

DATE August 6, 2001

CERTIFICATION AND ACCREDITATION OF INFORMATION SYSTEMS

1. Purpose and Scope. This Circular establishes policy and defines the responsibilities of Bureau of Engraving and Printing (BEP or Bureau) officials for ensuring that information systems have been certified and accredited (or authorized) for operation by a management official. The objectives of certification and accreditation (C&A) 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 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 process identifies and evaluates system vulnerabilities, threats, and countermeasures in order to provide a clear understanding of the risks involved in operating a system. Accreditation is a process by which the Principal Accrediting Authority (PAA) understands and accepts the risks associated with system operation.

Systems must be re-accredited at least every three years. They must be re-accredited more often if there is a high risk or a high potential for harm from system compromise. Re-accreditation must also occur prior to implementation of significant changes in processing.

The certification and accreditation (C&A) process is central to many other information technology (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, and capital and operational planning. This Circular applies to all IT systems or processes, and to operational or planned manufacturing, security, support or administrative equipment which utilizes information processing technologies.

2. References.

Treasury Directive TD P 71-10, "Treasury Security Manual," August 23, 1999.
OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources" (Rev), November 2000.

OMB Memorandum M-01-08, "Guidance on Implementing the Government Information Security Reform Act," January 16, 2001.

DATE August 6, 2001

PL 104-106, Division E, Information Technology Management Reform Act of 1996, "Clinger-Cohen Act."

PL 104-13, Paperwork Reduction Act of 1995.

Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection."

PL 106-398, FY2001 Defense Authorization Act; Title X, Subtitle G, "Government Information Security Reform."

PL 100-235, The Computer Security Act of 1987.

Federal Information Processing Standards (FIPS) Publication 102, "Guidelines for Computer Certification and Accreditation," September 1983.

NIST Special Publication 800-XX (Draft), "Self-Assessment Guide for Information Technology Systems," March 9, 2001.

NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.

NIST Special Publication 800-30 (Draft), "Risk Management Guide – Computer Security," June 2001.

"Information Technology Security Assessment Framework," November 2000, Federal CIO Council.

3. Supersession.

Bureau Circular No. 10-08.8, "Certification of Automated Information System Applications and Facilities," dated December 10, 1987, is superseded.

4. Definitions.

a. Information Technology (IT) – 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. This includes computers, ancillary equipment, software, firmware, and related procedures, services (including support services) and resources.

b. Certification – the technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This is a technical process performed by technical security personnel.

c. Accreditation – the authorization and approval which is granted to a system or network to process data. The decision to accredit a system is made on the basis of the certification of that system by technical personnel. Accreditation is the granting of the authority to process by the Principal Accrediting Authority (PAA). By granting this authority, the PAA explicitly accepts the risks associated with system operation.

d. Interim Authority to Operate (IAO) – the authorization for a system to process data, pending final certification and accreditation (C&A). The PAA may grant an Interim Authority to Operate for cases in which a processing capability is needed, but

DATE August 6, 2001

certification has not been completed. The IAO is given with an understanding and acceptance of the security risks resulting from this operation.

e. Program official – also known as the management official or the system owner. This is the individual who has responsibility for the program, operations, information and assets which form part of or utilize information systems and processes. In most cases, this official will either be the PAA, share the duties of the PAA or appoint the PAA.

f. Principal Accrediting Authority (PAA) – This is the individual who authorizes processing on the IT system, based on information gained through the certification process. The Director, Bureau of Engraving and Printing, has overall responsibility for accreditation of all Bureau systems, and may delegate this responsibility to the Associate Directors. The Associate Directors may delegate this responsibility to an Office Chief or equivalent, but it may not be further delegated. In some cases, accrediting authority may be shared.

g. General support system – an interconnected set of information resources under the same management control which shares common functionality. Examples of BEP general support systems are local area networks (LAN) and the computer center.

h. Major application – information resources which satisfy a specific set of user requirements and which require special attention due to risk and magnitude of harm which could result from information loss, compromise, misuse, or unauthorized access. BEPMIS is an example of a system which incorporates several major applications.

5. Responsibilities.

a. The Chief Information Officer (CIO) is responsible for:

- (1) Developing and promulgating Bureau system security policies, rules, general procedures, and criteria;
- (2) Assisting program officials in identifying systems or processes which require accreditation and assisting in the development of supplementary studies, plans, and reviews on IT system security status;
- (3) Assisting in the development of Bureau wide performance plans for implementation of required security programs, including budgeting, staffing and training resources necessary to implement these programs;
- (4) Assisting program officials in the preparation of performance reviews as required by law or regulation. These reviews may be required as often as every year or as infrequently as every three years;
- (5) Incorporating summary information on system security plans in the Bureau's Strategic Plan, annual budget submissions, and capital planning documents;
- (6) Developing the guidelines and requirements for the certification and accreditation (C&A) process and providing technical assistance for certification; and

