DCI Director of
Central
Intelligence

Confidential

COMPUTER SECURITY MANUAL

Prepared for
The Director of
Central Intelligence
by the
Security
Committee

Confidential

4 January 1983

COMPUTER SECURITY MANUAL

(Attachment to "Security Policy on Intelligence Information in Automated Systems and Networks")

CL BY DCI
DECL OADR

Table of Contents

Page

CHAPTER I

CHAPTER II

CHAPTER III

CHAPTER I

Introduction

I.1. Director of Central Intelligence security policy requires Intelligence Community agencies and all other United States Government departments and agencies processing and/or storing intelligence information in ADP systems and networks to establish and maintain a formal ADP security program to ensure adequate protection of intelligence information. This Manual is promulgated to establish the minimum security requirements for the allowed operating modes of an ADP system or network as defined in Chapters II and III. ADP security programs shall be based on these programs.

I.2. All ADP systems and networks not otherwise exempted pursuant to DCI Security Policy on Intelligence Information in Automated Systems and Networks, which process and/or store intelligence information, must meet the requirements prescribed in Chapters II and III of this Manual. Accreditation, as prescribed herein, is required for the operation of each ADP system and network. The accreditation is contingent upon the results of a recurring review, testing, and favorable evaluation of employed security features. These security features shall include hardware/software features, operating procedures, accountability procedures, access controls, management constraints, physical structures, and appropriate communications security (COMSEC) measures to provide minimum security protection for intelligence information processed and/or stored by the ADP system or network.

I.3. An Information System Security Officer (ISSO) shall be appointed for each ADP system processing and/or storing intelligence information. An ISSO may serve for more than one system. Duties and responsibilities of the ISSO are specified in Chapters II and III.

I.4. The SOIC or his designee responsible for the management of an ADP network shall appoint a Network Security Officer (NSO). Duties and responsibilities of the NSO are specified in Chapter III of this Manual.

CHAPTER II

Modes of Operation and Minimum Security Requirements for Processing and/or Storing Intelligence Information in ADP Systems

Three modes of operation of an ADP system are allowed for the processing and/or storing of intelligence information. They are: (a) Dedicated Mode; (b) System High Mode; and (c) Compartmented Mode. The minimum security requirements for each mode of operation are contained in this Chapter. Chapter III identifies the requirements for ADP networks which are formed by the interconnection of ADP systems operating in any of these allowed modes.

II.1. General security requirements for ADP systems processing and/or storing intelligence information.

II.1.a. ***Information System Security Officer (ISSO).*** The ISSO is specifically responsible for ensuring continued compliance with the requirements set forth in this Manual, providing system accreditation statements, reporting major security deficiencies in system operation to the SOIC or his designee, and monitoring any changes in system operation that may affect the security status of the total system.

II.1.b. ***Communications Links.*** The communications links between all components of the ADP system shall be secured in accordance with appropriate directives for the highest classification of information designated for transmission.

II.1.c. ***Emanations Security Aspects.*** The vulnerability of system operations to exploitation through compromising emanations shall be determined in the process of system accreditation. Evaluation of the risks associated with the central computer facility and the remote terminal areas and application of control measures shall be in accordance with appropriate directives.

II.1.d. ***Individual Security Responsibilities.*** All users of the system shall be briefed on the need for exercising sound security practices in protecting the information processed and/or stored in the system, including all input and output. Users shall be informed of the security mode in which the system is operating and that the receipt of any information not specifically requested shall be reported immediately to the ISSO, or his designee.

II.1.e. ***Administrative Approvals.*** Administrative approvals (not requiring substantive briefings) may be used to grant persons access to the central computer facility and remote terminal areas when such persons do not require access to the intelligence information processed and/or stored in the system.

II.2. Modes of Operation and Minimum Security Requirements.

II.2.a. ***Dedicated Mode.***

II.2.a(1) Intelligence information may be processed and/or stored in an ADP system operating in the Dedicated Mode; that is, the system is specifically and exclusively dedicated to, and controlled for, the processing of that one particular type of intelligence information, either for full-time operation or for a specified period of time.

II.2.a(2) ***Accreditation Process.*** The SOIC or his designee can accredit an ADP system operating in the Dedicated Mode after receiving written assurance from the computer system manager and the responsible ISSO that the ADP system meets the minimum security requirements for this mode as outlined below.

