DIRECTOR OF CENTRAL INTELLIGENCE

COMPUTER SECURITY REGULATION

(Attachment to DCID 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks")

COMPUTER SECURITY REGULATION

INDEX

CHAPTER I

Introduction

I.1. Director of Central Intelligence Directive No. 1/16 (DCID 1/16) requires National Foreign Intelligence Board (NFIB) member 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 Regulation 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 the provisions of this Regulation and DCID 1/16.

I.2. All ADP systems and networks, not exempted in DCID 1/16, processing and/or storing intelligence information must meet the requirements prescribed in Chapters II and III of this Regulation. 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 NFIB member 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 Regulation.

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 Systems Security Officer.* Each NFIB member or his designee shall provide for the appointment of an Information System Security Officer (ISSO). It is desirable for an ISSO to be responsible for only one system; however, he may be responsible for more than one. The ISSO is specifically responsible for ensuring continued compliance with the requirements set forth in this Regulation, providing system accreditation statements, reporting major security deficiencies in system operation to the NFIB member 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 NFIB member 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).[1]

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 NFIB member 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.

[1] Definition as set forth in DCID 1/16.

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 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 NFIB member can accredit an ADP system for operating 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 NFIB member.

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 [2] and formal access approvals for all data processed and/or stored in the ADP system. Need-to-know criteria shall apply.

II.2.c(3)(b) All unescorted personnel requiring access to any remote terminal facility shall have a valid TOP SECRET clearance [3] 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.

[2] Such clearance must have been granted based on investigative requirements of DCID 1/14.

[3] *Ibid.*

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, if any, 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 or 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.

II.2.c(5)(i) *Residue Clear-out.* 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.

CHAPTER III

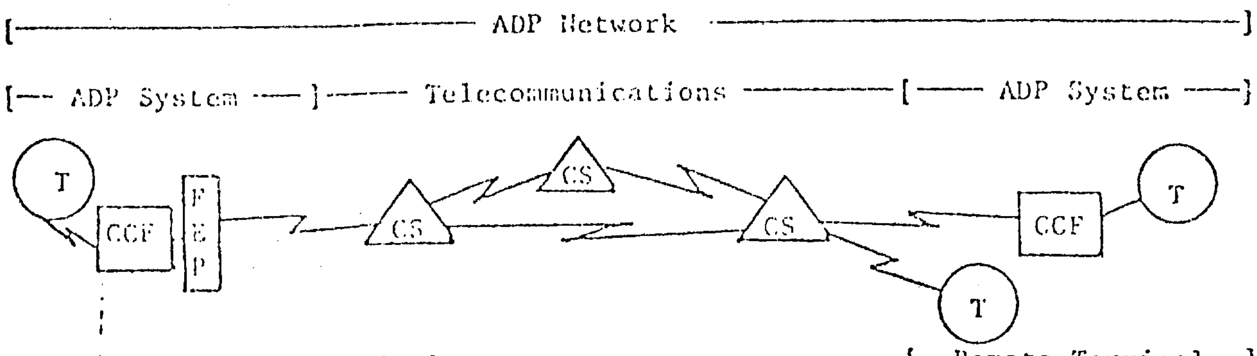
ADP Networks

III.1. *Definition*

III.1.a. For the purpose of this regulation and implementation of DCID 1/16, an ADP network is defined as the interconnection of two or more ADP systems that operate in any of the modes defined in Chapter II. The ADP network consists of the components (central computer facility, remote terminals, and interconnecting communications links) of the various ADP systems, front-end processors, and telecommunications. This Regulation shall not apply to the individual ADP systems, if any (e.g., CS in Figure 1), that make up the telecommunications; these are controlled by pertinent national policies and regulations.

III.1.b. There are numerous ways in which ADP systems operating in any of the modes defined in Chapter II can be interconnected to form an ADP network. However, most of these combinations will increase the minimum security requirements of the individual ADP systems since their original operating modes cannot be maintained when they become a part of a network. (For example, when two Dedicated Mode ADP systems interconnect, they can continue to operate in the Dedicated Mode only if both ADP systems process the same classification and type of intelligence information. If this is not the case, their interconnection would require both systems to meet the requirements of operating in the System High Mode (Network High) or the Compartmented Mode, depending on the classification and type of intelligence information to which each ADP system was originally dedicated.) Therefore, each proposed configuration of ADP systems must be assessed to determine the appropriate mode of operation (Dedicated, Network High, or Compartmented) for the resultant network. Each ADP system in the network must be accredited for operation in the new mode when a change of operating mode is required.

