are connected to Bureau automated information systems and networks, on the premises or via remote access.

For the purposes of this policy, **ALL** information processed on Bureau automated information systems, networks and the peripheral devices connected to them, shall be categorized as Sensitive But Unclassified.

3. DEFINITIONS.

Portable Electronic Device: The generic title identifying a class of small electronic devices. Typically, the capabilities of these devices go beyond their originally designed purpose. An example is the cell phone. In addition to basic telephone services, it may have one or more of the following capabilities:

- Function as a PDA;
- Connect to the Internet to retrieve electronic mail;
- Used to access the Internet; and
- Function as a pager.

Personal Digital Assistant (PDA): An electronic device designed to function as an address and/or telephone book, calendar, and calculator. The capabilities of these devices have been expanded to include paging, Internet access, audio recording, and file exchanges with a variety of computer systems.

Peripheral device: (Re: automated information systems and networks) An electronic device used to receive, process and/or transmit data. Examples include printers, facsimile machines, optical scanners, PDAs, and video conferencing equipment.

MANUAL

DATE July 6, 2001

Unclassified information: Information that if lost, misused; or accessed, disclosed, or modified without authority would not adversely affect the national interest, or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, US Code (The Privacy Act).

Sensitive information: Information that if lost, misused; or accessed, disclosed, or modified without authority could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be classified in the interest of national defense or foreign policy. Information classifications found in this class are Sensitive But Unclassified (SBU), For Official Use Only, Limited Official Use, and Treasury Sensitive Information.

Classified National Security Information: Information that has been determined, pursuant to Executive Order 12958 or any successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Information classifications found in this category are Top Secret, Secret, Confidential, and Special Compartmented Information and/or Facilities (SCI/SCIF).

Virtual Private Network (VPN): A secure electronic means of connecting to one's business or office network.

4. BACKGROUND. PDAs are small, portable personal electronic devices that are vulnerable to theft and the loss or disclosure of all data contained on them. The technology of the PDA provides useful functionality including:

- Easy storage and retrieval of personal data;
- Personal calendaring;
- Telephone number retrieval;
- Audio recording;
- Offline and remote e-mail capability;
- Connectivity via analog or wireless modems;
- Paging; and
- Internet browsing.

The current technology also permits the user to upload, download and synchronize information with the office workstation. This procedure can be accomplished using a cable connecting the PDA to the workstation. Many PDAs also contain sound recording devices. All of these technological advances also represent vulnerabilities that require careful consideration and elements of control.

MANUAL

DATE July 6, 2001

5. POLICY. As it pertains to the usage of PDAs, the aforementioned classes of information will be handled as follows:

a. Unclassified information.

For the purposes of this policy, all unclassified BEP data will be elevated to SBU and treated accordingly. Unclassified Bureau business data may only be stored on government furnished PDAs.

b. Sensitive Information.

(1) Government Owned PDAs;

- a) Government owned PDAs may be used for SBU information. Government owned PDAs may be connected to a Bureau computer or network that processes SBU information to perform file sharing and for other purposes such as updating of calendars. **Government PDAs will not be connected to any non-Bureau computer or network except as specified by this policy.**
- b) Bureau employees who are authorized to use a PDA must first attend an orientation briefing on the proper use of and the associated risks of the PDA. They will execute a statement of understanding **prior to** PDA issuance and use of a government owned PDA. An original signed statement of understanding will be executed with the CIO Directorate and a file copy will be provided to and maintained by the user's respective office.
- c) The PDA standards are established and maintained by the CIO Directorate. Only PDAs that conform to these standards may be procured.
- d) There will be two levels of PDA use within the Bureau. There will be no "in between" categories and no exceptions or variances granted. They are:
 - Level 1: Requires synchronizing via cable with user's office PC.
 - Level 2: Additionally provides remote access to BEP system resources via the Bureau Virtual Private Network (VPN). The Bureau VPN will be the only authorized means of remote access to the Bureau network. Training will be provided on the use of the VPN.

MANUAL

DATE July 6, 2001

- e) User identification and level of use selection.
- Each Office Chief will determine individuals who require a PDA.
 - Level 1 users will be authorized by the Office Chief.
 - Level 2 users must be authorized by the respective Associate Director.
- f) The PDA procurement process is as follows:
- The PDA standards are established by the CIO Directorate.
 - Each Office will procure the requisite PDAs against this standard.
 - Each Office will also be responsible for purchasing the Internet service provider (ISP) access services required for Level 2 PDAs to function.
 - Each Office is responsible for maintaining an accurate inventory of all PDAs procured, on hand, and to whom they are assigned.
 - Each Office will maintain a copy of each user's signed statement of understanding.
 - PDAs and monthly ISP contracts may be procured using credit cards assigned to Offices that are generally used to secure administrative support items.
- (Note:** The PDA standards will be available on the CIO page on the Bureau intranet site, In\$ite.)
- g) PDAs will be subject to random review by IT Security Division (ITSD), Office of IT Operations, Chief Information Officer Directorate (CIO) to determine adherence to policies. If the information is considered by the Bureau CIO to be highly sensitive, the information must be removed.
- (Note:** Contact ITSD for the current list of approved encryption software authorized for handling SBU information.)
- h) PDAs will be issued to and signed for by individual name only. No PDAs will be issued to a pool, organizational component name or activity.
- i) The PDA will be returned to the issuing Office when:
- The user no longer requires the PDA.
 - The user is transferring to another Bureau Office.
 - He/She is terminating Bureau employment.

MANUAL

DATE July 6, 2001

- j) All files on Government owned PDAs are to be erased before the PDA is reissued to another individual. Bureau Office Chiefs will make appropriate arrangements with the CIO Directorate for the accomplishment of this procedure.
- (2) Personally Owned PDAs.
- a) **Personally owned PDAs shall not be connected to any Bureau computer or network for any purpose.**
- b) Personally owned PDAs **shall be restricted from any Bureau area** where particularly sensitive data is stored or discussed.
- c. National Security Information.
- Treasury policy prohibits the processing or storage of National Security Information on personally owned PDAs. Under no circumstances will Classified or National Security Information be placed, processed, stored, or handled by means of a Bureau PDA.
- d. Approved Models of PDAs for Government Purchase and Use.
- Visit the CIO Intranet web site or contact the ITSD, for the current PDAs approved for Bureau use. Due to the rapid changes in technology, this list will be dynamic.
- e. Proper Procedures on the Use of Government Owned PDAs with Government Information Systems.
- (1) When powering on the PDA, all users are required to utilize the identification and password feature on their respective PDA. This feature must always be in the active mode and never disabled. Users, once logged on, shall not leave the PDA unattended when logged on.
- (2) The only approved methods for accomplishing file sharing and updating calendars between workstations and PDAs are:
- Via connecting cable between the PDA to the user's workstation; and/or
 - Use of a cradle, holder or other device connected to the user's workstation enabling the PDA to be synchronized.
- (3) Users are not authorized to add, modify, or delete software applications contained on the PDA once issued. If the user requires changes to software

MANUAL

DATE July 6, 2001

configurations, a written request with justification will be required from the Office Chief to the CIO Directorate.

- (4) Only Bureau approved ISPs will be used when connecting PDAs to the Internet. Visit the CIO Intranet web site or contact the ITSD for the current list of approved ISPs.
- (5) Bureau email shall be transmitted remotely only via VPN. Otherwise, all email transfers must be accomplished via the two previously described methods (in paragraph (2), above).
- (6) Government-owned PDAs are to be used for official purposes, and as authorized by ethics regulations, may be used for personal convenience.

6. WAIVERS. All sections of this policy are mandatory. No waivers will be granted.

7. RESPONSIBILITIES.

a. The Bureau users:

- (1) Will undergo a brief orientation acquainting them with the proper use of the PDA and the proper handling and storage of data, read the Bureau policy on PDAs, and execute a statement of understanding with the CIO Directorate prior to issuance and use of a government owned PDA.
- (2) Will not effect any connections of a government owned PDA to any non-government computer or network; nor connect to any classified government computer or network.
- (3) Will use proper logon and password procedures to activate each session of the PDA; and will not leave it unattended while logged on or while the PDA is active.
- (4) Will report immediately to his/her respective Office Chief any missing, misplaced, or lost equipment associated with the PDA (i.e., modem, cradle, synchronization cable) and/or missing, misplaced, or lost components (i.e., PDA, memory cards, lost or corrupted data, unintentional or unauthorized disclosure of SBU information).
- (5) Perform all file transfers and synchronizations via the Bureau approved methods.

MANUAL

DATE July 6, 2001

- (6) Upon transfer or termination of employment, return the PDA to the issuing Office.

b. Office Chiefs.

- (1) If the user is leaving the Office that issued the PDA, secure its return.
- (2) Coordinate with the ITSD for the erasure of all data and reconfiguration of applications **before** PDA is issued to next prospective user. Prior to PDA re-issuance, ensure the prospective user has attended the security briefing on the appropriate use and risks associated with PDA use.

(Note: Simply 'deleting' the data is not adequate for this procedure.)

- (3) Determine those persons within your respective Office requiring a PDA. The respective Office Chief may approve the issuance of PDAs to those persons not requiring access to Bureau networks via remote means. Names of those persons requiring Internet access/VPN remote access function to Bureau networks shall be forwarded to the respective Associate Director for approval/disapproval. PDAs will be issued to a named individual (the actual user) only.
- (4) Perform an annual internal review of all PDAs issued by the Office. The review, which includes an inventory of PDAs and peripheral equipment, will assess and certify compliance with PDA policy. Furnish copies of these audits to the CIO Directorate. These documents will be used to maintain accountability of the PDAs.
- (5) Ensure that the theft or loss of any PDA containing sensitive information is reported to the Bureau CIO immediately.

c. Associate Directors/Deputy Director/Director.

- (1) Review requests for issuance of PDAs with remote access to Bureau networks capability. Approve/disapprove.
- (2) Prior to PDA issuance, ensure the prospective user has attended the security briefing on the appropriate use and risks associated with PDA use.
- (3) Recover PDA from user if he/she is leaving the Directorate that issued the PDA.

MANUAL

DATE July 6, 2001

- (4) Coordinate with the ITSD for the erasure of all data and reconfiguration of applications before issuance to next prospective user.

(Note: Simply 'deleting' the data is not adequate for this procedure.)

- (5) Determine those persons within your respective Directorate that require or need a PDA. Where access to Bureau networks via remote means is not required by the user, the respective Office Chief may approve the request. The respective Associate Director, Deputy Director or Director will review and approve/disapprove the names of persons requiring remote access to Bureau networks. PDAs will be issued only to a named individual (the actual user).
- (6) Ensure that the theft or loss of any PDA containing sensitive information is reported to the Bureau CIO.

d. Bureau Chief Information Officer (CIO).

- (1) Develop and publish protective measures as Bureau policies for the safeguarding and dissemination of SBU information processed or stored on PDAs.
- (2) Review cases where highly sensitive SBU information may exist. Make a determination and prescribe the appropriate encryption standards for the specific Bureau PDAs handling/storing the highly sensitive information.
- (3) Add the operation and security of PDAs to current security awareness programs.
- (4) Accredite PDAs in accordance with TDP 71-10 Chapter VI, Section 7.
- (5) Compile source documentation of annual internal reviews for all government owned PDAs. The annual review results shall be maintained for three years.

In the event of missing, loss, or theft of any government owned PDA, it will be immediately reported to the Departmental Office of Information Systems Security.

