TRANSMITTAL SLIP	DATE 8/20/84
TO:	MS/ODP
ROOM NO. 2D0105	BUILDING Hqs.

REMARKS:

This has not yet been released by the CIRS Security Working Group. NSA is still in the approval process. As stated in ORD-0832-84 dtd 18 July 1984, the operational Guard will be directed against the ETCB requirement for the CIRS program.

Jan
- p/s file with RECON Guard material.

STAT

FROM:	ORD/ISRD
ROOM NO. 726	BUILDING Ames

STAT

EXTENSION

FORM NO. REPLACES FORM 36-8 (47)

25X1

SECRET

F I N A L

D R A F T

PRELIMINARY

CIRS SECURITY PLAN

18 JANUARY 1984

Prepared by the DCI's
Intelligence Information Handling Committee's
Community Information Retrieval System
Security Working Group

Dr. Robert S. Smith
The BDM Corporation

25X1

SECRET

FOREWORD

Pursuant to Section 102 of the National Security Act of 1947 and Executive Order 12333, the Director of Central Intelligence established the Information Handling Committee (IHC). One of the functions of the Committee is to promote and coordinate the development of Intelligence Community information handling capabilities which will provide analysts relevant multi-source information on a timely basis. As a part of this effort, a working group was established to develop a plan for constructing a Community Information Retrieval System (CIRS). The full IHC adopted the plan in September 1982. Subsequently, a Security Working Group was established to consider the security problems involved in the CIRS and prepare a CIRS Security Plan. This plan parallels the CIRS phased implementation plan with staged sets of security requirements designed to provide acceptable levels of security during the development of CIRS and for continued use after the full implementation of the plan (circa 1990). (U)

(BLANK PAGE)

TABLE OF CONTENTS

(BLANK PAGE)

I. EXECUTIVE SUMMARY

INTRODUCTION

1.1 This report presents a security plan to govern the implementation of the Community Information Retrieval System (CIRS). It is divided into an introduction describing the CIRS plan, a chapter specifying the security requirements implemented through Automatic Data Processing (ADP) features, a chapter presenting security features provided by environmental and administrative controls, and sections presenting supporting material. (U)

The CIRS Plan and Implementation Efforts

1.2 The CIRS plan was approved by the Information Handling Committe (IHC) to provide authorized United States intelligence analysts with relevant multi-source information on a timely basis. The recommended architecture is a confederation of systems in which the information storage and retrieval nodes will be NSA/WINDMILL, FTD/CIRC, NPIC INS, D-SAFE and C-SAFE. User access will be through the COINS and DODIIS networks via a gateway between the two networks. (U)

1.3 Eight areas of security have been identified and addressed by the CIRS Security Working Group (SWG). These are shown in Table 1.

Table 1 - CIRS Security Areas (U)

- ADP Security Functions
  - -- Computer hardware
  - -- Computer software
  - -- Related documentation
- Environmental and Administrative Controls
  - -- Communications Security (COMSEC)
  - -- Physical security
  - -- Emanation Control (TEMPEST)
  - -- Documentation
  - -- Personnel
  - -- Procedures

Objectives of the CIRS Security Plan

1.4 Three basic objectives have been identified for this security plan. They are:

1) To ensure that a [redacted] will be working under [redacted],

2) [redacted] define a time schedule for the implementation of the security enhancements identified in the three CIRS security stages, and

3) To furnish planning guidance to the CIRS components to assist them in defining what must be accomplished in order to achieve the results identified in the CIRS plan. (U)

CIRS Implementation Schedule

1.5 The schedule for implementation of the CIRS security plan is divided into three stages for the requirements specified under ADP security functions. Each stage builds upon previous security features to provide a uniform basis for minimum protection of the information processed by CIRS components. All environmental and administrative security requirements identified in this plan are expected to be in place before a CIRS component is integrated into the confederation of systems that will comprise CIRS. Table 2 below presents the basic schedule.

