Security of Foreign Intelligence in Automated Systems and Networks

(Effective _____)

Pursuant to section 102 of the National Security Act of 1947, Executive Order 12356, and National Security Council (NSC) Directives, this Director of Central Intelligence Directive (DCID) establishes policy and prescribes authority and responsibilities for the protection of foreign intelligence and counterintelligence (2). derived through sensitive sources and methods and processed, stored, or communicated by automated systems or networks (3).

APPLICABILITY

This Directive applies to all United States government departments and agencies which use automated systems to process, store, or communicate intelligence information. It applies with equal force to automated systems or networks owned or operated by the United States Government and those owned or operated by contractors or consultants performing for the United States Government.

POLICY

The rapid proliferation of automated tools and methods for the electronic processing of information reinforces the requirement for providing security and surety for the intelligence information they contain and process equal to that heretofore applied to the manual and printed world. Automated systems and networks of the Intelligence Community (IC) will be managed and protected in a manner which insures that both the intelligence information and the sensitive sources and methods through which it is derived are effectively secured against successful attack by hostile intelligence activities. The goal of this Directive and the accompanying Regulation is to provide policy and broad technical guidance which will enforce the same classification, compartmentation, and need-to-know standards now applied to the manual handling of intelligence information.

---

1. Supercedes DCID 1/16, 6 June 1978
2. Foreign intelligence and counterintelligence are used in this directive as defined in Executive Order 12333 and as classified under the provisions of Executive Order 12356. For the purposes of this Directive, the term "intelligence information" shall include both foreign intelligence and foreign counterintelligence.
3. Automated systems and networks are defined as collections of computer-based equipment and software which are designed to process, store, or communicate information as digital data. Automated systems and networks include automated data processing (ADP),shared logic word processing (WP), automated office (AO), and electronic mail (EM) systems.

The diversity and complexity of automated systems and networks now in operation in the U.S. Intelligence Community and those already designed for future installation may not provide for full compliance with the provisions of the Directive and the attached Computer Security Regulation. Therefore, the extent to which the exceptions to this Directive are applied to such systems and networks is left to the determination of each National Foreign Intelligence Board (NFIB) member in view of his ultimate responsibility for the protection of classified intelligence information.

The NFIB member shall establish and maintain a formal security program to ensure adequate protection is provided for classified intelligence information processed in the community's automated systems and networks. The use of automated systems requires that classified intelligence information, when processed by computers, be afforded protection equivalent to that dictated by Presidential Policy, NSC Directives, Director of Central (DCI) Directives, and other regulations concerning the overall information security requirements, need-to-know controls, handling caveats, personnel access requirements, and dissemination procedures.

The minimum security requirements for the authorized modes of operation and the recommended criteria for determining whether the specific system or network provides the required protection is contained in the attached security regulation. The NFIB member(s) concerned may establish for specific systems or networks additional security measures and capabilities if deemed appropriate. Automated systems involving foreign governments shall be addressed on a case-by-case basis by the NFIB member(s) involved.

This Directive does not supercede or augment the requirements on the control, use, and dissemination of Restricted Data, Formerly Restriced Data, or Communications Security (COMSEC) related material as establihed by or under existing statutes, directives, or Presidential Policy.

AUTHORITY

The NFIB members are assigned the following authority concerning automated systems/network accreditations:

Automated System/Network - When an automated system or network is serving only a single NFIB member agency, the NFIB member who is the single user of the automated system/network is designated the Accreditation Authority for that system/network.

Multiple NFIB Members' System/Network - When an automated system or network is serving two or more NFIB member agencies, one NFIB member, selected by those NFIB members involved, will be designated as the Principal Accreditation Authority for that system/network.

NFIB Members' Concatenated Systems/Networks - When two or more systems/ networks are interconnected or when a system is connected to

a network of systems, the NFIB members who are already designated as the Accreditation or Principal Accreditation Authority of any of the systems/networks involved will become members of the Joint Accreditation Authority for the concatenated systems/networks. One of the NFIB members of the Joint Accreditation Authority will be designated, by joint agreement, Principal Joint Accreditation Authority and all participating NFIB members shall act as a common body for executing the responsibilities of the Joint Accreditation Authority.