MANUAL

DATE September 21, 2006

2-6-7 USB STORAGE DEVICES

- 1. POLICY.** This policy establishes the rules of acceptable use and the process for requesting authorized Universal Serial Bus (USB) storage devices.
- a. Only authorized USB storage devices are approved for use with Bureau IT equipment and storage of Bureau information.
 - b. USB storage devices are for official and authorized use and are subject to monitoring.
 - c. All data contained on USB storage devices are considered property of the Bureau, thus there can be no expectation of personal privacy.
 - d. BEP reserves the right to terminate authorization to use a USB storage device at any time.
 - e. Unauthorized use of the USB storage device is prohibited and could be subject to criminal and/or administrative disciplinary action as well as civil penalties.
 - f. Authorized USB storage devices shall:
 - (1) Be requested and approved using BEP Form 2475, "Request for USB Storage Device," available on WebForms;
 - (2) Be assigned to named individuals and inventoried annually. The inventory shall include the following:
 - (a) Device make, model, and serial number;
 - (b) An approved "Request for USB Storage Device" form;
 - (c) Signed Rules of Acceptable Use.
 - (3) Not be used for storage or transport of classified information;
 - (4) Not be connected to non-BEP information systems unless authorized in writing by the Chief Information Officer (CIO);
 - (5) Be treated as removable media and shall be stored in a secure location, such as locked desk or locked room, when not in use and not left unattended; and
 - (6) Use National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)-compliant encryption to restrict access to sensitive stored data.

2. DEFINITIONS.

Universal Serial Bus (USB): A widely used hardware interface for attaching peripheral devices.

USB Storage Device: A hardware device used to record and store data or software that connects to a computer via the USB port. Examples include thumb- and flash-drives (memory sticks). These devices pose special risks to BEP systems and information because of their small size, large storage capacity, and ease of use. Devices can be configured to run software programs, including malware such as viruses, Trojans,

MANUAL

DATE September 21, 2006

keystroke loggers, and data collectors, immediately and automatically upon connection to a computer.

Authorized USB Storage Device: A USB storage device approved and issued in accordance with this policy.

3. REFERENCES.

1. Circular 10-08.37, "Limited Personal Use for BEP Office Equipment and IT Resources," July 2005.
2. Circular 10-08.33, "Control and Accountability of Sensitive Digital Images," July 2004.
3. Office of Management and Budget (OMB) Memorandum 06-16, "Protection of Sensitive Agency Information," June 23, 2006.

4. RESPONSIBILITIES.

a. Users shall:

1. Fill out and submit a "Request for USB Storage Device" form to request a USB device and agree to abide by the rules of acceptable use;
2. Use the USB storage device in compliance with Bureau policy;
3. Protect the USB storage device from theft, loss, and physical damage;
4. Immediately report lost, stolen, or damaged USB storage devices to the BEP Help Desk;
5. Protect the information on the device against loss by backing up the data to an approved BEP system;
6. Obtain written approval from the CIO before taking the USB storage device outside the United States;
7. Contact the Help Desk to request assistance with resetting the USB storage device password after three (3) failed access attempts. (BEP devices are configured to prevent brute force password attacks. Such attacks will destroy any information on the device so that it cannot be recovered);
8. Return the USB storage device to the Office Chief that approved issuance upon termination of employment at BEP, transfer to another office within BEP, or when the device is no longer required or authorized for use; and
9. Not use any unauthorized USB device on Bureau IT equipment or to store Bureau information.

b. Office of IT Operations (OITO) shall:

1. Purchase and issue authorized USB storage devices;
2. Maintain the inventory of BEP-issued storage devices and verify inventory annually;
3. In coordination with Office Chiefs, determine if data and software on USB storage devices is to be deleted or archived, when the USB storage device is

MANUAL

DATE September 21, 2006

- returned to OITO;
4. Sanitize or "clean" each USB storage device before re-issuance to another user;
 5. Ensure that the Basic Input Output Settings (BIOS) for BEP computers are configured to prevent systems from booting from a USB storage device.
- c. Office of Security (OS) shall:
1. Issue authorized USB storage devices for Continuity of Operations Planning (COOP) use;
 2. Provide OITO with inventory information on issued USB storage devices; and
 3. Return used USB storage devices to OITO for sanitization prior to re-issuing the device to another user.
- d. Office Chiefs/Western Currency Facility Division Managers shall:
1. Approve/disapprove user requests for a USB storage device;
 2. Ensure USB storage devices are returned to OITO upon the user's termination of employment at BEP, transfer to another office within BEP, or when the device is no longer required or authorized for use; and
 3. Determine and notify OITO whether the data on the USB storage device is to be either deleted or archived.
- e. Office of Critical Infrastructure and IT Security (OCITTS) shall:
1. Issue password resets for USB storage devices;
 2. Establish standards and processes for sanitizing USB storage devices;
 3. Establish standards and select software for encrypting sensitive information on USB storage devices;
 4. Establish standards and select the USB storage device(s) approved for use on BEP information systems; and
 5. Implement and maintain a system for monitoring and auditing USB storage device use to detect unauthorized use on BEP IT systems.
- f. CIO shall:
1. Approve/disapprove connection of USB storage device to non-BEP information systems; and
 2. Approve/disapprove requests to take USB storage device to foreign countries.

MANUAL

DATE May 15, 2007

2-7 COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)

1. POLICY. The Bureau of Engraving and Printing (BEP/Bureau) Computer Security Incident Response Capability (CSIRC) provides a coordinated response for threats to information technology assets and information systems that includes preparation, detection and analysis, containment, eradication, and recovery. The BEP CSIRC will comply with Treasury policy and other Federal laws/regulations for handling and reporting incidents.

- a. Significant incidents, as defined in [Treasury TD P 85-01](#), shall be reported to the Department of Treasury CSIRC (TCSIRC) within one (1) hour of incident identification, with a follow-up report every 4 hours thereafter until the incident is resolved.
- b. Monthly summary reports of minor incidents shall be provided to the TCSIRC by the fifth calendar day of each month for incidents that occurred the previous month.

2. SUPERSESION. This chapter supersedes Chapter 2-7, "Computer Security Incident Response Capability (CSIRC)," dated May 21, 2001.

3. BEP CSIRC ORGANIZATION. The Associate Director, CIO, provides oversight of the BEP CSIRC program and ensures that the Bureau complies with Treasury policy in advocating a strong CSIRC program at the Bureau executive management level. The BEP CSIRC organization consists of the BEP CSIRC Management Team, supplemented by members of an extended team, and an Incident Response Support Team, as needed. These teams are primarily assembled with personnel from within the Associate Director, CIO organization.

- a. The BEP CSIRC Management Team directs CSIRC activities. The team consists of the following:
 - (1) Chair – Chief, Office of Critical Infrastructure and IT Security (OCIITS)
 - (2) BEP Incident Coordinator – Manager, IT Security Division (ITSD)
 - (3) Members – Chief, Office of IT Operations (OITO), Alternate Chair; Manager, IT Technical Support Division; and Manager, WCF IT Support Division.
- b. The BEP CSIRC Extended Team is composed of individuals with functional responsibilities for, or expertise in, specialized operating systems, applications, and non-standard system resources. Examples of BEP CSIRC Extended Team members include:

MANUAL

DATE May 15, 2007

- (1) Chief, Office of Enterprise Solutions (OES)
 - (2) Chief, Office of Engraving
 - (3) Chief, Office of Product Development
 - (4) Chief, Office of Financial Management
 - (5) Chief, Office of Security
 - (6) Chief, Office of Human Resources
 - (7) Chief, Office of External Relations
 - (8) Chief, Office of Quality
 - (9) Chief Counsel and/or Office of Chief Counsel representative
- c. The BEP CSIRC Incident Response Support is an ad-hoc team assembled to support the activities deemed necessary by the BEP CSIRC Management Team. This team, staffed by personnel from the CIO Directorate who are trained in incident response procedures, may include additional individuals with specialized expertise or responsibility for systems, technologies, or procedures that would help support the incident response effort.

4. RESPONSIBILITIES.

- a. The Associate Director (Chief Information Officer (CIO)) shall:
- (1) Provide oversight of the BEP incident response program;
 - (2) Assure that the Bureau complies with Treasury policy; and
 - (3) Advocate for a strong CSIRC program at the Bureau executive management level.
- b. The Chief, Office of Critical Infrastructure and IT Security (OCIITS), BEP CSIRC Management Team Chairperson, shall:
- (1) Direct the BEP CSIRC and approve resource allocations;
 - (2) Maintain a minimum security clearance level of Secret and be the primary BEP point of contact (POC) for reporting significant and minor computer security incidents;
 - (3) Coordinate all requests for outside assistance;
 - (4) Monitor and maintain the security for the BEP Enterprise IT infrastructure;
 - (5) Brief Bureau executives and managers on incidents;
 - (6) Assess the impact of incidents and security measures on IT operations;
 - (7) Respond and report to TCSIRC or other external requests for information regarding the security posture of the BEP infrastructure or the response to a security incident;
 - (8) Appoint and oversee activities of the BEP Incident Coordinator;
 - (9) Implement an annual training program to:

MANUAL

DATE May 15, 2007

- (a) Familiarize key incident response personnel with their role(s) and responsibilities; and
 - (b) Facilitate effective response by personnel in crisis situations by including simulated events into the training program.
- (10) Implement an annual test/exercise program for the incident response capability using [NIST SP 800-61](#) to determine the incident response effectiveness and have the test results documented.
- (a) When practical, automated mechanisms shall be used to more thoroughly and effectively test/exercise the incident response capability; and
 - (b) The results of the testing shall be used to update the BEP CSIRC policies and procedures.
- (11) Maintain the BEP CSIRC policy.
- c. Manager, IT Security Division (ITSD), the BEP Incident Coordinator for the BEP CSIRC Management Team, shall:
- (1) Designate at least one alternate POC who, in addition to the BEP Help Desk, can be reached after hours in the event of an emergency;
 - (2) Determine the CSIRC team resources (management and extended) required to assess any threats;
 - (3) Coordinate the efforts and facilitate communication between the BEP CSIRC Incident Response Support Team, the system owners, and the BEP CSIRC Management Team;
 - (4) Monitor for and alert the BEP CSIRC Management Team to potential threats and vulnerabilities;
 - (5) Perform internal investigations to verify the occurrence of a security compromise;
 - (6) Initiate incident evaluation, and assist and advise system owners, administrators and POCs in response and recovery operations to Bureau systems and computers. Advise and assist system owners and administrators in implementing appropriate countermeasures;
 - (7) Provide advice on technical and management measures to mitigate risk and/or recover from adverse incidents;
 - (8) Coordinate with the system owners to ensure that the corrective actions are implemented in accordance with the BEP and/or system change management procedures;
 - (9) Track and prepare reports on incidents and the outcome of completed investigations, in support of BEP or TCSIRC investigations. Prepare a monthly report of all minor incidents, as required by Treasury policy, and submit to the BEP CSIRC Chair for approval;
 - (10) Perform post-incident assessment and security enhancement; and
 - (11) Maintain the CSIRC procedures.