Table 2 - CIRS Implementation Schedule (U)

Date (CY)	NODE	CIRS Security Stage
Late 1985	NSA/WINDMILL	I
Early 1986	FTD/CIRC	I
Late 1986	DIA-SAFE	I
Mid 1987	NPIC INS	II
Late 1988	Compartmented-Mode Operations (per DCID 1/16)	III
Mid 1990	CIA-SAFE	III

Implementation Guidelines

1.6 The diversity present in the different hardware and software systems used or planned for use at the CIRS components requires a flexible implementation plan. [redacted]nt will be expected to implement the security requirements presented in this plan by the method they deem best for use at their individual installations. (U)

SECURITY FEATURES PROVIDED BY ADP FUNCTIONS

1.7 Chapter III of this document addresses three of the eight basic security areas: computer hardware, computer software, and related documentation topics. Minimum security requirements in each of the CIRS security stages are based on the applicable guidelines defined in "DOD Trusted Computer System Evaluation Criteria" (TCSEC) dated 15 August 1983. Some requirements made necessary by the unique architecture of CIRS have been added, and a definition for an Extended Trusted Computing Base has been developed to cover networking configurations and as an aid to understanding and formulating the CIRS-specific aspects of the security requirements. (U)

Initial CIRS ADP Security (Stage I/1985-1986)

1.8 This stage of CIRS ADP security is based on the discretionary access control security policy described in the TCSEC but is modified by requiring some mandatory controls on access to stored information. Individual user identification and the creation of an audit trail of security-related user actions are prime requirements. Prior to acceptance of the system for general use, a test of the software will be made to see if any obvious ways of bypassing the security mechanisms exist. A certification of this test will be made as part of an annual re-certification reporting to the IHC. In this

initial stage of CIRS security, all users must have a Top Secret clearance and be indoctrinated for both the SI and TK compartments of SCI. Access by foreign nationals to data bases identified under the CIRS plan is not permitted. (U)

Intermediate CIRS ADP Security (Stage II/1986-1988)

1.9 This stage of CIRS ADP security builds on the initial requirements from the first stage. It adds several requirements adding to the information controls available and bringing the full set of requirements into rough correspondence to the mandatory labeled security protection level of the TCSEC. Internal and external labeling of all stored items is now required and all stored items are placed under a mandatory access control policy enforced by the ADP system. The system is now required to keep information as to the security clearance level and special access authorizations of each individual user. (U)

Final CIRS ADP Security (Stage III/1988-1990)

1.10 The last stage in the growth of CIRS ADP security features adds sufficient elements to those of Stage II to permit compartmented mode operations. This will allow removing the requirement for all users to be indoctrinated for both SI and TK compartments, but the system will maintain a policy of not allowing access to foreign nationals. Tighter controls are applied to access control mechanisms and system architecture. Covert information channels must be considered in the system design and logging of events which may be related to their use is now a requirement in the security audit trail. System acceptance testing requirements are also broadened and configuration management of the security-related software is required. (U)

SECURITY FEATURES PROVIDED BY ENVIRONMENTAL AND ADMINISTRATIVE CONTROLS

1.11 This section of the CIRS security plan addresses the COMSEC, documentation, personnel, physical, procedures, and TEMPEST considerations in the eight basic security areas covered by this plan. Since these controls supply basic security in depth and fulfill mandatory requirements within traditional security areas, they are expected to be in place at CIRS IOC and continue in force throughout system life. (U)

Communications Security

1.12 All communications and data links carrying CIRS data are required to be accredited for transmitting TS/SCI. Each CIRS component network (COINS and DODIIS) must also have a network control station furnishing such information as needed by the corresponding network security officer to monitor the security aspects of his network. (U)

Physical Security

1.13 All CIRS host sites, networks and communications links and their personnel and environs are required to be in compliance with applicable Community standards. In addition, when physical access to a terminal authorized for CIRS use cannot be restricted to full CIRS user clearance standards, a double method of verifying user identity is required (e.g., password and badge reader or password and fingerprint scan). (U)

Emanation Control

1.14 All equipment or circuits carrying CIRS information in clear text form must meet all applicable sections of NACSIM 5100A (TEMPEST specifications). The KAG 30 emanation standards must be met for critical cryptographic functions. (U)

Documentation

1.15 Each CIRS component is required to prepare a system security plan which will present all applicable regulations and special procedures in a single document. (U)

1.16 In addition, each component will be required to file copies of documents relating to security certifications and inter-component agreements (or notification that such agreements have been made) with the IHC at the IHC staff. The IHC staff will also be responsible for coordinating the acquisition and distribution of such security-related audit data as may be needed to construct a complete audit trail of a CIRS-related event. (U)

