R-14

IBSEC-CSS-R-14
17 October 1973

COMPUTER SECURITY SUBCOMMITTEE

OF THE

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

MEMORANDUM FOR: Chairman, USIB Security Committee

SUBJECT : Sanitized Version of DCID No. 1/16 for USIB Contractors and Non-USIB Government Agencies

1. Earlier this year the Computer Security Subcommittee identified a requirement for disseminating the substance of DCID No. 1/16, "Security of Compartmented Computer Operations" outside the Intelligence Community where sensitive compartmented information is processed by computer. This requirement was acute at certain USIB contractor installations and in non-USIB Government agencies involved in the computer processing of compartmented material.

2. In response to this requirement the Subcommittee has developed the attached "Intelligence Community Policy - Security of Compartmented Computer Operations" as a sanitized version of DCID No. 1/16. This sanitization will permit dissemination of Community security requirements in this area to other agencies and to contractors where dissemination of the Directive itself is constrained due to the controls on DCID formatted material.

25X1

3. It is proposed that following Security Committee approval of the attachment and USIB consideration, if necessary, the attached policy paper may be distributed as required on a selective basis through normal compartmented control officers but without compartmented controls.

[redacted] 25X1

Chairman
Computer Security Subcommittee

Att

Distribution:
Orig & 1 - Addressee
1 - ISSG File: Custodian Files, USIB/CSS, Reports to SECOM
1 - ISSG Chrono
OS/P&M/ISSG/[redacted]fm (17 October 1973) 25X1

INTELLIGENCE COMMUNITY POLICY

SECURITY OF COMPARTMENTED COMPUTER OPERATIONS

(Effective 7 January 1971)

Applicability

In order to insure uniform protection of sensitive compartmented information* when such information is stored and/or processed in remotely accessed resource-sharing computer systems, minimum security requirements are established for the utilization of such computer systems in a compartmented mode of operation. These requirements are equally applicable within the Intelligence Community, and to contractors and other government systems handling sensitive compartmented information.

---

* The term "sensitive compartmented information" as used in this paper is intended to include all information and material bearing special Community controls indicating restricted handling within Community intelligence collection programs and their end products for which Community systems of compartmentation are formally established. The term does not include Restricted Data as defined in Section 11, Atomic Energy Act of 1954, as amended, nor does anything in this paper supersede or augment requirements on the control, use and dissemination of Restricted Data or Formerly Restricted Data.

25X1

Purpose

1. This paper prescribes the basic policy concerning the security aspects of using remotely accessed resource-sharing computer systems in a compartmented mode of operation. It specifies the conditions and prescribes minimum security requirements under which such systems may be operated. Responsibilities for the security analysis, testing and evaluation as well as for the accreditation of such systems are prescribed in applicable national directives.

2. The computer processing of sensitive compartmented information in some instances may constitute a threat of such proportion that it can only be offset by more stringent security arrangements than those specified in this paper; conversely, instances may occur when full compliance with the requirements of this paper is impossible. Such instances shall be referred to the cognizant approving authority in sufficient time to allow their consideration to any request for deviation from this policy paper.

Definitions

3. Remotely Accessed Resource-Sharing Computer System: A system which includes one or more central processing units, peripheral devices, remote terminals, communications equip-

ment and interconnecting links, which allocates its resources to more than one user, and which can be entered from terminals located outside the computer center.

4. Compartmented Mode of Operation: Utilization of a remotely accessed resource-sharing computer system for the concurrent processing and/or storage (a) of two or more types of sensitive compartmented information or (b) of any type of sensitive compartmented information with other than sensitive compartmented information. System access is afforded personnel holding TOP SECRET clearances but not necessarily all the sensitive compartmented information access approvals involved.

5. Controlled Top Secret Environment: Total system protection and control from a physical, technical and personnel security standpoint in accordance with the minimum requirements for the processing and handling of Top Secret material.

6. System Accreditation: Approval by cognizant sensitive compartmented information authority for a remotely accessed resource-sharing computer system to be operated in a compartmented mode within a controlled Top Secret environment as defined above.

Policy

7. Remotely accessed resource-sharing computer systems shall not be utilized for the concurrent processing and/or storage of two or more types of sensitive compartmented information, or of any type of sensitive compartmented information with other than sensitive compartmented information unless the total system is secured to the highest classification level for all types of sensitive compartmented information processed or stored therein, except as provided in paragraph 8 below.