MANUAL

DATE May 15, 2007

- d. The Chief Office of IT Operations shall:
- (1) Serve as the alternate to the BEP CSIRC Management Team chair; and
 - (2) Assume operational responsibility for implementing the CSIRC processes in the event the CSIRC Management Team chairperson is unavailable.
- e. The Manager, IT Technical Support Division and Manager, WCF IT Support Division shall:
- (1) Maintain a complete and accurate inventory of the hardware and software in the BEP operating environment;
 - (2) Ensure that systems and applications are maintained with the proper updates and security patches;
 - (3) Provide technical advice regarding the implementation of measures to contain damage and mitigate risk;
 - (4) Provide technical specifications and status on the state of the current IT infrastructure – to include implementing, documenting, and monitoring patches, workarounds and updates;
 - (5) Facilitate communications between the WCF and Washington, DC facilities with respect to CSIRC activities;
 - (6) Identify and allocate resources for protecting IT resources and responding to incidents, assess the impact of incidents and security measures on IT operations; and
 - (7) Provide status on the state of the current IT infrastructure.
- f. Office Chiefs shall:
- (1) Designate a POC for each specialized system, equipment, or application within their functional area for reporting incidents and distributing information relating to computer security and incident reporting to users;
 - (2) Immediately notify the BEP Incident Coordinator of any security incident or compromise of information; and
 - (3) Coordinate with the BEP Incident Coordinator, in responding to security incidents and in initiating recovery efforts.
- g. System Owners shall:
- (1) Coordinate with the BEP Incident Coordinator and system administrators to initiate response and recovery operations to Bureau systems and computers, and to implement appropriate countermeasures;
 - (2) Coordinate with OCIITS and system administrators to develop a comprehensive incident response training program; and
 - (3) Review the system operational state to verify that services were restored

MANUAL

DATE May 15, 2007

successfully, if system restoration procedures are implemented in response to an incident.

h. System Administrators shall:

- (1) Coordinate with the BEP Incident Coordinator and system owners to initiate response and recovery operations to Bureau systems and computers, and to implement appropriate countermeasures; and
- (2) Coordinate with OCIITS and system owners to develop a comprehensive incident response training program.

i. Designated Accrediting Authority (DAA) shall in response to a security incident for a system under their authority:

- (1) Coordinate with the Chair, BEP CSIRC Management Team to determine if the risk(s) to the system are mitigated to an acceptable level or if additional actions are required; and
- (2) Work with OCIITS, system owner(s), administrator(s), and developer(s) to establish an action plan to mitigate any significant risk areas identified.

j. BEP CSIRC Incident Response Support Team shall:

- (1) Support the activities deemed necessary by the BEP CSIRC Management Team to respond to a security incident; and
- (2) Report any actions taken to identify, contain, or recover from a security incident to the BEP Incident Coordinator.

k. Extended Team Members shall:

- (1) When called upon by the BEP CSIRC Management Team in response to a security incident, report and begin working under the direction of the BEP Incident Coordinator to resolve the security incident; and
- (2) Consider their responsibilities to support the incident response process as their top priority task until the incident is resolved and/or the BEP Incident Coordinator has determined that their continued involvement with the incident response is no longer required.

l. The Office of Security shall assume the role of the BEP CSIRC Management Team for incidents involving classified information.

m. Bureau employees and contractors shall notify the BEP Help Desk immediately upon suspecting that an IT security related incident has, or is, occurring.

MANUAL

DATE May 15, 2007

5. REFERENCES.

- a. "Computer Security Incident Handling Guide," ([NIST SP 800-61](#)), dated January 2004.
- b. "Guide to Malware Incident Prevention and Handling," ([NIST SP 800-83](#)), dated November 2005.
- c. [Treasury Directive TD P 85-01](#), "Information Technology Security Program – Unclassified Systems," current version.
- d. [BEP Manual 10-08.29](#), "Computer Security Incident Response Capability (CSIRC) Procedures," current version.

MANUAL

DATE January 21, 2004

2-11 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.

MANUAL

DATE January 21, 2004

e. BEP Circular No. 40-00.6, "Record Systems Subject to the Privacy Act," dated February 20, 2003.

f. Executive Order 12958, "Classified National Security Information," dated April 17, 1995.

g. Privacy Act of 1974, 5 United States Code (USC) Section 552a

4. 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.

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.

MANUAL

DATE January 21, 2004

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 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.

MANUAL

DATE January 21, 2004

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.

5. 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 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.

MANUAL

DATE January 21, 2004

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 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,

MANUAL

DATE January 21, 2004

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.

6. 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.

(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

MANUAL

DATE January 21, 2004

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).

(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.

MANUAL

DATE January 21, 2004

(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.

(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.

MANUAL

DATE January 21, 2004

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

MANUAL

DATE January 21, 2004

(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.

7. 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.

8. 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.

MANUAL

DATE March 31, 2005

3-1 IDENTIFICATION AND AUTHENTICATION

1. POLICY. Security safeguards shall be in place to ensure each person having access to Bureau of Engraving and Printing (BEP) IT systems and resources is individually accountable for his or her actions on the system. User and administrator account access shall be controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.

- a. Mechanisms supporting identification and authentication shall uniquely identify each user.
- b. Cost-effective identification, authentication, and access control mechanisms shall be selected and implemented based upon information sensitivity and criticality, and level of risk.
- c. Any IT system, application, network, or device shall ensure that each user is authenticated before allowing IT system access.
- d. Shared and group user or administrator accounts shall not be implemented without a waiver. When authorized, the number of individuals having access to those accounts shall be kept to a minimum.
- e. Requests for emergency and temporary access shall be forwarded to the Information Technology Security Division (ITSD) for approval, prior to being granted.
- f. User and administrator accounts shall be suspended after 30 days of inactivity or after 3 failed logon attempts. After 180 days of inactivity, user and administrator accounts shall be deleted.
- g. User and administrator accounts for personnel on extended leave or detail for over 90 days shall be suspended within 1 business day of going on leave or detail.
- h. User and administrator accounts shall be deactivated within 1 business day of notification of an individual's departure on friendly terms and immediately upon notification of an individual's departure on unfriendly terms.
- i. Users must return all media (e.g., smart cards, SecurID) used to gain system access to ITSD on or prior to their last workday.

2. BACKGROUND. User identification and authentication (I&A) is the means of verifying the identity of users before granting access to a requested resource. Authentication counters the threat of masquerading. Users identify themselves to the system and then authenticate their identity by providing a second piece of information that is known only by the individual user or can be produced only by the user. Authentication can be implemented in varying degrees of strength and lays a foundation for other security services, such as access control and audit.

MANUAL

DATE March 31, 2005

3. RESPONSIBILITIES.

a. Access Administrator shall:

- (1) Suspend user and administrator accounts after 30 days of inactivity and delete user and administrator accounts after 180 days of inactivity; and
- (2) Authenticate the user prior to processing requests to reactivate accounts that have been inactive for less than 180 days. Valid methods of authentication are personal identification number (PIN) or in-person identification using a valid BEP badge.

b. The Support Services Division (Washington, D.C.) and the WCF IT Division shall:

- (1) Perform access administrator duties for all BEP networks and systems other than the mainframe (exceptions must be documented and approved as part of the system certification and accreditation).

c. The Information Technology Security Division (ITSD) (Washington D.C.) and the Management Control Branch (MCB) (WCF) shall:

- (1) Perform access administrator duties for the BEP mainframe. (Exceptions must be documented and approved as part of the system certification and accreditation).

MANUAL

DATE March 31, 2005

3-1-1 PASSWORD

1. **POLICY.** The Bureau shall comply with Federal regulations and standards and with Department of the Treasury and Bureau policies for providing access controls based on the positive identification and authentication of users which are appropriate for the level of the information protected. Where passwords are used for authentication the following rules apply. These rules shall be implemented and enforced using technical controls when possible.
 - a. **Creating Valid Passwords:**
 - (1) Passwords must be difficult to guess.
 - (2) Passwords shall not be a word found in a dictionary, foreign or domestic; and shall not contain common names, words related to the Bureau, birth dates or other words or phrases related to the user's personal identity.
 - (3) User passwords shall be at least eight non-blank characters long.
 - (4) System and Access Administrator passwords shall be at least 12 non-blank characters long, where technically feasible.
 - (5) Passwords shall contain a combination of uppercase and lowercase letters, and shall contain at least one number, or special character, where technically feasible.
 - b. **Changing Passwords**
 - (1) Passwords must be changed immediately after receipt of an initial or reset password.
 - (2) Passwords shall be changed at least every 90 days or when requested by OCIITS, an access administrator, a system administrator, or at the Western Currency Facility (WCF), Management Control Branch (MCB).
 - (3) The same password shall not be re-used for a period of at least six months. Password history shall be kept to prevent the reuse of the last five used passwords.
 - (4) All default or vendor passwords shall be changed, including those for software packages and maintenance accounts, prior to implementing the system in production.
 - c. **Protecting Passwords**
 - (1) Passwords shall not be shared with anyone, regardless of their position.
 - (2) Passwords shall not be kept in plain view or where easily found.
 - (3) Passwords shall not be entered into any file, program, record, or script for the purpose of creating an automated log-in feature. This means that the creation of "macro-" or other files or programs that automatically enter system identification and passwords is prohibited.
 - (4) Passwords shall be stored and transmitted using secure protocols and

MANUAL

DATE March 31, 2005

algorithms.

- (5) Passwords shall not be displayed when entered.

2. RESPONSIBILITIES.

a. Users shall:

- (1) Create, change, and protect their passwords in compliance with the password policy;
- (2) Protect user password from others. Passwords, encrypted or unencrypted, shall not be stored on any computer media;
- (3) Not use anyone else's password;
- (4) If a password compromise is suspected, change the password immediately and report it accordingly to the Help Desk;
- (5) If a password is lost or forgotten, report it according to the guidelines located at the end of this policy;
- (6) Provide identification when requesting an administrator to reset or unlock a password. Approved forms of identification include a valid personal identification number (PIN) or in person presentation of a Bureau badge; and
- (7) Notify the Help Desk in Washington; or notify the MCB for BEPMIS (including VACS), or the WCF IT Division for non-BEPMIS in Fort Worth of any unusual occurrences during logging in, signing off or while using the computer.

b. Supervisors shall:

- (1) Ensure that employees know how to create, change, and protect a password and how to protect Bureau information from unauthorized access;
- (2) Periodically review computer use policies with employees to ensure that access and other rules and regulations are being followed; and
- (3) Ensure that instances of suspected password compromise are reported to the Help Desk.

c. Access Administrators shall:

- (1) Issue initial and reset passwords for all systems assigned to them. Initial and reset passwords must comply with password policy and not be easily guessed;
- (2) Authenticate the user prior to unlocking an account or providing a new or reset password. Valid methods of authentication are personal identification number (PIN) or in-person identification using a valid BEP badge. Passwords shall be provided directly to the account owner; and
- (3) Report instances of lost passwords and suspected password compromises to OCIITS.

d. Designated Administrators in the OITO Support Services and the WCF IT Divisions shall:

- (1) Perform the Access Administrator responsibilities for all BEP networks and

MANUAL

DATE March 31, 2005

- systems other than the mainframe (exceptions must be documented and approved as part of the system certification and accreditation); and
- (2) Report instances of lost passwords and suspected password compromises to OCIITS.
- e. The Information Technology Security Division (ITSD) for the Washington D.C. facility and the Management Control Branch (MCB) (WCF) shall:
- (1) Perform the Access Administrator responsibilities for the BEP mainframe (exceptions must be documented and approved as part of the system certification and accreditation).
- f. The System Administrator shall:
- (1) Change all default or vendor passwords, including those for software packages and maintenance accounts, prior to implementing the system in production;
- (2) For shared administrative accounts or system accounts, change the password immediately when any administrator with rights to the account leaves the Bureau or is no longer responsible for the system; and
- (3) Ensure that technical controls are implemented to enforce the password rules.
- g. The Office of Critical Information and IT Security (OCIITS) shall:
- (1) Monitor the use of passwords for all authorized users, including privileged user account holders, for compliance with Bureau policy;
- (2) Audit passwords for compliance by periodically testing password strength and use;
- (3) Ensure users and administrators are trained on password use and policy;
- (4) Investigate and record instances of suspected compromised passwords; and
- (5) Deny access to BEP systems when necessary, such as in cases of intentional misuse of passwords.

Password Reset and Assistance Responsibility Matrix

	Mainframe (BEPMIS)		PC/Network	
	Day Shift	Other Shifts	Day Shift	Other Shifts
Washington, D.C.	Help Desk (202) 874-3010	Help Desk (202) 874-3010	Help Desk (202) 874-3010	Help Desk (202) 874-3010
WCF	Management Control Branch	Help Desk (202) 874-3010	WCF IT Division	Help Desk (202) 874-3010

MANUAL

DATE August 1, 2005

3-2 ACCESS CONTROLS

1. POLICY. Access controls shall be implemented to protect information technology systems and the information stored, processed, or transmitted by the system in a manner appropriate for the confidentiality, integrity, and availability levels for the information being protected.

