

DATE May 21, 2001

IT CONFIGURATION CONTROL BOARD

1. PURPOSE AND SCOPE. This Circular 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.

DATE May 21, 2001

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

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 nonintrusive 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
- (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.

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

CIRCULAR

DATE May 21, 2001

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.

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

<SIGNED>

Ronald W. Falter
Associate Director (Chief Information Officer)

DISTRIBUTION - D