RESPONSIBILITIES - The NFIB member(s) serving as Accreditation Authorities are responsible to:

a. assure that compliance with stated DCI policy is accomplished in the most economical and effective operational manner.

b. Identify the information security requirements for the specific system/ network based on applicable intelligence information security policies and regulations.

c. Define the complete set of security measures/mechanisms required based on the functionality of the system/network, the user/operational environment, the information characteristics, and applicable information security criteria.

d. Perform the technical assessments, risk analyses, and security tests upon which an accreditation of the system/network can be granted.

e. Evaluate the system/network for compliance with this Directive and the requirements established in the accompanying Regulation, and certify such compliance.

f. Accredit or re-accredit the system/network and establish the allowable operational environment based on the assessment and the security tests of the system/network.

g. Coordinate all system security actions to ensure that all managers and users of an automated system or network implement the established security measures and capabilities.

EXEMPTIONS - The NFIB member or his designee may temporarily exempt specific systems under his jurisdiction from complete compliance with this Directive and the accompanying Regulation when such compliance would significantly impair the execution of his mission. An exemption shall be granted only when the NFIB member or his designee has assured himself that additional temporary measures in place will adequately protect the intelligence information being processed in the specific automated system or network.

SUPERSESSION - This Directive supersedes Director of Central Intelligence Directive No. 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks", effective _____; and all existing directives, regulations, and other documents referencing the superseded Directive.

IMPLEMENTATION - Within one year of the effective date of this Directive each NFIB member will develop and promulgate a formal automated systems security program, implementing directives and regulations for systems and networks under his jurisdiction.

ADMINISTRATIVE REPORTS - Each NFIB member or his designee will provide to the DCI (attn. Chairman, Security Committee) an annual report as of 31 December detailing the accredited and exempted systems currently operating under his jurisdiction.

REVIEW - This Directive and the accompanying Regulation will be reviewed within three years from the effective date.

DCI Reg. xx-xx

Security Standards for the Protection of Intelligence Information in Automated Systems and Networks

Chapter I

GENERAL

Introduction

I.1 Director of Central Intelligence Directive No. 1/16 (DCID 1/16) requires that all United States Government departments and agencies which store, process, or communicate classified intelligence information by means of computer-based automated systems or networks establish and maintain formal systems security programs for the protection of that information and the sensitive sources and methods through which it was derived. DCID 1/16 assigns primary responsibility for the management of that protection to the National Foreign Intelligence Board (NFIB) members involved.

I.1.a The purpose of this regulation is to:

(1) Define a set of generic security requirements which must be satisfied by any system processing classified intelligence information. These are intended to be used as criteria by which a system can be engineered and evaluated.

(2) Prescribe certain minimum security requirements;

(3) Define the security modes under which automated systems and networks of the Intelligence Community (IC) may be operated;

(4) Establish a set of security standards and criteria suitable for use with various combinations of security modes, functions performed, and operating environments;

(5) Describe an accreditation process through which individual NFIB members, or groups of members, may manage the defense of automated systems or networks against hostile intelligence attack.

Provided minimum security requirements are met, individual NFIB members, or consortiums of members, are encouraged to exercise every initiative to provide cost-effective security to their systems.

I.2 Generic Security Requirements

I.2.a The various policy statements concerning the protection to be afforded to classified intelligence information allow one to derive several fundamental requirements, which fall under the following headings:

(1) Information protection based upon classification and compartmentation.

(2) Information protection based upon Need-to-Know

(3) Labelling

(4) Accountability

(5) Continuous Protection

I.2.b. In this section it will be useful to define the concept of "protection system", which will be defined as the totality of mechanisms which enforce the identified security requirements. Thus, the protection system for automated systems and networks includes hardware and software features, personnel security, physical security, and administrative procedures. The intent of this regulation is to define a uniform level of protection to be afforded foreign intelligence and counterintelligence, and to provide sufficient guidance to allow specific protection systems to be engineered for specific operational environments which will provide the requisite level of security in a cost-effective manner. Thus, it is allowed, within the limits defined herein, to substitute security features with others which provide an equivalent level of protection.

I.2.b(1) Protection based upon classification and compartmentation - The protection system must enforce the formal system of information control reflected in the security classification and compartmentation definitions associated with classified intelligence information, together with the clearance and special access authorizations associated with individuals who may request access to the information.