- a. Access Controls shall:
 - (1) Support the principles of least privilege and separation of duties;
 - (2) Require users to be positively identified and authenticated with a unique identifier prior to accessing the system or its data;
 - (3) Provide timely and reliable access to Bureau networks and computers for authorized users while securing these resources from unauthorized users;
 - (4) Detect and report any unauthorized access attempts to access the protected system or information;
 - (5) Prevent an individual from having sufficient authority or information access to allow fraudulent activity without collusion; and
 - (6) Comply with Federal regulations and standards and Department of the Treasury policies in providing adequate access controls, management controls, and physical safeguards.
- b. Shared files and folders must be placed on the network. Users are not permitted to share access to files and folders located on local workstations.
- c. Access controls for all systems shall be documented in the appropriate System Security Plan.
- d. Service accounts and process accounts used to execute programs as services or processes within a system shall be documented to identify the type of access required, the purpose the account is established to support, and provide for authorization signatures to approve the use of the account on the system prior to implementation.
- e. Access to sensitive Bureau information shall be provided only after express management authorization has been obtained. The following tables describe common forms and procedures for access to BEP IT resources. All system specific access request controls shall be followed as documented in the appropriate System Security Plan.

PC/Network Access Requests (Establish, Change, or Delete)			
Type of Access	Form	Acceptable Use	Required Approvals
Standard Account	PC/Network Access Request (BEP Form 8392)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager, ITSD

MANUAL

DATE August 1, 2005

PC/Network Access Requests (Establish, Change, or Delete)			
Type of Access	Form	Acceptable Use	Required Approvals
Operating System Administrator Privileges	Special Access Request (BEP Form 8393)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager, SSD 4. Manager, ITSD
Special Account or Access Request	Special Access Request (BEP Form 8393)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager, ITSD
Internet	Internet Access Form (BEP Form 8397)	Included on internet access form	1. Office Chief 2. CIO 3. Manager, ITSD
Virtual Private Network (VPN)	Virtual Private Network (VPN) Request (BEP Form 8395)	Remote Access to Computer Systems Policy	1. Office Chief 2. Associate Director, Deputy Director, or Director 3. Manager, ITSD
Personal Electronic Device (PED)	Personal Electronic Device (PED) Authorization Request (BEP Form 9316)	Personal Digital Assistant and Multifunctional Wireless Device Policy	1. Office Chief 2. Associate Director, Deputy Director, or Director 3. Manager, ITSD

Mainframe Access Requests (Establish, Change, or Delete)			
Type of Access	Form	Acceptable Use	Required Approvals
Mainframe user account access	Request for Personnel Access Profile Change (BEP Form 8331)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. Manager, ITSD
Dispatch (to view reports on-line)	Request for DISPTACH Access (BEP Form 8391)	N/A	1. Division Manager or higher 2. Manager, ITSD
TSO/Batch Access	Request for TSO/Batch Access (BEP Form 8390)	N/A	1. Division Manager or higher 2. Manager, ITSD

MANUAL

DATE August 1, 2005

Mainframe Access Requests (Establish, Change, or Delete)			
Type of Access	Form	Acceptable Use	Required Approvals
Establish or Change an Access Profile	Request for a Profile Structural Change (BEP Form 8389)	N/A	1. System Owner(s) 2. Manager, ITSD

UNIX Access Requests (Establish, Change, or Delete)			
Type of Access	Form	Acceptable Use	Required Approvals
Standard Account	Special Access Request (BEP Form 8393)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager, ITSD
Operating System Administrative Privileges	Special Access Request (BEP Form 8393)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager SSD 4. Manager, ITSD

Database Access Requests (Establish, Change or Delete)			
Type of Access	Form	Acceptable Use	Required Approvals
Oracle user account access	Request for Oracle Database Access (BEP Form 8421)	IT Rules of Acceptable Use (BEP Form 8394)	1. System Owner 2. Manager, ITSD 3. Manager, OES
Oracle Database Profile or Access Role	Request for Oracle Database System Profiles and Access Roles (BEP Form 8420)	IT Rules of Acceptable Use (BEP Form 8394)	1. System Owner 2. Manager, ITSD 3. Manager, OES
Microsoft SQL Server user account access	Special Access Request (BEP Form 8393)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager, ITSD
Microsoft SQL Server Administrator Privileges	Special Access Request (BEP Form 8393)	IT Rules of Acceptable Use (BEP Form 8394)	1. Division Manager or higher 2. System Owner 3. Manager, OWD 4. Manager, ITSD

MANUAL

DATE August 1, 2005

2. RESPONSIBILITIES.

a. Users shall:

- (1) Complete the appropriate access request form and acceptable use agreement and obtain approvals to access BEP IT resources as documented in the preceding tables or established in the appropriate System Security Plan;
- (2) Only access systems, files, networks, and programs necessary to perform management-approved responsibilities;
- (3) Protect their account(s) and BEP information and systems from unauthorized access;
- (4) Not share their access privileges with anyone else regardless of their position;
- (5) Be accountable for all activity that occurs using their account(s);
- (6) Not attempt to bypass any implemented security or access controls on Bureau IT systems;
- (7) Not use a service account, process account, or another user account to gain access to a system or data;
- (8) Promptly report any unusual account activity or occurrences during log-on, sign-off, or during use of the IT resource to ITSD (Washington D.C.) or, to the MCB (WCF);
- (9) Identify sensitive and/or Privacy Act data and coordinate with ITSD to ensure proper access control measures are implemented;
- (10) Log-off or lock their computer system with a password protected screen saver when leaving the computer unattended;
- (11) Not access or permit access to any Bureau computer resource from a remote location unless explicitly authorized and implemented in compliance with Bureau policy; and
- (12) Promptly report any violation of this policy to ITSD (Washington D.C.) or to the MCB (WCF).

b. System Administrators shall:

- (1) Use administrator accounts for administrative duties only and not for standard user privileges (e.g. e-mail or Internet access);
- (2) Ensure that vendor-supplied default security parameters are reinitialized to more secure settings in compliance with Bureau policy;
- (3) Ensure that vendor-supplied passwords are changed and user accounts are either renamed or disabled;
- (4) Ensure the production and retention of logs for monitoring and auditing system access activities in compliance with Bureau policy;
- (5) Ensure that access to security software is restricted to authorized personnel;
- (6) Process requests to create shared network directories; and
- (7) Ensure service and process accounts are:
 - a) Properly documented and authorized for the system prior to establishing

MANUAL

DATE August 1, 2005

- the account;
- b) Used only for the purpose which is authorized; and
 - c) Secured against unauthorized access using a non-expiring password that is at least 12 non-blank characters long containing a combination of uppercase and lowercase letters with at least one number, or special character.
- c. Access Administrators shall:
- (1) Maintain the access controls in accordance with the documented System Security Plan and System Security Matrix;
 - (2) Issue access privileges for systems assigned to them;
 - (3) Ensure that the appropriate access request and acceptable use agreements have been submitted prior to implementing access;
 - (4) Process approved requests to update, disable, or delete accounts and access privileges in compliance with Bureau policy;
 - (5) Require written requests with proper authorization(s) prior to granting access to any information or resource protected by access controls; and
 - (6) Maintain authorized access request documentation.
- d. Supervisors and Contracting Officer's Technical Representatives (COTRs) shall:
- (1) Protect Bureau systems and information by ensuring that the appropriate access request form(s) and acceptable **use** agreements are submitted by the user and that the request is for the appropriate level of network, application, system, and file access for the user, based on job requirements and need-to-know;
 - (2) Ensure that authorized user accesses maintain appropriate separation of duties;
 - (3) Ensure that users have the proper level of personnel security clearances for the information or functions they will access;
 - (4) Perform reviews of and re-certify user account access and permissions at least annually;
 - (5) Submit requests to remove user access that is no longer valid or needed;
 - (6) Ensure that appropriate access controls are implemented for all Bureau information stored, processed, or transmitted in electronic form;
 - (7) Immediately notify the ITSD (Washington, D.C.) or the MCB (WCF) of all personnel suspensions, removals, or departures from duty on unfriendly terms; and expedite requests for suspension or removal of system access privileges; Following notification, approve and submit the appropriate access requests;
 - (8) Submit the appropriate requests to delete access to the ITSD (Washington, D.C.) or the MCB (WCF) when personnel leave the service of the Bureau on friendly terms no later than Close of Business (COB) on the day of departure; and
 - (9) Promptly submit the appropriate access requests to the ITSD (Washington,

MANUAL

DATE August 1, 2005

- D.C.) or the MCB (WCF) for all personnel reassignments, transfers, or access requirement changes.
- e. System Owners shall:
- (1) Identify sensitive and/or Privacy Act data and coordinate with ITSD (Washington, D.C.) to ensure proper access control measures are implemented;
 - (2) Document the access controls for their systems using a System Security Matrix and maintain this documentation as part of the system certification and accreditation package; and
 - (3) Review and approve or disapprove access requests as documented in the preceding tables to ensure appropriate level of access and separation of duties.
- f. The Chief, Office of Critical Infrastructure and IT Security (OCIITS) has the authority to approve or disapprove special requests for access to information protected by access controls.
- g. The Office of Critical Infrastructure and IT Security (OCIITS) shall:
- (1) Review all administrator position appointments for IT systems within the Bureau to ensure that a proper background investigation has been conducted based on the sensitivity of the system or information being supported;
 - (2) Ensure that administrators:
 - a) Have receive proper training to support the assigned system(s);
 - b) Understand Bureau policies, CSIRC processes, and reporting requirements for supporting the BEP security program prior to authorizing them to support the system; and
 - c) Maintain the separation of duties principles by not performing audit reviews.
 - (3) Establish audit policy to ensure events related to system security (e.g. failed logon attempts, password resets) are captured in system logs;
 - (4) Ensure that system logs are monitored and reviewed in accordance with Bureau policy and the System Security Plan to identify apparent security violations;
 - (5) Monitor account, system, and file usage for all users including system and access administrators for compliance with Bureau policy, in accordance with the System Security Plan;
 - (6) Ensure that inactive accounts are disabled and deleted in accordance with Bureau policy (Section 3-1 of this Manual);
 - (7) Document and investigate any reported unauthorized access attempts or security control breach; and
 - (8) Ensure that appropriate actions are taken to investigate, reconcile, and report any suspicious activities according to system audit and BEP CSIRC procedures; for cases involving repeated and intentional violations of access

MANUAL

DATE August 1, 2005

- policy or account misuses, deny access to BEP computer systems, networks, and Bureau authorized systems.
- h. Information Technology Security Division (ITSD) shall:
- (1) Perform access administrator duties for mainframe accounts (e.g. BEPMIS and VACS) at the Washington, D.C. facility (exceptions shall be documented and approved as part of the system certification and accreditation);
 - (2) Periodically assess the access controls and provide assistance to Bureau personnel for the design and implementation of appropriate mainframe access controls for Bureau information that is stored, processed, or transmitted in electronic form; and
 - (3) Maintain the BEPMIS Access Profiles and Security Matrix in compliance with Bureau policy and within the guidelines of Section 3-2-2 of this manual.
- i. The Manager, ITSD shall:
- (1) Ensure requests have the required approvals;
 - (2) Review and approve or disapprove all access request forms submitted as documented in the preceding tables; and
 - (3) Coordinate with Access Administrators to remove system access when notified of personnel suspensions, removals, or departures from duty on unfriendly terms and expedite requests for suspension or removal of system access privileges.
- j. The Management Control Branch (MCB) (WCF) shall:
- (1) Perform access administrator duties for mainframe accounts (e.g. BEPMIS and VACS) at the WCF (exceptions shall be documented and approved as part of the system certification and accreditation);
 - (2) Periodically assess the access controls and provide assistance to Bureau personnel for the design and implementation of appropriate mainframe access controls for Bureau information that is stored, processed, or transmitted in electronic form;
 - (3) Immediately notify the ITSD (Washington, D.C.) and WCF IT Division of all personnel suspensions, removals, or departures from duty on unfriendly terms and expedite requests for suspension or removal of system access privileges.
- k. The Manager, System Support Division shall review and approve or disapprove all access requests for operating system administrative privileges.
- l. The Chief, Office of Enterprise Systems shall review and approve or disapprove requests for database as documented in the preceding tables.
- m. The Chief, Office of Web Development shall review and approve or disapprove requests for database as documented in the preceding tables.