(FIGURE 1)



T	-	Remote Terminal
CCF	-	Central Computer Facility
FEP	-	Front End Processor
CS	-	Communications Computer or Switch (e.g., AUTODIN)

III.1.c. Some examples of possible configurations of ADP systems and the resulting ADP network mode of operation are shown in Table 1 below.

III.2. *Responsibilities for ADP Network Security Administration*

III.2.a. *Responsible Authorities.* The authority, organization, or manager responsible for the overall operation and control of the ADP network shall ensure that each ADP system which is a part of the network adheres to the security required by the current network configuration (see III.1.b. and c. above). The security measures shall be agreed to in writing by the ADP network authority and the ADP system authority and implemented before an ADP system is connected to the network. However, each NFIB member is the responsible security authority for his ADP system participating in the network.

III.2.b. *Remote Station Authority.* Security requirements for remote terminals and peripheral devices of an ADP network shall be prescribed by the authority responsible for the security of the ADP network. In some cases, this may be a different NFIB member or designee than the terminal or device user.

III.2.c. *Exceptions.* When an ADP system becomes a part of an existing ADP network, approval of any temporary exceptions to the network security requirements will require the written concurrence of the ADP system authority and the ADP network authority. The ADP network authority will approve the temporary exception only with the consensus of all the network participants.

III.2.d. *Security Anomalies.* Each NFIB member or his designee is responsible for assuring that he is aware of any known system irregularities occurring within his ADP system. Any evidence indicating a possible violation of the security integrity or unexplainable phenomenon of the system shall be made known to the ISSO. The ISSO

Table 1

ADP System Mode(s)	ADP Network Mode
1. All systems are Dedicated to processing and/or storing the same type of intelligence information.	1. Dedicated
2. All systems are Dedicated [a] to same classification level but not same type of intelligence information, and not SCI.	2. Network High [b]
3. Some systems are Dedicated [a] to same classification level and same or different type(s) of intelligence information and some systems are System High at classification level of the Dedicated systems, but not SCI.	3. Network High [b]
4. Some systems are Dedicated [a] to TOP SECRET level and same or different types of intelligence information and some systems are Compartmented.	4. Compartmented
5. All systems are System High to the same classification level	5. Network High [b]
6. Some systems are System high at TOP SECRET level and some systems are Compartmented.	6. Compartmented
7. All systems are Compartmented	7. Compartmented
8. Some systems are Dedicated to TOP SECRET level and same or different types of intelligence information, some systems and System High at TOP SECRET level, and some systems are Compartmented.	8. Compartmented

[a] These systems, in effect, adopt the operating mode of the network and, therefore, must meet the minimum security requirements of that mode as expressed in Chapter II.

[b] Network High requires that all unescorted personnel having access to any of the ADP systems of the network must have formal access approvals for all data processed and/or stored by all of the ADP systems in the network.

shall immediately notify the Network Security Officer (NSO) when network security breaches are suspected or possible; this notification shall be followed by a written report as appropriate. The NSO shall determine the impact on network security of any abnormalities of ADP system operation. Each NFIB member or his designee retains the prerogative of suspending his organization's operational participation in the network prior to any notification if he believes sufficient threat of compromise exists.

III.2.e. *ISSO Network Responsibilities.* Each ADP system in an ADP network shall have a formally designated ISSO whose responsibilities are as follows:

III.2.e(1) Advise and assist his NFIB member or designee on all physical, personnel, procedural, hardware/software, and communications security matters pertaining to the network.

III.2.e(2) Coordinate with other ISSO's and the NSO in the administration of network security-related activities as required by this Regulation.

III.2.f. *Responsibilities and Functions of the NSO*

III.2.f(1) Coordinate the application of network security hardware/software (security labeling, audit trails, dissemination controls, etc.), physical/personnel security measures, communications security, and administrative/procedural security measures within the ADP network.

III.2.f(2) Investigate and resolve network security incidents and/or violations leading to or involving a potential compromise of classified information.

III.2.f(3) Determine that network security requirements are met before an ADP system is connected to the ADP network.

III.2.f(4) Advise and assist the ADP network manager on studies, projects, tests and evaluations, and experiments which relate to the security of the ADP network.

III.2.f(5) Assist the network manager in assuring that all ADP network participants adhere to the security requirements specified in this Regulation.

III.2.g. *Reporting.* All ADP system security-related incidents shall be reported by the ISSO to the NSO. The nature and extent of the report shall be based upon the security urgency of the event.