Personnel

1.17 Requirements have been established in conformance with Community standards to ensure that all personnel associated with the use of CIRS information or the maintenance of both hardware and software used within CIRS have been suitably investigated and cleared as necessary to perform their jobs. The principles of restricted access and need-to-know establishment will be used throughout the life cycle of CIRS. (U)

Procedures

1.18 Requirements for administrative procedures have been established in the areas of: accreditation records and frequency, access to all CIRS information files, protection of security-related software, use of intelligent terminals and personal computers as CIRS terminals, and retention period and media for security audit records. (U)

NETWORK SECURITY

1.19 Initial guidance has been formulated, and appears in Chapter III, relating to the security features of network operations as they relate to the CIRS project. Many aspects of network security, inter-network connections in particular, have not been resolved as yet in their relationships to CIRS. A full set of CIRS requirements for network and inter-network security will be developed as these issues can be resolved. (U)

CONCLUSIONS

1.20 This CIRS security plan presents a set of security requirements designed to meet the increasing security needs of CIRS as the number of hosts and users grows. The mechanisms specified will enable the information owners to control access to their data and assure themselves that the protection mechanisms in place are sufficient to meet Community needs. (U)

(BLANK PAGE)

II. INTRODUCTION

OVERVIEW OF THE CIRS PLAN

2.1 The Community Information Retrieval System (CIRS) plan was adopted by the Information Handling Committee (IHC) in order to provide authorized US intelligence analysts with relevant multi-source information on a timely basis. Several alternatives for implementing CIRS were studied by a working group composed of representatives from major agencies within the Community. The architecture recommended by the working group in their report to the IHC was a confederation of systems in which five information storage and retrieval nodes will be connected and made available to users through two networks. The nodes will be NSA/WINDMILL, FTD/CIRC, NPIC INS, D-SAFE and C-SAFE. Networking will be accomplished using the COINS and DODIIS networks through a gateway between them. (U)

2.2 The CIRS Security Working Group (SWG) has identified eight areas of security in establishing CIRS security requirements. The areas addressed by Automatic Data Processing (ADP) security functions are computer hardware, computer software, and documentation related to these. The criteria for these areas are consistent with the DOD Computer Security Evaluation Center's (CSEC) criteria but have been modified as necessary to address specific CIRS security requirements. Security features provided by environmental and administrative controls are communications security (COMSEC), physical, emanation control (TEMPEST), documentation, personnel, and procedures. (U)

OBJECTIVES OF THIS PLAN

2.3 There are three basic objectives for this security plan. The first is to specify a framework to ensure that the CIRS components maintain a mutually agreeable level of security that will adequately protect the information processed under the CIRS plan. In order to meet this requirement, this plan will specify a uniform set of security criteria which will be adhered to by all CIRS components, which include both hosts and networks. This set of security criteria and requirements is intended to establish a mutually agreeable secure environment for the storage and retrieval of sensitive intelligence information and will assure the owners of such information that access to their data in the CIRS components is controlled in accordance with these security criteria. (U)

2.4 The second objective is to define a time schedule for implementation of the CIRS security plan. The proposed schedule is linked to the dates for bringing the various nodes on line and also takes into account the relative difficulty of implementing tested versions of software to meet the increasing stages of security features specified in Chapter III of this plan. (C)

2.5 The third objective is to furnish planning guidance for bringing an adequate and achievable set of security features on-line within an identified cost range. (U)

IMPLEMENTATION SCHEDULE FOR CIRS SECURITY FEATURES

2.6 The schedule for implementation of the CIRS security plan is divided into three stages. Each of the latter stages builds on the security features present in previous ADP system hardware and software to increase the security measures operational at the CIRS component installations. This increase in security is necessary as more users and more data are put on-line. In

addition this increased level of security is necessary to achieve compartmented operations. (U)

2.7 The environmental and administrative security features listed in Chapter IV of this plan should be implemented fully by each CIRS component when it becomes operational within the CIRS network. Scheduled dates for each of the data storage and retrieval nodes are by the end of the calendar year shown in the table below. (U)

CIRS Implementation Plan
(Jun '84)

Node	Date
NSA/WINDMILL	Late 1985
FTD/CIRC	Early 1986
DIA-SAFE	Late 1986
NPIC INS	Mid 1987
CIA-SAFE	Mid 1990