MANUAL

DATE August 1, 2005

- n. The System Support Division (Washington, D.C.) and the WCF IT Division shall:
 - (1) Perform access administrator duties for all BEP networks and systems (other than the mainframe) for both user and administrator accounts (exceptions shall be documented and approved as part of the system certification and accreditation).

3-2-1 ADP SECURITY MATRICES

1. PURPOSE AND SCOPE. This circular is to inform all managers of the procedures for developing, modifying, and maintaining ADP security matrices for the Bureau of Engraving and Printing Information Systems or any other computer application which has limited access provisions. A security matrix for a computer database software application is a list of all of the transactions in the application and the categories of employees who are authorized to use each transaction; it is accompanied by a list of the names of the individual employees in each category. The matrix is used to ensure that only authorized employees may use the application, and that the transactions each employee uses are appropriate to the employee's functional responsibilities. These procedures are applicable to all Bureau employees using any computer software or database applications with limited access requirements.

2. POLICY. Bureau policy is to ensure the data integrity and system security of Bureau Information Systems by developing, implementing, modifying, and maintaining ADP security matrices to prevent intentional and unintentional misuse of the computer applications used in these systems.

3. BACKGROUND. In April 1985, the Bureau implemented the first ADP security matrix (General Ledger) for the Cullinet software applications that are used for the FMIS, PAMIS, and MMS applications. Since then, several additional ADP security matrices have been developed, implemented, modified and maintained for subsequently implemented systems.

Additional Bureau Information Systems will require the development, implementation, modification, and maintenance of security matrices. To ensure an adequate level of security for all software applications, procedures for ADP security matrices must be established.

The Information Resource Security Manager (ADP Security Manager) is responsible for providing or assisting in the development of directives, standards, guidelines, and procedures needed to ensure the proper implementation and operation of security for Bureau information resources.

4. PROCEDURAL GUIDELINES.

a. DEVELOPMENT OF THE ADP SECURITY MATRIX.

(1) The application software implementation team is responsible to identify and document the specific transactions in each software application that are

MANUAL

No. 10-08.35

DATE December 18, 1986

required to access the system. The implementation team will document the transactions in the form of a matrix, with the employees identified within each users category.

(a) The matrix will include an alphabetical listing of transactions and user categories that should have access to the transactions.

(b) Each user category identified for a transaction must have two or more designated employees. Exceptions must be approved by the ADP Security Manager and the project manager.

(2) The ADP Information Resource Security Manager will review and approve the ADP security matrix in writing before distribution is made to the appropriate Office Chiefs.

(3) Each Office Chief with employees on the matrix is required to approve the original matrix and subsequent modifications to the matrix by signature.

(4) The respective project manager for each system implementation is responsible for obtaining all required signatures.

(5) The ADP Security Manager is responsible for maintaining and providing the DBA with the original security matrix and subsequent changes to be implemented.

b. MODIFICATIONS TO EXISTING ADP SECURITY MATRICES.

There are two types of modifications to an established matrix; 1) personnel and 2) structural.

(1) PROCEDURES FOR REQUESTING A PERSONNEL CHANGE. To add or delete an employee (user) from a category, or to move an employee from one category to another category within the same organizational component, the Office Chief of the organizational component must send a memorandum requesting the action to the ADP Security Manager. The ADP Security Manager will review and approve the request and forward the action to the Chief, Office of Information Systems.

(2) PROCEDURES FOR REQUESTING A STRUCTURAL CHANGE. Structural changes include the addition or deletion of transaction(s) for a category, addition or deletion of a category or modifications to access transactions within an application.

Regardless of any changes needed, each category will have a minimum of two employees, unless otherwise approved by the ADP Security Manager. The following procedures are required for a structural change:

(a) The requesting organizational component will complete a Request for Information Services (RIS) form supplied by the Office of Information Systems, User

MANUAL

No. 10-08.35

DATE December 18, 1986

Support Division (USD). The form will be accompanied by documentation which clearly defines the structural change required;

(b) Based on their knowledge of the integration properties of different software applications, the User Support Division will advise the requesting official if the change is appropriate, as submitted, or if further modification is warranted.

(c) The User Support Division Manager will forward all requests to the ADP Security Manager;

(d) The ADP Security Manager will review and approve or disapprove all requests;

(e) The requesting organization component will then obtain concurrence from all organizational components which share the data within the Bureau, as shown by the signature(s) of the Office Chief(s) with employees on the matrix;

(f) The ADP Security Manager will develop an updated security matrix reflecting the requested modifications and forward it to the DBA for implementation;

(g) The DBA will implement the requested modifications and notify the User Support Division when implementation is complete.

(3) PROCEDURES FOR REQUESTING SPECIAL CHANGES.

When a modification of a transaction requires program changes, the requesting official will consult with the DBA Staff and User Support Division prior to submitting a request through the normal procedures.

5. ADP SECURITY MANAGER RESPONSIBILITIES.

a. Approve all requested modifications to security matrices and maintain current listings of all ADP Security Matrices: and

b. To verify and resolve any security matrix related conflicts about separation of duties and responsibilities within the BEP organizational units.

6. DATA BASE ADMINISTRATOR RESPONSIBILITIES.

a. Ensure that all signature blocks on the request for new matrices, or modifications for existing matrices are signed prior to implementing the change.

b. Implement all requests within two weeks of receipt of approved security matrix from the ADP Security Manager.

7. USERS SUPPORT DIVISION RESPONSIBILITIES.

- a. Provide the necessary forms and guidance to obtain the appropriate documentation regarding modifications and the signatures required for the form(s).
- b. Maintain back-up copies of all approved security matrices, as well as requested modifications to them, in the specific application project file to which they pertain.
- c. Advise the user on changes involved with the integration properties of software application.

3-2-2 MANAGEMENT INFORMATION SYSTEM SECURITY PROFILES

1. PURPOSE. This circular establishes the policy and procedures for maintaining and modifying a set of security profiles for computer applications and users of the Bureau of Engraving and Printing Management Information System (BEPMIS). These security profiles are access control mechanisms used to ensure only authorized personnel use the applications and transactions appropriate to their functional responsibilities, thus promoting a separation of duties.

2. POLICY. It is the policy of the Bureau of Engraving and Printing (BEP/Bureau) to ensure that data integrity and system security of BEPMIS applications are maintained by security profiles established for the purpose of preventing intentional and accidental misuse of BEPMIS computer applications.

3. SCOPE. This circular applies to all Bureau employees and all personnel under contract or subcontract to the Bureau who access applications on BEPMIS.

4. BACKGROUND. In April 1985, the Bureau of Engraving and Printing implemented its first automated security matrix to administer access control for BEPMIS application systems. Due to the upgrade of the BEPMIS software, the existing security mechanism and procedures have changed. This policy has been revised to reflect these changes.

5. DEFINITIONS.

a. **Security Matrix.** The security matrix was a tool for authorizing access to help secure the Bureau's information systems. It consisted of like transactions grouped together for all Computer Associate's Consolidated Application Systems (CAS) and user written applications representing financial, manufacturing and administrative activities carried out in the Bureau.

b. **Security Profiles.** The security profiles are pre-approved groups of transactions that delineate a job function. People are assigned to these groups based on their job requirements for using Computer Associate's Consolidated Application Systems software and user written applications. The security profiles ensure that only authorized users gain access to the appropriate computer applications needed to perform their job.

6. RESPONSIBILITIES.

a. The User Support Division (USD), Office of Information Systems, shall analyze all requests for changes to the structure of the security profiles.

b. The Computer Systems Security Division (CSSD), Office of Management Control shall:

MANUAL

DATE May 22, 1997

(1) provide final review, approval and/or disapproval of all requests for changes to the security profiles.

(2) verify that the structure of the security profiles is in compliance with internal controls.

(3) implement approved user access profile changes for existing users.

(4) create Accessor IDs (ACIDS) and user access profiles in both the mainframe's security software package (Top Secret) and the BEPMIS software application for approved new users.

(5) implement all structural changes to the profiles within 10 working days of receipt of the approved profiles structural change request form.

c. Designated Approving Officials shall:

(1) provide a first level review, approval and/or disapproval of all requests for changes to the security profiles.

(2) verify the accuracy of the security profiles for each application under their authority.

d. Access Sponsors shall:

(1) accept full responsibility for authorizing access to users within their organizational component. Users have a duty and responsibility to ensure the ethical conduct and protection of the data associated with the access privileges provided them by the sponsor.

(2) verify with CSSD all access authorizations for individuals under their authority.

(3) request access for individuals under their authority on a Request for Personnel Access Profile Change (Exhibit A).

(4) initiate any additions, deletions, or modifications to a user's access profile.

7. PROCEDURES.

The following procedures shall be followed to process a request for personnel and structural profile changes or special requests.

a. Request for Personnel Access Profile Change (Exhibit A).

(1) The access sponsor shall initiate a request and provide the individual's name, badge ID, type of change and access desired. The access sponsor shall submit the request to CSSD.

(2) CSSD shall review requests to determine that the requests are within the scope of authorized activities for the computer user. If the scope of activities is not appropriate, the access sponsor and designated approving officials shall resolve the issue(s). If the scope of activities is appropriate, the approving officials shall approve the request and return it to CSSD.

(3) CSSD shall review all requests for access to administrative, financial, manufacturing and product accountability applications for compliance with Bureau internal controls. If the request is in compliance with internal controls, CSSD shall approve and implement the requested access changes as specified on the request within 5 working days and notify the access sponsor of the requested status.

b. Request for a Profile Structural Change (Exhibit B).

(1) Bureau managers shall submit requests for changes to the security profile structure to CSSD.

(2) USD and CSSD shall perform an analysis of the requirements from computer users and analyze the data properties to determine if a structural change is needed.

(3) USD and CSSD shall review the options to determine the impacts of a structural change on the profiles and established internal controls.

(4) CSSD shall approve or disapprove a profile structural change request received from USD and approved by the appropriate Financial Management Systems, Production and Inventory Management Systems, Purchasing Systems and Product Accountability Systems approving officials. A disapproval request will be returned to USD. An approved request will be implemented by CSSD.

(5) CSSD staff will implement the profile structural change within 10 working days of the receipt of the change request form. CSSD staff will then notify USD when the change is complete.

MANUAL

No. 10-08.35

DATE May 22, 1997

(6) CSSD will prepare and distribute a report showing the new security profile structure.

c. Special Request for Changes.

All special requests for changes to the security profile structure shall be coordinated directly with USD and CSSD managers prior to submitting a formal request for change.