DATE August 6, 2001

(7) Carrying out the responsibilities of Program Official for Bureau general support systems, including accrediting those systems and completing periodic performance reviews.

b. Program Officials are responsible for:

(1) Ensuring that information systems and processes are identified and registered with the Information Technology Security Division (ITSD) and that the criticality of the system and the sensitivity of the information processed are defined. The most critical designations are for major applications and general support systems;

(2) Appointing a principal accrediting authority for major applications and general support systems;

(3) Ensuring that systems are certified prior to authorizing initial processing (interim approval or accreditation), implementation, or deployment. For systems that are operational but have not been accredited, the program official will ensure that the C&A process is initiated as quickly as possible; and

(4) Ensuring that information security training is provided to employees.

c. The Principal Accrediting Authority is responsible for:

(1) Authorizing a system to begin processing, based on an evaluation and acceptance of the risk of operations. This authorization shall either be an Interim Approval to Operate (pending certification) or Accreditation (with certification);

(2) Performing annual program reviews of major applications or general support systems. Performing reviews every three years of other systems and processes; and

(3) Providing results of certification and performance reviews to the CIO for compilation and reporting through the annual budget process.

d. The Information Technology Security Division (ITSD) is responsible for:

(1) Developing and recommending standards and standard methodologies for certifying IT systems, resources or processes. This includes guidelines for security plans, certification testing and documentation, and Interconnection Security Agreements;

(2) Reviewing capital and other IT resource procurements and system development project documents to assure adequacy of security and contingency planning;

(3) Providing guidance and assistance in general support system or major application performance reviews;

(4) Developing Bureau wide IT security training and assisting in the development of specific requirements and curricula for training in Bureau Offices, Sections, or other functional areas;

DATE August 6, 2001

(5) Providing risk and vulnerability analyses, preparing Bureau-wide IT security plans, and providing assistance on evaluation and recommendation of technical security controls;

(6) Auditing and testing security features for Bureau information systems, processes, resources, hardware, software, equipment, and procedures; and

(7) Maintaining the official BEP repository of all certification, accreditation, and performance review documentation.

6. Elements of the Certification Process. The requirements for certification of either a general support system or a major application are similar.

a. Responsibility for security must be assigned. Overall Bureau IT security responsibility rests with the IT Security Division. As required by law, the CIO has also appointed an IT Security Advocate with responsibility for program review and coordination across the Bureau. In addition, Program Officials must designate a Principal Accrediting Authority and must coordinate security and contingency planning for those systems for which they are responsible.

b. A system security plan must be prepared. This document will follow guidelines provided by the National Institute of Standards and Technology (NIST) and must consider the connectivity of the system with other networks/systems or, in the case of applications, must consider the security requirements of all systems within which the application operates.

c. When the application is connected to or resident on other Bureau systems, or the general support system is connected to other systems, the PAA for those other systems must also sign off on the security plan. When there is connectivity with systems at non-BEP organizations, an Interconnection Security Agreement must be prepared and signed by Program Officials of both organizations. This Agreement will document and formally authorize these interconnection arrangements and will specify any details that may be required to ensure overall security safeguards for both systems.

d. A set of rules of use must be prepared. These are rules of behavior which concern the use of the system/application and the acceptable level of risk. The rules must delineate responsibilities and expected behaviors of those with system access or who use the application. They also should provide a list of consequences for failure to comply.

e. Training must be provided to all administrators and users of the system or application. This training will include their security responsibilities, the rules of use, rules on system access and permitted activities, and information on where to get security and other assistance. Training plans must also include provisions for periodic refresher training.

DATE August 6, 2001

f. A personnel security plan will be prepared which will identify required clearances for various system/application access levels, particularly for individuals who are authorized to bypass technical and operational security controls. There should be a discussion of system risks, responsibilities of individuals or job categories, and especially for sensitive applications, a clear separation of duties. In addition, this plan should provide methods of enforcement of the principle of least privilege and should provide controls to ensure individual accountability.

g. Provision must be made for disruption of operations, whether from outside or inside attacks, natural or man-made disasters. The certification should also document an incident response capability which will provide help to users when an incident occurs and will also ensure that information on common vulnerabilities and threats will be identified and shared with other organizations. In addition, contingency planning for system disruptions must be completed. This includes developing alternative capabilities, resources, or strategies and periodically testing them.

h. There must be an evaluation of technical security controls. This will ensure that appropriate technical controls are specified, designed, tested, and accepted in the system deployment or application.

i. To maintain accreditation under current law and regulation, there must be periodic assessments of the system security. These can be performed by the Program Official, another Government agency or can be contracted out. The period for review is either every year or every three years depending on the criticality of the system and the risk of damage or compromise. Major applications and general support systems must be reviewed every year.

7. Office of Primary Responsibility. Associate Director (CIO).

<SIGNED>

Ronald W. Falter
Associate Director
(CIO)

Distribution: Office Chiefs
CIO Directorate