I.2.b(2) Protection based upon Need-to Know - The protection system must enforce access limitations placed on information which is based on the determination that identified individuals or groups of individuals have valid operational Need-to-Know for the information.

I.2.b(3) Labelling - In order to be able to insure that proper controls can be afforded to foreign intelligence and counterintelligence, its classification level and any compartmentation restrictions must be clearly identified. Thus, the protection system must be able to reliably and accurately associate security labels with all information for which it has responsibility, which identifies classification, compartmentation, and special handling restrictions. The direct implication of this requirement for an automated system is that information which is intended to be exported from the system (e.g., tapes, line printer output) be labelled either on the basis of internally maintained security markings, or on the basis of unique characteristics of the installation.

A.I.2.b(4) Accountability - The protection system must be capable of tracing actions affecting security to the party responsible for the action. This requirement implies that the protection system be able to establish the identity of individuals, determine and authenticate their clearance level and access authorizations, and maintain accounting information of sufficient detail and granularity to support tracing the auditable events

to a specific individual who has taken the actions in question, or in whose behalf the action was taken.

I.2.b(4) Continuous Protection - The protection system must be able to provide continuous protection to classified data under its control. The implication of this requirement for that portion of the protection system which is implemented in an automated system is that the security relevant portions of the automated system be identified and maintained under continuous control to assure that unauthorized changes have not been made which could possibly subvert the system's ability to control classified information.

Chapter II

Minimum Requirements for System Security

As established in this chapter, the general standards, the system security requirements for automated data processing systems (hereinafter referred to as the system), and the criteria for evaluating a system's ability to protect intelligence information will be uniformly applied throughout the NFIB Community.

II.1. General Security Standards

II.1.a. Information System Security Officer - An Information System Security Officer (ISSO) will be appointed for each ADP system processing intelligence information. The ISSO is responsible for ensuring compliance with the security standards established in this Regulation as well as the implementing directives promulgated by the responsible authority. The ISSO will monitor any changes in system operation that may affect the security status of the total system, report major security deficiencies in system operation, and provide system accreditation statements and recommendations to the responsible authority.

II.2. Personnel Security

II.2.a. When a system is approved to process collateral information up to but excluding Top Secret, all personnel requiring unescorted access to either the central computing facility or the magnetic media storage facility must have a valid security clearance for the security classification level of the collateral information being processed by the system. All personnel requiring unescorted access to a remote terminal/terminal area must have a valid security clearance for the highest security classification of the information designated for input/output at the assigned terminal.

II.2.b. When a system is approved to process Top Secret collateral intelligence information, all personnel requiring unescorted access to either the central computing facility or magnetic storage facility must have a valid Top Secret clearance, and all personnel requiring unescorted access to a remote terminal/terminal area must have a valid security clearance for the highest security classification of the information accessible through the assigned terminal

II.2.c. When a system is approved to process Sensitive Compartmented Information (SCI), all personnel requiring unescorted access to the central computing facility or magnetic media storage facility must be security approved in accordance with DCID 1/14 and have formal access approval for

each SCI program being processed by the system, and all personnel requiring unescorted access to a terminal/terminal area must be security approved for the highest security classification of information accessible through the assigned terminal.

II.3. Administrative

II.3.a. All system users must be briefed on the need for exercising sound security practices to protect the intelligence information processed by the system. Users will be informed of the security classification level at which the system is operating and the security requirements for that level.

II.3.a. The processing of intelligence information at any level requires that the Need-to-Know criteria be rigidly enforced. That is, even though all personnel are appropriately cleared, not all personnel shall automatically have authorization to see or use all of the data being processed.

II.3.b. Approval for unescorted visits to a system approved to process intelligence information will be requested in advance via appropriate command channels. In all cases, the request must indicate that the person to make the visit possesses a valid security clearance, is access approvable for any SCI data being processed, and has an established need-to-know.

II.3.c. Administrative approvals (i.e., those not requiring substantive briefings) may be used to grant persons escorted access to the central computing facility and remote terminal areas when, and only when, such persons do not require access to the intelligence information being processed.