MANUAL

No. 10-08.35

DATE May 22, 1997

(PLEASE PRINT CLEARLY)

1. USER'S NAME - PRINT THE PERSON'S FULL NAME

II. USER'S BADGE NO - PRINT THE NUMBER THAT APPEARS ON THE FRONT OF THE PERSON'S BADGE

III. USER'S JOB TITLE - PRINT THE PERSON'S JOB TITLE FOR VERIFICATION OF ACCESS PROFILE

IV. USER'S OFFICE - PRINT THE PERSON'S OFFICE AND SECTION

V. PLACE AN 'X' BY THE DESIRED COURSE OF ACTION. IN ORDER TO ADD OR CHANGE A USER'S PROFILE, SEE THE ATTACHED SHEET OF VALID PROFILES

IV. ACCESS SPONSOR SIGNATURE, TITLE AND DATE- MUST BE SIGNED AND DATED BY A MANAGER, SUPERVISOR OR OFFICE CHIEF

SEND COMPLETED FORM TO: COMPUTER SYSTEMS SECURITY DIVISION
 ROOM 321-8A
 ATTN: ACCESS REQUEST

MANUAL

No. 10-08.35

DATE May 22, 1997

EXHIBIT "B"

REQUEST FOR PROFILE STRUCTURAL CHANGE (G12PIDMS)

SEE INSTRUCTIONS ON BACK

I. PROFILE NAME: _____

II. PROFILE OFFICE: _____

III. ACTION TO BE TAKEN:

- ADD PROFILE
- DELETE PROFILE
- CHANGE PROFILE

IV. ADD TRANSACTION TO PROFILE:

DELETE TRANSACTION FROM PROFILE:

V. COMMENTS: _____

VI. COORDINATED BY:

USER SUPPORT DIVISION (OIS)	DATE
-----------------------------	------

VII. APPROVALS: (PROJECT MANAGERS - REQUIRES ALL SIGNATURES)

FINANCIAL SYSTEMS PROJECT MANAGER	DATE
-----------------------------------	------

PRODUCTION & INVENTORY SYSTEMS PROJECT MANAGER	DATE
--	------

PURCHASING SYSTEMS PROJECT MANAGER	DATE
------------------------------------	------

PRODUCT ACCOUNTABILITY SYSTEMS PROJECT MANAGER	DATE
--	------

OFFICE OF SECURITY PROJECT MANAGER	DATE
------------------------------------	------

VIII. CONCURRENCE:

COMPUTER SYSTEMS SECURITY DIVISION MANAGER	DATE
--	------

FOR COMPUTER SYSTEMS SECURITY DIVISION USE

Date Received: _____

Date Implemented: _____ by _____

PROFILE ID ASSIGNED: _____

Date Verified: _____ by _____

Date Filed: _____

DATE May 22, 1997

INSTRUCTIONS FOR COMPLETING REQUEST FOR PROFILE STRUCTURAL CHANGE FORM

(PLEASE PRINT CLEARLY)

- I. PROFILE NAME - LIST THE NAME OF THE PROFILE TO BE ADDED OR CHANGED (see attached list)
 - II. PROFILE OFFICE - LIST THE OFFICE THE PROFILE BELONGS TO.
 - III. PLACE AN 'X' BY THE DESIRED COURSE OF ACTION.
 - IV. PRINT THE TRANSACTION AND APPLICATION TO BE ADDED TO OR DELETED FROM THE PROFILE
 - V. COMMENTS: - ANY SUPPORTIVE OR ADDITIONAL INFORMATION SHOULD BE INSERTED HERE
 - VI. COORDINATED BY - MUST BE SIGNED AND DATED BY AN OIS/USD STAFF MEMBER
 - VII. APPROVALS - MUST BE SIGNED AND DATED BY ALL PROJECT MANAGERS
 - VIII CONCURRENCE - MUST BE SIGNED AND DATED BY THE OMC/CSSD MANAGER
- SEND COMPLETED FORM TO: COMPUTER SYSTEMS SECURITY DIVISION
 ROOM 321-8A
 ATTN: PROFILE CHANGE

DATE July 30, 1987

3-2-3 MAINFRAME SECURITY SOFTWARE POLICY

- 1. PURPOSE.** This circular establishes policy, and assigns responsibility for administering, maintaining, and using mainframe security software in the Bureau of Engraving and Printing (BEP).
- 2. POLICY.** The Bureau of Engraving and Printing objectives for mainframe security software are to:
 - a. Restrict computer processing activities to only personnel who have the proper authority.
 - b. Protect critical information from accidental or intentional modification, destruction, duplication, or disclosure.
 - c. Monitor computer processing activities and produce audit reports that show who accessed what resources.
 - d. Hold individual users of the system accountable for their actions.
- 3. SCOPE.** This circular applies to all Bureau employees and all personnel under contract or subcontract to the Bureau.
- 4. BACKGROUND.** Security software was developed to protect mainframe computers from unauthorized access. It allows the Bureau to control access based on the information needs of individuals and offices. The information that is being protected includes Privacy Act data as well as sensitive and mission-critical data.
- 5. DEFINITIONS.** For the purpose of this circular, the following definitions apply:
 - a. Access. The way in which a resource can be used. This includes creating, modifying, and deleting it.
 - b. ACID. (Accessor ID) an alphanumeric sequence of characters by which a group of one or more users is authorized to access specified resources on the mainframe computer.
 - c. Audit/Tracking File. The file used by the mainframe security software to record security violations, job and session initiations, and resource and user activities.
 - d. Backup/Recovery File. A backup copy of the Security File which is saved daily. The backup is used with the Recovery File to recreate the Security File when it becomes necessary.

MANUAL

No. 10-08.35

DATE July 30, 1987

e. Computer Security Violation. An action or lack of action that provides the potential for unauthorized access to any computer resource. An unauthorized attempt to access a computer resource or the use of legitimate authorization in any manner other than it was intended.

f. Recovery File. The file that records all changes made to the Security File.

g. Resources. The mainframe computer, any equipment that is connected to the mainframe, expendable and non-expendable computer supplies, storage media, computer programs and data.

h. Security Administrators.

(1) Central Security Administrator. A person assigned administrative authority and control by the Master Security Administrator to identify users and resources within their designated area. In BEP this function will be performed by the Central Security Co-Administrators (see below).

(2) Co-Administrators. In BEP, administration of the mainframe security program is performed jointly by the Office of Security and the Office of Information Systems. One Central Security Co-Administrator is appointed by each Master Security Co-Administrator. The authorities and responsibilities of the Master Security Co-Administrators and the Central Security Co-Administrators are given below.

(3) Department Security Administrator. A person assigned administrative authority and control by the Division Security Administrator to identify users and resources within their designated area.

(4) Division Security Administrator. A person assigned administrative authority and control by the Central Security Administrator to identify users and resources within their designated area.

(5) Master Security Administrator. A person with complete administrative authority and control for identifying users and resources for the mainframe security software. In BEP this is a joint function shared by the Chiefs of the Office of Security (OS) and the Office of Information Systems (OIS).

i. Security File. The computer file that is used by the mainframe security software that specifies those activities and resources for which each user is authorized.

6. RESPONSIBILITIES.**a. OFFICE OF SECURITY AND OFFICE OF INFORMATION SYSTEMS.**

The Office of Security and the Office of Information Systems will co-administer all mainframe security software through the Master Security Administrator and the Central Security Administrator functions. The co-administration duties and responsibilities include:

(1) As Master Security Co-Administrators, the Chief, Office of Security and the Chief, Office of Information Systems will:

(a) Jointly develop a unique password that can not be known without both being present.

(b) Jointly store the unique password in an approved safe where it will only be removed by the OS Duty Officer in the presence of both Chiefs. In the case of the unavoidable unavailability of either of the Office Chiefs, their appointed representative Central Security Co-Administrator may act in their place.

(c) Jointly enter the date, time, reason for access, in the Duty Officer's log when the unique password is used in case of an emergency.

(d) Jointly assign ACID's and passwords for non-Bureau auditors. The Office of the Management Services will be notified whenever an audit is to be performed.

(e) Each appoint a representative to be one of the two Central Security Co-Administrators of the mainframe security software.

(f) Jointly appoint additional Central Security Administrators if they are required for the administration of sub-systems. These additional Central Security Administrators have less authority than the Central Security Co-Administrators.

(g) Monitor all aspects of the mainframe security software program.

(2) The Central Security Co-Administrators:

(a) Educate all mainframe computer users about BEP security software policy and in the use and features of the security software.

(b) Assist computer users in determining and implementing security protection that is appropriate for their computer resources.

(c) Document the security controls available, and communicate them to all appropriate security system users.

(d) Support and monitor decentralized administration where decentralization is required. Assigning security software package passwords and user ID's will not be decentralized beyond the Co-Administrators.

(e) Log and report violations to the appropriate individuals.

(f) Generate and review security violation reports, and take appropriate actions.

(g) Monitor user activity.

(h) Jointly design the security requirements for general purpose software including, but not limited to, the operating system, communications software, database management, sort/merge, and similar software.

(i) Appoint the Department Security Administrators that are needed to manage the mainframe security software.

b. OFFICE OF SECURITY. The Office of Security administers and maintains all mainframe security software jointly with OIS through the Central Security Administrators via the ADP Security Manager and has the responsibility to:

(1) Develop and promulgate automated information resource security standards to be followed by users of the mainframe security software.

(2) Identify any risks and vulnerabilities in the mainframe security software.

(3) Administer security within the guidelines of this policy.

(4) Monitor all aspects of the mainframe security software package to ensure that it is functioning properly and to discover any attempts to evade its effectiveness.

(5) Monitor the use of all system and application resources on the mainframe computers to reduce the opportunity for any automated information resources security violation.

(6) Provide auditing assistance by use of the mainframe security software when required.

(7) Approve all data for the Security File.

(8) Verify that the Security File is implemented properly.

DATE July 30, 1987

c. OFFICE OF INFORMATION SYSTEMS. The Office of Information Systems administers and maintains all mainframe security software jointly with OS through the Central Security Administrators and has the responsibility to:

(1) Maintain the security software in a secure and responsible manner, ensuring that the data processing environment is always protected. This includes notifying the ADP Security Manager as soon as possible if the security software is ever disabled. A written explanation will be provided to the ADP Security Manger once the crisis has past.

(2) Distribute passwords and ACIDs to approved users.

(3) Maintain up-to-date lists for use by the Central Co-Administrators of users and accounts for TSO, ROSCOE, IDMS and/or similar software packages which are maintained solely by OIS.

(4) Limit development and availability of any computer program capable of bypassing security to only those situations which have been approved jointly by the Co-Administrators.

(5) Assure that full security software protection is used after an application is moved from test status into production status.

(6) Install and maintain security software package(s).

(7) Develop and maintain the Security File which shows which users have authorized access to what computer resources.

(8) Develop and maintain the Backup/Recovery Files and procedures for the security software package.

(9) Maintain the Backup/Recovery Files for the security software on a different physical device from the Security File.

(10) Perform customization of security software only after joint approval of the Co-Administrators.

(11) Provide the following information which is needed to establish the Security File when security software is initially installed on a mainframe computer system:

(a) A list of all computer terminals and their physical locations.

(b) A list of all user ID's. For each user ID, show the names of authorized users and the names of the applications that are accessible by the ID. For each

MANUAL

No. 10-08.35

DATE July 30, 1987

application show all computer files and programs which it can access. For each file, show any read/write or other keys that are associated with it.

(12) Coordinate with the ADP Security manager prior to installing any new applications on the computer. This applies only to new applications which have not been approved by the IRM Committee.

(13) Notify the ADP Security Manager prior to authorizing any new user to any application other than those listed in c(3) above.

(14) Notify the ADP Security Manager whenever authorization is increased, reduced or withdrawn from any user.

(15) Provide an up to date list of all terminals that are connected to the mainframe computer as required by the ADP Security Manger or others who are authorized to audit the mainframe computer system.

(16) Select and install additional data security controls that are recommended by the Co-Administrators.

(17) Report security violations to the ADP Security Manager.

(18) Define and implement security requirements for Bureau applications including work performed by the Database Administration Staff.

(19) Provide auditing assistance as required. All audits will be reported, in writing, to the BEP ADP Security Manager before any audit work is begun.

d. **ALL USERS.**

(1) Keep all passwords used to access data processing resources and facilities confidential.

(2) Change their password at least every 30 days.

(3) Notify the Central Security Administrators whenever abuse of a password or ACID is suspected.

(4) Actively support all ADP security procedures.