2.8 The three proposed CIRS security stages will be implemented according to the following schedule:

2.9 Stage I ADP security features are required to be in place by the end of CY 85. The NSA WINDMILL system will be the only operational node in CIRS at this time and COINS will be the primary operational network. A limited number of IDHSC II users will have access to some of the CIRS data bases (if approved by the originators of the data) via the interactive gateway between the COINS and IDHSC II networks. The NSA WINDMILL host and the two networks (COINS and IDHSC) were included in the Stage I security requirements. (U)

Stage I requirements are composed primarily of those specified for discretionary controlled access protection (class C2) by the CSEC, and are given in detail in Chapter III of this plan. For the purposes of Stage I of this security plan, network processors such as the COINS HAS, TAS and NAS

machines are considered to be hosts. DODIIS Network Front Ends (NFEs) implementing a host-dependent Network Label Module will be considered a part of the host to which they are linked. In this stage, all hosts will be operating in the system-high mode and all users will be cleared to the TS/SI/TK level.

25X1

2.10 Stage II features are scheduled to be in place by the end of CY 87 when the CIRS network will have added the D-SAFE, NPIC, and FTD/CIRC nodes and will also use both COINS and DODIIS communication networks linked by a gateway. ADP security features in this stage of CIRS are keyed to the mandatory labeled security protection (class B1) defined by the CSEC. A goal of CIRS is to achieve compartmented mode operations by the end of CY 1988. Until all active hosts are operating in compartmented mode, all users will be cleared to the TS/SI/TK level.

25X1

2.11 Stage III features based on the CSEC's mandatory structured protection (class B2) are required by CIRS FOC in CY 90. At this time, the C-SAFE node will be in place to complete the full CIRS. All hosts will be operating in compartmented mode. All users will be cleared to the TS level and granted access to those compartments for which they have been indoctrinated (e.g., either SI or TK, but not necessarily both).

25X1

IMPLEMENTATION GUIDELINES

2.12 Because of the diversity present in different manufacturers' hardware and software products, it will be the responsibility of each CIRS component to select the implementation method which best meets the security requirements of the three stages defined in this plan.

25X1

III. SECURITY FEATURES PROVIDED BY ADP FUNCTIONS

Security Criteria for ADP Systems

3.1 This chapter addresses three of the eight basic security areas of concern in the CIRS plan. These three are the computer hardware, computer software and (partially) the documentation. Applicable CIRS requirements have been extracted from and are compatible with sections of the DOD publication "DOD Trusted Computer System Evaluation Criteria," (TCSEC) dated 15 August 1983. Other requirements meeting unique CIRS needs have been added. An overview of the basic features in each of the TCSEC divisions and classes is presented in Appendix A of this document. (U)

3.2 The three sections which follow list the specific CIRS security requirements applicable to each of the three CIRS security stages identified in Chapter II. (U)

3.3 The definitions of technical terms used herein are in most cases compatible with those used in the "DOD Trusted Computer System Evaluation Criteria" (see Section VII, Glossary of Terms). There is, however, one important exception to this general rule. In addition to the TCSEC definition of a Trusted Computing Base (TCB), a definition of an Extended Trusted Computing Base (ETCB) has been developed to define the appropriate level of security that is needed to enable a user to access CIRS data bases through and across one or more networks. The control of such access and the mediation and auditing of activity during a session may be implemented by the cooperating TCB's of the host to which a user's terminal is physically attached, the host upon which a data base is resident, and by a host which has been connected to a network and assigned to perform security functions

related to all or a portion of a network's user base. Whereas it is the purpose of this security plan to provide assurance that all of the security related functions will be carried out in accordance with its provisions, the responsibility for the performance of these functions may be distributed between and among more than one computer system in accordance with MOUs or letters of agreement executed between the components and agencies operating computer systems and Offices of Primary Interest (OPI) controlling information to be stored thereon. For this reason the definition of an "Extended Trusted Computing Base (ETCB)," used throughout this plan, is as follows:

Extended Trusted Computing Base (ETCB) - The totality of protection mechanisms within a computer system, or within two or more cooperating computer systems linked by a network or networks--including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system or combination of cooperating computer systems. (U)

3.4 In all sections which follow, there are several other key terms which affect the interpretation of the text. These terms and their definitions are:

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. (U)

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: data bases, documents, records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, network nodes, etc. (U)

Security Level[1] - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information. (U)

Security Label - A piece of information that represents the security level of an object and that describes the sensitivity of the data in the object. Security labels are needed by the TCB to provide the basis for mandatory access control decisions. (U)

