DCID No. 1/16
(New Series)

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/16

SECURITY OF COMPARTMENTED COMPUTER OPERATIONS

(Effective 7 January 1971)

Pursuant to the provisions of NSCID No. 1 (New Series, revised 4 March 1964), paragraph 2, subparagraph a. (5) and in order to ensure uniform protection of sensitive compartmented information [1] 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 USIB Community, and to contractor and non-USIB government systems handling sensitive compartmented information.

The diversity and complexity of such computer systems now in place in the Community and those already designed for future placement may not provide for compliance with the requirements of this directive in their entirety. Recognizing both the validity of the requirements and the difficulty involved in their application to currently installed and already designed systems, the extent to which the requirements of this directive are applied to such systems is left to the determination of each USIB member in view of his ultimate responsibility for the security of sensitive compartmented information.

Nothing in this directive shall supersede or augment the requirements on the control, use and dissemination of Restricted Data or Formerly Restricted Data made by or under existing statutes, directives and Presidential policy. Whenever Restricted Data or Formerly Restricted Data is involved in any compartmented operation of remotely accessed resource-sharing computer systems, appropriate personnel and physical security procedures and controls shall be implemented. (See Section 11, 141, 142.e., 144.a., b., c. and d., 143, and 145, of the Atomic Energy Act of 1954, as amended.)

[1] The term "sensitive compartmented information" as used in this directive is identical with its use in DCID No. 1/14 (New Series, effective 1 July 1968). It 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.

Purpose

1. This directive prescribes the basic policy concerning the security aspects of utilizing 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. Further it assigns the responsibility for the security analysis, test, and evaluation as well as for the accreditation of such systems to individual USIB members.

Definitions

2. *Remotely Accessed Resource-Sharing Computer System:* A system which includes one or more central processing units, peripheral devices, remote terminals, communications equipment and interconnecting links, which allocates its resources to more than one user, and which can be entered from terminals located outside the computer center.

3. *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.

4. *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.

5. *System Accreditation:* Approval by USIB member 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

6. 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 and for all types of sensitive compartmented information processed or stored therein, except as provided for below:

a. 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 directive are implemented and made a part of system operation;

b. Upon the determination by a USIB member in unique situations that immediate implementation of the minimum requirements will significantly impair his mission effectiveness, he may temporarily exempt specific systems operating in a compartmented mode from compliance; however, every USIB member authorizing such an exemption must strive for the earliest feasible attainment of the minimum requirements identified in this directive.

7. 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. Each USIB member is responsible for conducting such testing and evaluation and has the authority to accredit systems within the purview of his responsibility for compartmented operation based on their meeting the requirements specified in this directive. Such accreditation shall be subject to periodic review of the security of system operation.

Minimum Requirements

8. 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):* Each USIB member shall appoint a security officer for each computer system operating in a compartmented mode within the purview of his responsibility. The ISSO is specifically responsible for ensuring continued application of the requirements set forth in this directive, for reporting security deficiencies in system operation to the USIB member, 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 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 each USIB member 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 within the appropriate agency.

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/Executive Modes of Operation:* The user and executive modes of system operation shall be separated so that a program operating in user mode is prevented from performing

unauthorized executive 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.

Effective Date

9. This directive declares the policy of the United States Intelligence Board concerning minimum security requirements for the compartmented operation of remotely accessed resource-sharing computer systems in a controlled Top Secret environment. This policy shall become effective as soon as practicable after approval of this directive but in no case later than 1 February 1971. Existing directives,[2] regulations, agreements and such other references governing access to sensitive compartmented information as defined herein shall be revised accordingly. This Directive shall be reviewed within three years from date of issuance and modified in the light of developments in computer security.

Richard Helms
Director of Central Intelligence

[2] These include pertinent portions of Annex E of DCID No. 6/3.

QUESTION 1

Compartmented Mode (as defined in 16 Mar 76 DCID 1/16)

The system may process two or more types of classified intelligence information, one of which must include sensitive compartmented information, where system access is secured to the TOP SECRET level, but not necessarily including access to all sensitive compartmented information being processed.

Compartmented Mode (Expanded)

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 types of sensitive compartmented information with other than sensitive compartmented information. System access is afforded personnel holding, at a minimum, final SECRET clearance, but not necessarily all of the sensitive compartmented access approvals for the highest level SCI contained within the system. Personnel will be able to access any information for which they hold valid clearances and a need-to-know requirement.

QUESTION 2

Proposed Definition of Sensitive Compartmented Information (SCI)

Sensitive compartmented information, which is defined as all information and material bearing special Intelligence Community controls indicating restricted handling within Community Intelligence collection program and their end products for which Community systems of compartmentation are formally established.

Definition of SCI as in DCID 1/14

Sensitive compartmented information includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include Restricted Data as defined in Section 11, Public Law 585, Atomic Energy Act of 1954, as amended.

QUESTION 3

Use of Computers for communications-related functions in networks.

Problem: "Ill-defined" interface area associated with the interconnection of major ADP equipment and a major communications systems.