6. SECURITY VIOLATIONS.

a. All security violations, whether intentional or unintentional, will be logged when they occur by the security software. Security violation reports will be prepared only by the Central Security Co-Administrators.

MANUAL

No. 10-08.35

DATE July 30, 1987

b. Repeated intentional security violations by individuals will result in suspension of computer access rights, disciplinary action and/or termination of employment.

3-3 REMOTE ACCESS TO COMPUTER SYSTEMS

1. PURPOSE AND SCOPE. This Circular establishes responsibilities and procedures for accessing Bureau of Engraving and Printing (Bureau/BEP) mainframe, servers, or other computer resources from a remote location. It is intended to limit access to Bureau systems to authorized users only, to allow access when required by these users, to protect sensitive information, and to protect Bureau property.

2. POLICY. It is the policy of the Bureau to protect the confidentiality of sensitive information, to ensure that it maintains its integrity and is not changed or manipulated by unauthorized users, and to ensure that those individuals who have a need to access Bureau communication systems, databases, files or documents have the ability to do so in a timely manner without compromising the data or their privacy.

3. DEFINITIONS.

a. Access – Entry into the Bureau Local Area Network, e-mail system, or other computer or communications link associated with the Bureau network or stand-alone computer. Access may be gained through approved methods of connection (e.g. secure modem or Virtual Private Network (VPN)/internet connection).

b. Computers – Only Bureau issued computing devices, which could be laptops, Bureau issued personal computers, or other hardware, may be connected to the Bureau network or other Bureau computers. Additional authorization is required to remove these computers from the Bureau.

c. Portable Electronic Devices (PEDs) – These devices can function as Personal Digital Assistants (PDAs) and connect to the internet to retrieve e-mail. They also have a number of other uses, including web surfing and paging. The policy for use of Portable Electronic Devices is covered in a separate circular.

d. Sensitive Information – This includes any information which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information may be (but is not always) marked “Sensitive But Unclassified” (SBU), “For Official Use Only” (FOUO), or “Limited Official Use Only” (LOU).

4. REFERENCES.

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

BEP Security Manual, No. 71-00, February 1, 2001.

Department of the Treasury Security Manual, TD 71-10.

“Electronic and Information Technology – Accessibility”, PL 105-220, Section 508 (29USC 794d), August 7, 1998.

“Protection of Laptop Computers”, Memorandum from James J. Flyzik, Deputy Assistant Secretary (Information Systems) and CIO, Department of the Treasury, March 2001.

Privacy Act of 1974 (5 USC 552a).

Computer Security Act of 1987 (PL 100-235).

“Security of Federal Automated Information Systems”, OMB Circular No. A-130, Appendix III (revised October 2000).

5. RESPONSIBILITIES.

a. The Manager, Information Technology Security Division (ITSD), is responsible for the Bureau’s overall automated information security program. The Manager shall:

- (1) authorize methods of connection for remote access (e.g., secure modem, VPN);
- (2) authorize remote access devices and communications methods (e.g. laptops, PDA’s, analog telephone, wireless, cable or DSL);
- (3) authorize users of remote access devices to connect to the Bureau computing equipment;
- (4) administer VPN configuration and access controls;
- (5) issue secure modems;
- (6) authorize the Systems Support Division (SSD) to install the approved access hardware or software;
- (7) evaluate technologies which ensure secure remote connections and approve devices or software for use;
- (8) maintain records of users who have remote access, including types of access devices, access levels, communications and approving authority; and
- (9) periodically audit use of remote access, assess security of connections, and verify appropriate levels of access.

MANUAL

No. 10-08.35

DATE May 21, 2001

b. The Manager, Systems Support Division, is responsible for the installation and maintenance of modems, VPNs, and other hardware or software which has been authorized by the appropriate parties. The Manager shall:

(1) ensure that all authorizations have been given before installing remote access devices; and

(2) assign system administrators the responsibility of operational security for devices installed or maintained. The system administrator has the responsibility to alert the Manager, SSD, and the Manager, ITSD, to viruses, attacks, or other security threats, and also to available patches or workarounds for security problems with installed software (if the system administrator is a contractor employee, the COTR for that contract shall be the operational security administrator).

c. Users shall:

(1) apply for authorization to connect to the Bureau mainframe, servers, or other computer resources from remote locations from appropriate authority (at least the Associate Director level for remote connectivity);

(2) provide justification for requiring remote access that is directly related to current job function;

(3) notify the Manager, Information Technology Security Division, if job function or position changes and the need for remote access changes;

(4) understand and agree to abide by rules of use for remote access and for remote access devices. These rules will include, but are not limited to:

(a) identification of the sensitivity of the information to be accessed on the Bureau network or equipment;

- Remote access will be for nonsensitive or sensitive but unclassified information only; if access is required for information which is within a National Security Classification or is otherwise compartmented, contact the Manager, Information Technology Security Division.

- Files which are stored on a remote device will be at the nonsensitive or SBU level only. If information maintained is at the SBU level, the user must consult with the Manager, Information Technology Security Division to ensure that appropriate protection is installed.

(b) connection to Bureau remote devices only as authorized;

- Only Bureau issued equipment that has been approved for remote access may be connected to the Bureau network, mainframe, servers, or other computers.

- Bureau equipment may be connected only through approved devices/software (e.g. encrypted modem or VPN software) issued by the Bureau. VPN connectivity shall be only through connections specifically authorized by the Manager, ITSD. This means that the Manager, ITSD, shall be notified of the type of access available to the laptop or PED; for example, whether it is analog telephone, wireless, cable or DSL, or other.

In certain circumstances, a Bureau employee may be authorized to use a Bureau issued personal computer from a remote location. Connectivity restrictions for these computers are the same as for laptops.

- Devices not specifically authorized by the IT Security Division shall not be connected to Bureau networks or computers. This means that non-Bureau issued personal computers, PDAs, etc. shall not be connected to the Bureau network.

- No Bureau device shall be connected to any non-Government network or to any other non-Government device. For Bureau VPN users, this means that any internet connectivity must be through the Bureau approved ISP.

- A personal firewall and virus scanning software must be used for all connections.

(c) protecting the information on the remote device from unauthorized disclosure. This includes ensuring that access to information on the laptop or PED is password protected. The password shall be chosen and changed as required by Bureau password policy and shall not be provided to any other individual. It also includes not using or leaving the laptop or PED in a public place where information may be viewed or retrieved by others;

(d) reporting the loss of any Bureau owned remote access equipment. Also reporting the potential loss or compromise of any sensitive information contained on a remote device; and

(e) reporting attacks on Bureau equipment or networks and reporting viruses or other malicious code to the Manager, ITSD.

d. Office Chiefs, through their Associate Directors, retain the responsibility for the appropriate and secure use of remote technologies by the employees who they have authorized to have access. They shall:

(1) Prepare requests for remote access for users if the access is justified in supporting a business need and related to the employee's job functions;

(2) Provide access requests with recommendations to the appropriate Associate Director for final approval;

(3) monitor usage and act to remove access when Bureau policy is violated;

(4) maintain records of authorized users and government owned equipment furnished to employees. Ensure accountability of issued assets and integrity of Bureau networks, systems and information; and

(5) notify the Manager, Information Technology Security Division, if functions or positions change and the need for remote access changes.

DATE June 27, 2001

3-7 GATEWAY/FIREWALL POLICY

1. PURPOSE AND SCOPE. This Circular establishes policy guidance for implementing Internet Protocol (IP) connectivity from Bureau networks to the Internet, intranets and other networks. The Circular has applicability to all communications within the Bureau, between the Bureau and Fort Worth, and between the Bureau and external sites. This policy does not affect user guidelines except in requiring that external communications are directed only through the Bureau firewall.

2. BACKGROUND. The purpose of a firewall is to protect internal information systems from external attacks. An inter-connected environment is desirable for conducting Bureau and Government business, but is also susceptible to various forms of attack, resulting in loss of service or compromise of information. A risk to one system becomes a risk to many systems and a firewall forms part of a comprehensive security strategy to counter external threats.

3. REFERENCES.

“Gateways/Firewalls,” Department of the Treasury Security Manual TD P 71-10, VI. 4.C.4-S., January 13, 1999.

“Technical Security Standard (TSS) 001: Gateways/Firewalls,” Department of the Treasury Security Manual TD P 71-10, VI.4.C.4, January 13, 1999.

“Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,” National Institute of Standards and Technology (NIST) Special Publication SP 800-10, December 1994.

“Firewalls,” Information Assurance Technical Framework (IATF) version 3.0, National Security Agency, September 2000.

“Firewall Technical Security Standard,” BEP Technical Standard, Associate Director (CIO).

“Certification and Accreditation of BEP Systems and Applications,” BEP Circular No. (in draft, pending approval).

4. POLICY. It is the policy of the Bureau of Engraving and Printing that:

a. All connections between Bureau networks or networked devices (including local area networks, e-mail services, InSite, or dedicated computers) and external sources (such as remote service to Bureau computing devices, the Internet, and Treasury or other extranets) shall be centrally managed. This requirement for central control and security review also applies to dial-up service, including modems and public telephone service, even though the service may not pass through a Bureau firewall.

b. Any direct connection to the Internet or an extranet or any e-mail service must pass through the Bureau firewall. Any incoming services, including dial-up access to the LAN or mainframe, shall also pass through the Bureau firewall.

c. The firewall will be configured so as to exclude any services or types of transmission except those which are explicitly permitted. For example, only those Transport Control Protocol (TCP) or User Datagram Protocol (UDP) services which are specifically permitted shall be allowed.

d. Bureau laptop computers which are operated in a remote configuration with connectivity to the Bureau LAN or any computer with independent connectivity to the Internet shall have a firewall installed, which will be configured to meet the requirements for laptop computers in the Bureau "Firewall Technical Security Standard."

e. The Bureau firewall will be treated as a general support system and will be certified and accredited in accordance with the requirements contained in the Bureau Circular, "Certification and Accreditation of BEP Systems and Applications."

f. The Bureau firewall will log incoming and outgoing traffic and will have the capability for identifying suspicious activities. These audit files will be maintained for a prescribed period and may be used in investigations or for other official purposes.

5. RESPONSIBILITIES.

a. The Manager, Systems Support Division shall:

(1) designate the system administrator and an alternate system administrator for the Bureau firewall;

(2) configure the Bureau firewall according to the applicable Firewall Technical Security Standard and shall document, with justification, any changes to the configuration. All configuration changes shall be coordinated with the Information Technology Security Division (ITSD) prior to implementation;

(3) provide mechanisms for reduction of audit logs and shall report suspicious activity to ITSD;

(4) enable log alarm functions and report alarms immediately to ITSD;

(5) maintain firewall operating capability, including developing contingency procedures for use when firewall is disabled or compromised; and

(6) develop a process for exceptions and waivers to firewall configuration or firewall standards that includes, as a minimum:

(a) a description of the exception or waiver and the rationale, including a business case, if applicable;

(b) an assessment of risk associated with granting the exception/waiver;

(c) a presentation of actions that could mitigate risk; and

(d) approval of ITSD.

MANUAL

No. 10-08.35

DATE June 27, 2001

- b. The Manager, Information Technology Security Division shall:
- (1) issue password and other administrator access and authorization for the Bureau firewall, and shall periodically monitor access and system utilization by the administrator;
 - (2) review and evaluate firewall configuration and changes to that configuration;
 - (3) identify patches and upgrades for system bugs or vulnerabilities;
 - (4) appoint a backup firewall system administrator;
 - (5) periodically audit the firewall and shall review system audit logs on other occasions as necessary;
 - (6) shall coordinate with the Manager, Systems Support Division, in certifying and accrediting the Bureau firewall and in making any subsequent hardware or software modifications;
 - (7) approve firewall software;
 - (8) review and approve any firewall contingency plans to ensure backup alternatives do not compromise security or privacy; and
 - (9) review and evaluate business cases or other justification for applications or services which require exceptions or amendments to firewall policy.
- c. The Chief, Office of Systems Development shall coordinate access requirements for new web, database, or intranet applications to ensure that services required to support the Bureau business through the firewall are within the approved security framework or that a business case has been developed and approved by the CIO for exceptions.
- d. Bureau users shall not attempt to circumvent the Bureau firewall or to disable the connectivity of computers through the firewall.