II.4 Physical Security

II.4.a. When used for the processing of collateral intelligence information the central computing facility and any remote terminal areas must be secured in a manner commensurate with the classification of the information being processed by the system.

II.4.b. When used for the processing of Top Secret and/or SCI intelligence information, the central computing facility and any remote terminal areas must be secured in accordance with the provisions of USIC Physical Security Standards for SCIFS, NFIB/NFIC-9.1/47.

II.5. Communications Security. - Communications links used to transmit intelligence information between system components or systems must be secured in accordance with appropriate communications security directives for the security level and SCI control channel(s) of the information designated for transmission.

II.6 Emanations Security - The vulnerability of a specific system's operation to exploitation of compromising emanations must be determined during system configuration. For new procurements, guidance on equipment TEMPEST characteristics should be obtained from the appropriate communications security office, and equipment known to have acceptable TEMPEST profiles should be selected. During the system accreditation process, appropriate communications security directives will be implemented for all security elements.

II.7. System Acquisition - Secure system criteria required to meet the general security standards and system security requirements set forth in this Regulation, or system features/capabilities available from advanced state-of-the-art technology, will be included as mandatory in procurement requests for all new systems which will process or handle intelligence information. Vendor submissions for either the development of integrated systems or the delivery of hardware systems must include a review of how the system satisfies the security-related specifications included.

II.8. Systems Maintainance

II.8.a. All vendor maintenance personnel who service automated systems used for the processing of intelligence information should possess a security clearance commensurate with the highest classification level of the information being processed and access approvable for all SCI being processed.

II.8.b. All uncleared vendor maintenance personnel will be monitored at all times by a system knowledgeable individual possessing a valid security clearance and access approvals for the highest security classification and SCI control channel(s) of the information being processed.

II.8.c As a rule, the use of remote diagnostic links for the maintenance of systems processing classified intelligence information is prohibited. The NFIB member may, however, grant exceptions on a case-by-case basis provided all channels to data storage devices are disabled, internal memory and memory buffers are cleared (both before and after the use of the diagnostic capability), and a separate operating system is used during the diagnostic procedure.

Chapter III

Security Modes of Operation

At this time there are four modes of operation defined for automated systems which process classified intelligences information. They are (a) Dedicated Mode, (b) System High Mode, (c) Compartmented Mode, and (d) Expanded Compartmented Mode. In each of these, the combination of hardware/software capability, personnel security, physical security, and administrative procedures are intended to satisfy the set of generic security requirements of Section I.2 (Generic Requirements). However, it is recognized that operating environments will exist, with unique sets of requirements, for which none of the modes defined herein provide the best cost-effective solution to achieving the requisite level of security while still allowing for operational requirements to be satisfied. Thus, some latitude is authorized in engineering specific installations, insofar as the equivalent level of protection is achieved. Deviations from the modes defined herein may only be accredited by the NFIB member in accordance with the procedures defined herein. However, no deviations are allowed to any of the modes which result in either (a) access to an ADP system containing SCI by a user cleared less than SECRET, or (b) granting of programming capability on a system which processes and/or stores SCI, to any user not authorized access to SCI.

III.1. Dedicated Mode

III.1.a. Intelligence information may be processed and/or stored in an automated system operating in the Dedicated Mode; that is, the system is specifically and exclusively dedicated 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.

III.1.b. Hardware/Software. The automated system, at a minimum, must be able to enforce Need-to-Know access control measures on a project, group, or per-user basis.

III.1.c. Accreditation Process. The NFIB member or his designee can accredit an automated 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 herein.

III.1.d. Personnel Security. All unescorted personnel requiring access to the central computer facility or any remote terminal shall have a valid security clearance for the one particular type of intelligence information contained within the system.

III.1.e. 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.

III.1.f. Administrative. 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 automated system.

III.1.g. Termination of Dedicated Mode Operation. On changing from Dedicated Mode of operation, all intelligence information and the media used in its processing and/or storing shall be secured or cleared in an approved manner. An automated system which has operated in the Dedicated Mode may then be returned to its original or different mode, as appropriate.

III.2 System High Mode

III.2.a. Intelligence information may be processed and/or stored in an automated system operating in the System High Mode; that is, the system is operating with security measures commensurate with the highest classification and sensitivity of information being processed and/or stored.