III.2.g(1) *Routine Security Report.* A routine security report shall be made of a system malfunction or security incident which has potential network security implications. The report shall include the following information:

III.2.g(1)(a) NFIB member or his designee submitting the report.

III.2.g(1)(b) The ADP system in which the abnormality occurred.

III.2.g(1)(c) Narrative description of the event.

III.2.g(1)(d) Date, time, location of event.

III.2.g(1)(e) Results of the ISSO's internal investigation as to the cause of the abnormality and remedial actions taken.

III.2.g(2) *Special Security Reports.* The ISSO shall immediately notify the Network Security Officer of a system abnormality providing reason to suspect a covert violation of the security integrity of the ADP system or network. An initial written report covering the basic information provided in a routine security report shall be forwarded as soon as possible. The nature and extent of the reporting requirement following such an event cannot be projected since it would involve extensive internal organizational counterintelligence investigation.

III.2.g(3) *Evaluation and Analysis of Report.* The NSO shall review all reports submitted for purposes of evaluating the security performance aspects of the network.

III.2.g(4) In the event a NFIB member or his designee takes exception to the content of, or actions required by, a security report, he shall appeal to the network authority who shall establish an ad hoc committee of network participants to resolve the issue.

III.3. *Accreditation Process*

III.3.a. The authority, organization, or manager responsible for the overall operation and control of the ADP network shall accredit it in cooperation with the NFIB members participating in the ADP network.

III.3.b. For networks having multiple NFIB members responsible for the overall operation and control of the ADP network, the accreditation shall be made jointly by these NFIB members.

III.3.c. The NSO shall provide written assurance to the appropriate network authority(ies) that the ADP network meets the minimum ADP network security requirements as outlined below.

III.4. *Minimum ADP Network Security Requirements*

III.4.a. *ADP System Security.* Each ADP system must be accredited for operation in the appropriate network mode before becoming an active participant of the ADP network. This accreditation shall be based on the requirements outlined in Chapter II. ADP system accreditation must be provided to the NSO.

III.4.b. *Telecommunications.* The communications links between all components (i.e., ADP systems, see Figure 1) of an ADP network shall be secured in accordance with appropriate directives for the highest classification of information designated for transmission.

III.4.c. *Emanations Security Aspects.* The vulnerability of network operations to exploitation through compromising emanations shall be determined in the process of network accreditation. Evaluation of the risks associated with the individual ADP systems and their interconnections shall be accomplished in accordance with appropriate directives.

III.4.d. *Network Components.* All ADP systems, terminals, and peripheral devices not designated for use in the current network mode of operation shall be disconnected from the ADP network in an approved manner.

III.4.e. *Security Identification and Labeling.* The security level of network users, remote sites, network programs, and files shall be identifiable. Specific classification level, common controls, procedures established by DCID 1/7, and SCI markings shall be identified. This identification shall be a primary factor in the monitoring and control of data transfers. Security classification and other control caveats shall be identified with the network information and programs while in the ADP network. Appropriate labeling of any output from the network shall be ensured.

III.4.f. *Access to Network Files.* Each data file in the network shall have an Office of Primary Interest (OPI). The OPI as owner, manager, and controller of the information in the file is responsible for file maintenance, file classification, and read/write access authorization of other network users of the file. A current list, by file, of network users and their access approvals shall be maintained, classified, and controlled by the OPI. A copy of this list shall be provided to the cognizant ISSO and NSO.

III.4.g. *Network User Access Control.* Each ADP system shall assure that a network user is confined within the bounds of that system's files to which the user has been authorized access, and that the user can exercise only those privileges for which he has been authorized. A network user shall not be able to access or alter any of the network security capabilities.

III.4.h. *Network Programs.* Network programs, such as log-in programs, file maintenance programs, and listing programs, shall perform network specific functions which are prohibited to the ADP systems' and users' programs. However, network programs shall not have complete freedom and shall be given only the authority that is needed to accomplish the particular network functions.

III.4.i. *Procedures.* The security procedures established for the protection, and operational security, of the network shall be coordinated among all participants by the Network Security Officer and administered by the ISSO of each ADP system in the network.

III.4.j. *Audit Trails.* Security audit trails shall be generated by the ADP systems in the network. This information shall be made available to the Network Security Officer to permit a regular security review of the network activity. In some instances a manual security audit may be warranted.

GLOSSARY

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

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 NFIB member 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 NFIB member 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 pre-processing functions. It may perform line control, message handling, code conversion, error control, data control, data management, terminal handling, etc. (See Regulation, 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.