II.2.a(3) ***Personnel Security.*** All unescorted personnel requiring access to the central computer facility or any remote terminal shall have a valid security clearance and formal access approval for the one particular type of intelligence information contained within the ADP system.

II.2.a(4) ***Physical Security.*** The central computer facility and any remote terminals connected to it shall be secured in a manner commensurate with the classification and control caveats of the one type of intelligence information contained in the system.

II.2.a(5) ***System.*** All peripheral devices not dedicated for use in the processing of the specific type of intelligence information shall be disconnected from the system in an approved manner. A controlled copy of the operating system shall be used to initialize an ADP system for processing TOP SECRET intelligence information or Sensitive Compartmented Information (SCI).

II.2.a(6) ***Termination of Dedicated Mode Operation.*** On changing from Dedicated Mode operation, all intelligence information and the media used in its processing and/or storing shall be secured or sanitized in an approved manner. An ADP system which has operated in the Dedicated Mode may then be returned to its original or different mode, as appropriate.

II.2.b. *System High Mode*

II.2.b.(1) Intelligence information may be processed and/or stored in an ADP system operating in the System High Mode; that is, the system is operating with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored.

II.2.b(2) ***Accreditation Process.*** The SOIC or his designee can accredit an ADP system operating in the System High Mode after receiving written assurance from the computer system manager and the responsible ISSO that the ADP system meets the minimum security requirements for this mode as outlined below.

II.2.b(3) ***Personnel Security.*** All unescorted personnel requiring access to the central computer facility or any remote terminal shall have a valid security clearance and formal access approvals for all data processed and/or stored in the ADP system. Unescorted personnel do not automatically have authorization to see or use all of the data processed and/or stored in the system. Need-to-know criteria shall apply.

II.2.b(4) ***Physical Security.*** The central computer and remote terminal facilities shall be secured in a manner commensurate with the highest classification and sensitivity of information contained in the system.

II.2.b(5) ***System.***

II.2.b(5)(a) All terminals and peripheral devices not designated for use in the current System High Mode of operation shall be disconnected from the system in an approved manner.

II.2.b(5)(b) Authentication of remote terminals and personnel shall be performed by the system. System controls shall be in conformity with those required for the protection of the most sensitive information being processed and/or stored in the system. System controls shall consist of software, hardware, and/or other appropriate measures designed to validate the identity and file access authority of the system users.

II.2.b(5)(c) Security classification and other required control caveats shall be identified with the information and programs in the system, and appropriate labeling of the output shall be ensured.

II.2.b(6) ***Audit Trails.*** Each system shall produce, in a secure manner, an audit trail containing sufficient information to permit the ISSO to perform a regular security review of the system activity.

II.2.b(7) ***Termination of System High Mode Operation.*** On changing from System High Mode operation, all intelligence information and the media used in its processing and/or storage shall be secured or sanitized in an approved manner. An ADP system which has operated in the System High Mode may then be returned to its original or different mode, as appropriate.

II.2.c. ***Compartmented Mode.***

II.2.c(1) SCI may be processed and/or stored in an ADP system operating in the Compartmented Mode; that is, the system is processing two or more types of SCI, or any one type of SCI with other than SCI, and system access is secured to at least the TOP SECRET level, but all system users need not necessarily be formally authorized access to all types of SCI being processed and/or stored in the system.

II.2.c(2) ***Accreditation Process.***

II.2.c(2)(a) Only the SOIC can accredit an ADP system for operation in the Compartmented Mode.

II.2.c(2)(b) The accreditation will be based upon the results of a security analysis, test, and evaluation to assure that the ADP system meets the minimum security requirements for this mode as outlined below. The ISSO will ensure that the security analysis, test, and evaluation is carried out and the results reported along with his recommendations to the SOIC.

II.2.c(3) ***Personnel Security.***

II.2.c(3)(a) All unescorted personnel requiring access to the central computer facility shall have a valid TOP SECRET clearance[1] and formal access approvals for all data processed and/or stored in the ADP system. Need-to-know criteria shall apply.

[1] Such clearance must have been granted based on the provisions of DCID 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," or successor policy guidance.

II.2.c(3)(b) All unescorted personnel requiring access to any remote terminal facility shall have a valid TOP SECRET clearance[2] and formal access approvals for all data designated for input/output at that terminal facility. Need-to-know criteria shall apply.

II.2.c(4) ***Physical Security.***

II.2.c(4)(a) The central computer facility shall be secured in a manner commensurate with the handling of TOP SECRET material and the most sensitive intelligence information contained in the facility.