DATE March 1, 1993

3-11 PROTECTING BUREAU COMPUTERS FROM COMPUTER VIRUSES

1. PURPOSE AND SCOPE. The purpose of this circular is to remind all Bureau employees and contractors of the threat posed by computer viruses, as well as presenting preventive measures which should be taken to protect Bureau computers against computer viruses.

2. POLICY. It is the policy of the Bureau to implement controls and procedures designed to protect information resources from damage and/or destruction by computer viruses and other forms of malicious software.

3. BACKGROUND. Personal computers (PC's), which are used by many Bureau employees and contractors in their daily job functions, are particularly vulnerable to a special kind of threat, namely computer viruses.

A computer virus is an unwanted computer program which attaches itself to (infects) other programs. Once a virus has infected a program, it will continue to spread itself by infecting other programs, both on the computer's hard disk, and on any floppy diskettes used in the computer. One of the most common ways by which viruses spread from computer to computer is through the use of floppy diskettes.

Once a virus has infected a computer, it may perform a wide variety of functions ranging from displaying simple messages on the monitor screen to destroying all of the data and programs on the computer's hard disk, as is the case with the Michelangelo virus. Additionally, once a virus infects a program, it may either begin to perform its functions immediately, or wait for a specific condition to occur (e.g., the Michelangelo virus does not activate until the computer's date is March 6 and the computer is turned on).

Finally, computer viruses, if not properly guarded against, can rapidly spread to large numbers of computers, causing considerable damage and destruction to data and programs. It is therefore, most important that all computer users take seriously the threat of computer viruses. Section 5 of this circular outlines some preventive measures to safeguard against the virus threat. If followed, these guidelines will significantly decrease the risk of valuable information from being damaged or destroyed.

4. REFERENCES. Department of the Treasury Directive TD P 71-10, Chapter 6, Number 5.A, "Malicious Software Countermeasures," dated October 1, 1992.

5. PROCEDURES.

A. To protect Bureau computers against viruses, all persons using Bureau computers should:

- (1) Use only Bureau-approved software on Bureau computers.

MANUAL

No. 10-08.35

DATE March 1, 1993

(2) Back up data and programs on a regular basis.

(3) Have anti-viral software installed on the computer on which you are working. If you do not have access to antiviral software, contact the Computer Systems Security Division (CSSD) at 874-3549 or 874-3554.

(4) Scan computers for viruses on a regular basis.

(5) Always scan diskettes before using them on any Bureau computer. This includes master and working diskettes containing off-the-shelf software since there have been cases where diskettes received from software manufacturers have been infected with viruses.

B. If you are certain that the computer you are using is infected with a virus, or you suspect that a virus may be present:

(1) Contact CSSD for assistance.

(2) Do not use the infected computer in stand-alone mode, or log on to the local area network (LAN) if the computer in question is networked.

(3) Do not use any diskettes in the infected computer.

(4) Do not share any diskettes used on the infected computer with co-workers. If a diskette is infected, the virus could be spread to other computers.

(5) Attach a notice to the front of the computer warning others not to use the computer because it is infected with a virus.

Your attention to and awareness of these procedures will greatly assist in protecting the Bureau's valuable information resources which you have worked hard to create and maintain. If you have any questions regarding computer viruses or any of the information presented in this circular, contact the Computer Systems Security Division at 874-3554.

3-14 Encryption

1. POLICY. This section establishes policy for the use of encryption for computer and telecommunication systems.

a. The Office of Critical Infrastructure and IT Security must evaluate and authorize all encryption methods and implementation plans prior to procurement; or if no procurement is involved, prior to implementation to ensure that:

- (1) When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation, except when no approved encryption technology solutions are available that address the specific technology;
- (2) The encryption solution is designed and implemented to meet security requirements;
- (3) When possible, the encryption technique does not depend on user choices or actions;
- (4) Encryption systems provide for centralized management and encryption key recovery to ensure data recovery and support availability requirements;
- (5) If public key certificates are used, the certificates shall be obtained or derived from the Treasury certificate authority; and
- (6) Separate certificates will be used for encryption and digital authentication (digital signature).

b. Encryption is for official use only. Personal use is not permitted.

c. All Bureau and Treasury information on all mobile media, including mobile media used within Bureau facilities, must be encrypted.

d. Encryption shall be used to protect the confidentiality of all remote access communications with Bureau systems.

e. When wireless access/transmission is permitted, encryption shall be used.

f. Data links among Bureau, Treasury or Government facilities via the Internet or dedicated telecommunications services shall be encrypted.

g. Highly sensitive information transmitted via e-mail messages and their attachments shall be encrypted.

h. Each encryption implementation shall be covered by an encryption plan that specifies:

- (1) Configuration layout, showing complete end-to-end details of the telecommunication or computer systems encryption points;
- (2) The type of encryption to be used;
- (3) The source of key generation and insertion for symmetrical and asymmetrical encryption methods;
- (4) The maximum length of time allowed before the encryption key must be updated; and
- (5) The assignment of responsibility and procedures for key generation, distribution and loading, update, validation, escrow, recovery, and revocation.

2. DEFINITIONS.

a. **Bureau and Treasury Information.** For the purpose of this policy, this does not include non-Treasury originated information and software such as operating systems and application programs. It also does not cover media prepared by the Bureau or Treasury intended for public dissemination.

b. **Mobile Media.** Any computer or storage media used to store information that is easily transportable. Examples include, but are not limited to, laptop computers, personal digital assistants, diskettes, CDs, tapes, USB or other flash storage devices. From a security exposure point of view, any of these media can hold significant amounts of sensitive information.

c. **Highly Sensitive Information.** Any Moderate or High impact Personally Identifiable Information (PII), information categorized as FIPS 199 High impact for confidentiality, or information identified by the System Owner or DAA as requiring additional protection measures.

3. REFERENCES.

- a. Treasury Chief Information Officer Memorandum, "Implementation of OMB M 06-16 for Non-National Security Systems," July 20, 2006.
- b. Treasury Chief Information Officer Memorandum, "Encryption of Mobile User Media," June 16, 2006.
- c. [National Institute of Standards and Technology \(NIST\) Federal Information Processing Standard Publication \(FIPS Pub\) 200, "Minimum Security Requirements for Federal Information and Information Systems,"](#) March 2006.
- d. [NIST Special Publication \(SP 800-53\), "Recommended Security Controls for Federal Information Systems,"](#) February 2005.

- e. [NIST FIPS PUB 140-2](#), “Security Requirements for Cryptographic Modules,” February 2005.
- f. [OMB Memorandum M-06-16](#), “Protection of Sensitive Agency Information,” June 23, 2006.
- g. [Circular 10-08.33](#), “Control and Accountability of Sensitive Digital Images,” July 2004.
- h. [NIST FIPS Pub 199](#), “Standards for Security Categorization of Federal Information and Information Systems,” February 2004.
- i. [BEP Manual 10-08.35](#), Chapter 2-2, “Protecting Sensitive and Personally Identifiable Information.”

4. RESPONSIBILITIES.

- a. Users shall:
 - (1) Ensure that computers, media, and communication methods they use comply with this policy; and
 - (2) Not circumvent or disable encryption.
- b. Office of IT Operations (OITO) shall ensure that equipment is deployed in compliance with this policy.
- c. System Owners and Designated Accrediting Authorities (DAAs) shall:
 - (1) Develop and submit encryption plans for systems that employ encryption; and
 - (2) Ensure that encryption is implemented in compliance with this policy.
- d. Office of Critical Infrastructure and IT Security (OCIITS) shall:
 - (1) Evaluate and approve encryption methods, plans and implementations to ensure compliance with Bureau and Treasury policy and Federal Information Processing Standards (FIPS) 140-2 and FIPS 200.
 - (2) Advise and assist System Owners and DAAs; and
 - (3) Implement and administer encryption systems and key recovery.

APPENDIX – A: GLOSSARY

1. TERMS AND DEFINITIONS.

Terms	Definition
Access Administrator	An individual authorized to perform limited system support functions associated with the creation and maintenance of user accounts on BEP information systems.
Availability	<p>“Ensuring timely and reliable access to and use of information...” [44 U.S.C., SEC. 3542]</p> <p>A loss of availability is the disruption of access to or use of information or an information system.</p>
Bureau System	An IT system (including telecommunications, networks, computers, and software programs) that is owned, leased, or operated by the Bureau or is operated by a contractor or another government agency on behalf of the Bureau.
Confidentiality	<p>“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542]</p> <p>A loss of confidentiality is the unauthorized disclosure of information.</p>
Database Administrator	An individual who has additional system rights, such as the ability to set configurations, make modifications and also perform functions such as supporting access controls on high-end database systems such as Microsoft SQL Server, Oracle, and Computer Associates IDMS
Denial of Service Attacks	A computer security incident event resulting in a loss of availability for critical resources such as e-mail servers, web servers, routers, gateways, or communication infrastructure.
Integrity	<p>“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” [44 U.S.C., Sec. 3542]</p> <p>A loss of integrity is the unauthorized modification or destruction of information.</p>
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.

MANUAL

No. 10-08.35

DATE October 6, 2005

Terms	Definition
Mechanism	The arrangement of individual components and the manner in which they perform to achieve the required security control.
Media Storage Facilities and Libraries	Environmentally and physically protected on-site or offsite facilities used to store system backup media and master copies of software.
Password	A sequence of characters used in conjunction with some type of user identification to authenticate the identity of the computer user.
Records Schedule	A document that describes agency records, establishes a period for document retention by the agency, and provides mandatory instructions for what to do with the documents when they are no longer needed for current government business.
Secure location	A physical and/or logical location that provides adequate controls based upon the sensitivity of the information being protected to ensure the confidentiality, integrity and availability of the information.
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.
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.
Storage Media (Media)	Objects used to magnetically, optically, or by other means store data. This includes internal, external, and removable storage devices (e.g., hard drives, tapes, diskettes, compact disks, and removable disk drives); master copies of software; and backup files, data, and programs.

MANUAL

No. 10-08.35

DATE October 6, 2005

Terms	Definition
System Administrator	An individual who has additional system rights, such as the ability to set configurations, make modifications and also perform functions such as supporting access controls on major systems such as the Internet and intranet, the mainframe, and the desktop operating environment.
System Owner	The program manager responsible for ensuring that an IT system meets the program area functional requirements and for approving changes to application requirements.
Unauthorized Disclosure	Exposure of information to persons, processes, or devices not authorized to receive it.
User	Any person or process authorized to access an IT system.
User Identification and Authentication	The means of verifying the identity of users before granting access to a requested resource.

APPENDIX B SUPERSESSION

The following circulars are superseded by this manual:

BEP Circular No. 10-08.8, "Certification and Accreditation of Information Systems," August 6, 2001;

BEP Circular No. 10-08.11, "Computer Password Policy," May 31, 2002;

BEP Circular No. 10-08.12, "Microcomputer Security Policy," January 25, 1989;

BEP Circular No. 10-08.14, "Management Information Systems Security Matrix," May 22, 1997;

BEP Circular No. 10-08.18, "Computer Access Control Policy," May 31, 2002;

BEP Circular No. 10-08.30, "Information Technology Security General Policy," October 18, 2004;

BEP Circular No. 70-04.4, "Bureau of Engraving and Printing Internet and Electronic Mail Policy," May 3, 1999;

BEP Circular No. 71-00.19, "ADP Security Resource Policy," July 8, 1985;