8. Such systems may be operated in a compartmented mode if maintained in a controlled Top Secret environment as defined herein and provided that at least the minimum requirements identified in this paper are implemented and made a part of system operation.

9. Judicious implementation of the basic requirements set forth below dictates a need to test and evaluate their effectiveness when applied to a specific system as a basis for accreditation of that system for compartmented computer operations. Further, such accreditation shall be subject to periodic review of the security of system operation.

Minimum Requirements

10. All remotely accessed resource-sharing computer systems accredited for compartmented operation shall contain the following security capabilities as an absolute minimum:

a. Information System Security Officer (ISSO): A security officer shall be appointed for each computer system operating in a compartmented mode. This ISSO is specifically responsible for ensuring continued application of the requirements set forth in this paper, for reporting security deficiencies in system operation to the cognizant approving authority, for reporting security deficiencies in system operation to such authority, and for monitoring any changes in system operation as they may affect the security status of the total system.

b. Personnel Security and System Access Control Measures: Unescorted access to the computer center shall be

limited to personnel with a predetermined need and holding Top Secret clearances as well as access approvals for those types of sensitive compartmented information stored and/or processed by the system. Other personnel requiring access to the computer center area shall be properly escorted. A record shall be maintained of personnel who have access to the computer center. Access to and use of remote terminals shall be limited to designated personnel holding Top Secret clearances and access approvals for all compartmented information designated for input/output at that terminal. Administrative approvals, not requiring substantive briefings, may be granted by cognizant authority for access to the computer center and/or remote terminals when access to all sensitive compartmented information stored and/or processed in the system is not operationally required.

c. Physical Security Protection: Physical security requirements for the computer center

and remote terminal areas shall be determined by the classification and types of sensitive compartmented information involved. The physical security of the computer center area shall be based on prescribed requirements, as implemented by the cognizant sensitive compartmented information authority for the most demanding sensitive compartmented information stored or processed by the system. Each remote terminal shall be protected in accordance with the requirements for Top Secret information and for all sensitive compartmented information designated for input/output at that terminal. Those terminals designated for the input/output of sensitive compartmented information shall be in areas approved at least as temporary work areas for the sensitive compartmented information involved while operating in a compartmented mode.

d. Communications Links: The communications links between all components of the system shall be secured in a manner appropriate for the transmission of Top Secret sensitive compartmented information.

e. Emanations Security Aspects: The vulnerability of system operations to exploitation through compromising emanations shall be considered in the process of system accreditation. Evaluation of the risks associated with the computer center and the remote terminal areas as well as related control measures shall be accomplished by the cognizant approving authority.

f. Software/Hardware Controls: Compartmentation of information stored and/or processed in the system shall be based on the features outlined below. Measures shall be implemented to provide special controls over access to and/or modification of these features.

(1) Security Labels: Security classification and other required control labels shall be identified with the information and programs in the system to ensure appropriate labeling of output.

(2) User Identification/Authentication: System operation shall include a mechanism that identifies and authenticates personnel accessing it remotely. This mechanism shall consist of software and/or hardware devices, manual control procedures at terminal sites, and other appropriate measures designed to validate the identity and access authority of system users.

(3) Memory Protection: Hardware and software control shall be exercised by the system over the addresses to which a user program has access.

(4) Separation of User/Execution Modes of Operation: The user and execution modes of system operation shall be separated so that a program operating in user mode is prevented from performing unauthorized execution functions. Controls shall be implemented to maintain continued separation of these modes.

(5) Residue Clean Out: Measures shall be implemented to ensure that memory residue from terminated user programs is made inaccessible to unauthorized users.

(6) Access Control: Effective controls shall be implemented to limit user and terminal access to authorized information and programs as well as to control read and/or write capability.

(7) Audit Trail Capability: Each system shall produce in a secure manner an audit trail containing sufficient information to permit a regular security review of system activity.

g. Individual Security Responsibilities: All users of the system shall be briefed on the need for exercising sound security practices in protecting the information stored and processed by the system, including all output. Users shall be informed that the system is operating in a compartmented security mode and that the receipt of any information not specifically requested shall be reported immediately to the ISSO.