II.2.c(4)(b) Each remote terminal area will be secured in a manner commensurate with the handling of TOP SECRET material and the most sensitive intelligence information, designated for input/output at that terminal facility.

II.2.c(5) ***System.*** The ADP system through a combination of hardware and software capabilities shall provide the requisite protection for intelligence information processed and/or stored by it. Systems not presently equipped with the required hardware/software security capabilities prescribed below must compensate for the lack thereof by the implementation of other security measures and procedures which afford the same degree of protection.

II.2.c(5)(a) All terminal and peripheral devices not designated for use in the current Compartmented Mode of operation shall be disconnected from the system in an approved manner.

II.2.c(5)(b) Authentication of remote terminals and personnel shall be performed by the system. System controls shall be in conformity with those required for the protection of the most sensitive information being processed and/or stored in the system. System controls shall consist of software, hardware, and/or other appropriate measures designed to validate the identity and file access authority of the system users.

II.2.c(5)(c) Security classification and other required control caveats shall be identified with the information and programs in the system and appropriate labeling of the output shall be ensured.

II.2.c(5)(d) ***Memory Access.*** System hardware/software features shall exercise control over the memory locations to which a user program has access.

II.2.c(5)(e) ***Privileged Instructions.*** The system shall utilize a special class or subset of instructions to perform and control all input/output operations and changes to memory boundaries, execution state variables, data elements or tables, and files of the operating system. The operating system alone shall execute these instructions or provide access to them.

II.2.c(5)(f) ***Verified Response.*** Machine instructions/operation codes, both privileged and user, with all possible tags or modifiers, whether legal or not, shall be designed and tested to produce results in a predefined set of responses by the computer hardware/firmware.

II.2.c(5)(g) ***Read, Write, and Execute Privileges.*** The system shall enforce the read, write, and execute privileges of a user with respect to any given file.

II.2.c(5)(h) ***Separation of User/Privileged Modes of Operation.*** The user and privileged modes of system operation shall be separated so that a program operating in user mode is prevented from unauthorized utilization of privileged functions. Controls shall be implemented to maintain continued separation of these modes.

[2] Ibid.

II.2.c(5)(i) ***Residue ClearOut.*** Measures shall be implemented to ensure that residue from terminated user programs are cleared before memory and on-line storage devices' locations are released by the system for use by another user program.

II.2.c(5)(j) ***Over-the-Counter Access Control.*** Effective controls shall be implemented to limit over-the-counter (batch) users to authorized access to information and programs, as well as to control read and/or write access authorizations.

II.2.c(6) ***Audit Trails.*** Each system shall produce, in a secure manner, an audit trail containing sufficient information to permit the ISSO to perform a regular security review of system activity.

II.2.c(7) ***Termination of Compartmented Mode Operation.*** On changing from Compartmented Mode operation, all intelligence information and the media used in its processing and/ or storing shall be secured or sanitized in an approved manner. An ADP system which has operated in the Compartmented Mode may then be returned to its original or different mode, as appropriate.

25X1

Next 4 Page(s) In Document Exempt

GLOSSARY

The following definitions apply to the terms used in the Computer Security Manual.

Access. The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system or network.

Accreditation. A formal declaration by the responsible SOIC, or his designee, as appropriate, that the ADP system or network provides an acceptable level of protection for processing and/or storing intelligence information. An accreditation should state the operating mode and other parameters peculiar to the ADP system or network being accredited.

ADP System. The central computer facility and any remote processors, terminals, or other input/output/storage devices connected to it by communications links. Generally, all of the components of an ADP system will be under the authority of one SOIC or his designee.

Authentication. A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified.

Central Computer Facility. One or more computers with their peripherals and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links.

Escort. Duly designated personnel who have appropriate clearances and access approvals for the material contained in the ADP system and are sufficiently knowledgeable to understand the security implications and to control the activities and access of the individual being escorted.

Front-end Processor. A computer associated with a host computer that performs preprocessing functions. It may perform line control, message handling, code conversion, error control, data control, data management, terminal handling, etc. (See Manual, Chapter III, Figure 1.)

Operating System (O/S). An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform input/output, accounting, resource allocation, compilation, storage assignment tasks, and other system-related functions.

Processing and/or Storing. All inclusive term used to include in addition to processing and storing such functions as manipulating, deleting, modifying, editing, outputting, etc.

Sensitive Compartmented Information (SCI). All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.