III.2.b. Hardware/Software. The automated system shall, at a minimum:

(1) enforce Need-to-Know access controls on a per-user basis.

(2) produce, selectively and securely, an audit trail of security events, containing enough information to permit the ISSO to perform a security review of system activity.

(3) reliably place security labels on removable output media.

III.2.c. Accreditation Process. The NFIB member or his designee can accredit an automated system operating in the System High Mode after receiving written assurance from the computer system manager and the responsible ISSO that the system meets the minimum security requirements for this mode as specified herein.

III.2.d. Personnel Security. All unescorted personnel requiring unescorted 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 system. Need-to-Know criteria shall apply.

III.2.e. 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.

III.2.f. Administrative. 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.

III.2.g. Termination of System High Mode of Operation. On changing from System High Mode of Operation, all intelligence information and the media used in its processing and/or storage shall be secured or cleared in an approved manner. An automated system which has operated in the System High Mode may then be returned to its original or different mode, as appropriate.

III.3 Compartmented Mode

III.3.a. SCI may be processed and/or stored in an automated system operating in the Compartmented Mode; that is, the system is processing two or more types of SCI with any other type of SCI, or any one type of SCI with other than SCI, and the 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.

III.3.b. Hardware/Software. The automated system shall, at a minimum:

(1) enforce classification/compartmentation access controls on all system storage objects (e.g., files, segments, devices). That is, the system must be able to support the identification of a number of hierarchical classification levels and an appropriate number of non-hierarchical categories at each level (to be labelled as desired by the system administrator), and enforce the access control rules based upon these attributes.

(2) enforce Need-to-Know access control on a per-user basis.

(3) produce, selectively and securely, an audit trail of security events, containing enough information to permit the ISSO to perform a security review of system activity.

(4) accurately maintain security labels internal to the system, and reliably place security labels on removable output media.

(5) ensure that residue from terminated user programs is cleared before memory and on-line storage devices' locations are released by the system for use by another user program.

(6) authenticate remote terminals and personnel.

(7) the system must exhibit sufficient internal structure to allow the identification of the security perimeter; that is, it should be possible to clearly distinguish security-critical code from non security-critical code. Evidence must be available to support the

assertion that programs operating in user mode are incapable of directly executing instructions which fall within the security perimeter. Additionally, the correct operation of the security-critical code must not be dependent upon the correct operation of any other code in the system.

III.3.c. Accreditation Process

III.3.c(1) Only the NFIB member can accredit an automated system operating in the Compartmented Mode.

III.3.c(2) The accreditation will be based upon the results of a security analysis, test, and evaluation to assure that the system meets the minimum requirements for this mode as defined herein. 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.3.d. Personnel Security

III.3.d(1) 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.

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

III.3.e. Physical Security

III.3.d(1) 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.

III.3.d(2) 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.

III.3.f. Administrative

III.3.f(1) No user cleared for less than SCI access will be granted programming capability on a system which processes and/or stores SCI. Hardware/software mechanisms must be in place which are capable of enforcing this restriction.

---

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

III.3.f(2) 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.

III.3.f(3) 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.

III.3.g. Termination of Compartmented Mode of Operation. On changing from Compartmented Mode of Operation, all intelligence information and the media used in its processing and/or storage shall be secured or cleared in an approved manner. An automated system which has operated in the Compartmented Mode may then be returned to its original or different mode, as appropriate.

III.4 Expanded Compartmented Mode

III.4.a. SCI may be processed and/or stored in an automated system operating in the Expanded Compartmented Mode; that is, the system is processing one or more types of SCI along with collateral (non-SCI), and system access is secured to at least the SECRET level, but all system users need not necessarily be formally authorized access to SCI. This mode is designed to accomodate unique instances (e.g., the tactical environment) in which specific individuals have a valid operational need to access collateral data which resides in a data base which also contains SCI data. It assumes that such systems have well-defined functions (e.g., DBMS), offering limited user interaction and, especially, do not support general user programming. It is intended that systems that operate in the Expanded Compartmented mode have been designed, engineered, and configured specifically to operate in that mode. Thus, operational and security requirements are documented and appropriate security mechanisms are designed and engineered into the system. Additionally, the NFIB member is involved in the decision to develop and implement a system operating in this mode, and specifically approves any plans to operate a system in the Expanded Compartmented Mode.

