

DATE July 30, 1987

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.

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.

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 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.

DATE July 30, 1987

7. 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.

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

8. OFFICE OF PRIMARY RESPONSIBILITY. Office of Security.**<SIGNED>**

Robert J. Leuver
Director

Distribution - B