III.4.b Hardware/Software. The automated system shall, at a minimum:

(1) enforce classification/compartmentation access controls on all system storage objects (e.g., files, segments, devices). That is, the system must be able to support the identification of a number of hierarchical classification levels and an appropriate number of non-hierarchical categories at each level (to be labelled as desired by the system administrator), and enforce the access control rules based upon these attributes.

(2) enforce Need-to-Know access controls on a per-user basis. The principle of least privilege shall pervade system operations.

(3) produce, selectively and securely, an audit trail of security events, containing enough information to permit the ISSO to perform a security review of system activity.

(4) accurately maintain security labels internal to the system, and reliably place security labels on removable output media.

(5) ensure that residue from terminated user programs is cleared before memory and on-line storage devices' locations are released by the system for use by another user program.

(6) authenticate remote terminals and personnel.

(7) enforce, on a per-user/per-terminal basis, any limitations defined for access to data and ability to exercise system capabilities.

(8) exhibit sufficient internal structure to allow the identification of the security perimeter; that is, it should be possible to clearly distinguish security-critical code from non security-critical code. Evidence must be available to support the assertion that programs operating in user mode are incapable of directly executing instructions which fall within the security perimeter. Additionally, the correct operation of the security-critical code must not be dependent upon the correct operation of any other code in the system.

(9) exhibit strong technical evidence to substantiate the claim that the original system security requirements defined as design goals are, in fact, satisfied by the operational system.

III.4.c Accreditation Process

III.4.c(1) Only the NFIB member can accredit an automated system operating in the Expanded Compartmented Mode.

III.4.c(2) The accreditation will be based upon the results of a security analysis, test, and evaluation to assure that the system meets the minimum requirements for this mode as defined herein. 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.

III.4.d. Personnel Security

III.4.d(1) All unescorted personnel requiring access to the central computer facility shall have a valid TOP SECRET clearance and formal access approvals for all data processed and/or stored in the system. Need-to-Know criteria shall apply.

III.4.d(2) All unescorted personnel requiring access to any remote terminal facility shall be cleared to the level of the data designated for

input/output at that facility, or at the SECRET level, whichever is higher. Need-to-Know criteria shall apply.

III.4.e. Physical Security

III.4.e(1) 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.

III.4.e(2) Each remote terminal area will be secured in a manner commensurate with the handling of the most sensitive data designated for output at that terminal facility, or at the SECRET level, whichever is higher.

III.4.f. Administrative

III.4.f(1) No user cleared for less than SCI access will be granted programming capability on a system which processes and/or stores SCI. Hardware/software mechanisms must be in place which are capable of enforcing this restriction.

III.4.f(2) The capabilities granted to users who have access to an automated system which processes and/or stores SCI, and who are cleared less than TOP SECRET, must be clearly defined. Hardware/software mechanisms must be in place which are capable of limiting access to only those capabilities which have been defined.

III.4.f(3) All terminal and peripheral devices not designated for use in the current Expanded Compartmented Mode of operation shall be disconnected from the system in an approved manner.

III.4.f.(4) 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.

III.4.g. Termination of Expanded Compartmented Mode of Operation. On changing from Expanded Compartmented Mode of Operation, all intelligence information and the media used in its processing and/or storage shall be secured or cleared in an approved manner. An automated system which has operated in the Compartmented Mode may then be returned to its original or different mode, as appropriate.

Memorandum of Agreement

When more than one NFIB member is involved in an automated system or network, a Memorandum of Agreement must be executed. This memorandum must, at minimum, identify the Principal Accreditation Authority, or, in concatenated systems or networks, the Joint Accreditation Authority and the Principal Joint Accreditation Authority. It must identify the level(s) of classification of data being processed and any operational restrictions which are placed on the system or network. This memorandum will be updated whenever a significant change is made to any of these items.

Accreditation

All automated systems and networks which processs classified foreign intelligence or counterintelligence must be accredited. The accreditiation statement must be supported by complete documentation which fully describes the technical assessments of the automated system or network, the vulnerabilities, risks, and associated countermeasures, and the results of the security tests and analyses which have been performed.