Single-Level Device - A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, security labels do not have to be stored with the data being processed. (U)

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, security labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed. (U)

3.5 The CIRS implementation plan approved by the IHC specifies the requirement for all approved by the IHC specifies the requirement for all ADP systems and networks

---

[1]It is noted that, according to the TSEC definition of "security level" which has been adopted for use herein, this term is used to encompass both the traditional hierarchical levels of security classification (Top Secret, Secret, and Confidential) and non-hierarchical security related categories (i.e., compartmentation and caveats including SI, NOFORN, ORCON, LIMDIS, etc.).

identified in the CIRS plan to be operating in the "compartmented mode" as prescribed under DCID 1/16. Therefore, all US intelligence analysts on the ADP system or network must be cleared in accordance with DCID 1/14 for access to at least one SCI compartment. There will be no users accessing CIRS components unless they are cleared to the Top Secret level. 25X1

Stage I - Initial CIRS ADP Security

3.6 The minimum requirements placed on CIRS components during Stage I represent many of the TCSEC criteria dealing with discretionary controlled access protection (class C2) with the additional specification of a minimum length for a system password and the deletion of some documentation requirements. The Office of Primary Interest (OPI) or originator of materials to be processed in accordance with the CIRS plan will specify the controls required via Memoranda of Understanding (MOUs) or letters of agreement. 25X1

Security Policy

Discretionary Access Control

3.7 The TCB shall define and control access between named users and named objects (documents and programs at a minimum in Stage I) in the ADP system. The enforcement mechanisms (e.g., group/public controls, access control lists), if requested by the Office of Primary Interest (OPI), shall allow the OPI to specify and control sharing of those objects by defined groups of individuals. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by CIRS users not already possessing access permission shall only be assigned by the OPI or its designee. 25X1

Object Reuse

3.8 When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the subject can obtain no data from any object for which the subject is not authorized access. (U)

Labeling Human-Readable Output

3.9 The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB. (U)

---

*The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

Accountability

Identification and Authentication

3.10 The ETCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the ETCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The ETCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The ETCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual accessing a CIRS data base. The ETCB shall also provide the capability of associating this identity with all auditable actions taken by that individual. (U)

3.11 If passwords are used as all or part of the authentication mechanism, they shall be a minimum of six alphanumeric characters in length and shall be changed at least once every six months. Passwords shall be distributed by the host responsible for their use in identifying and authenticating the user. (U)

Audit

3.12 The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of CIRS file user-related events: use of identification and authentication mechanisms, introduction of program(s) and/or files and related material into a user's address space, deletion of all or any part of a file from a data base, and actions taken by computer operators and system administrators and/or system security officers. Audit trails shall be maintained to enable tracing the access to or retrieval of any one document by a user. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and

success or failure of the event. For identification/ authentication events the origin of request, either a terminal ID or host ID, shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity. Audit records shall be maintained in either on-line, off-line, or microfiche form for a period of at least one year from their creation (see Chapter IV, Administrative Controls--Procedures). (U)

Assurance

System Architecture

3.13 The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are access controlled and audited according to system requirements. (U)

System Integrity

3.14 Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB. At a minimum, these procedures will be performed at every scheduled preventive maintenance period for the hardware. A series of software test drive modules shall be used to exercise all features of the security software to verify correct operation. These tests shall be performed at least daily. (U)

Security Testing

3.15 Prior to acceptance of security-related software by a CIRS component, a knowledgeable team not a part of the software production staff will test the security mechanisms of the ADP system to determine whether they work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. (U)

Documentation

Security Features Guide

3.16 A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another. (U)

Trusted Facility Manual

3.17 A manual addressed to the ADP system administrator shall present cautions about functions and privileges which should be controlled when running a security facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. In addition, procedures for obtaining and exchanging certification and accreditation data and applicable MOUs with appropriate representative of other organizations identified in the CIRS plan shall be described. (U)

Network Security

ADP Security Aspects

3.18 All ADP equipment used in part or whole as a component of a network carrying CIRS information shall be governed by the same ADP requirements stated for CIRS retrieval nodes. (U)

Security-Related Information Content

3.19 Each packet transmitted as part of a user log-on procedure or session shall contain information which will allow unique identification of the individual user who is logged on and of the host and terminal in use for the session, as soon as such information is available. (U)

3.20 The identification information inserted into a packet by the transmitting entity must be readable by the receiving entity without regard to the transmission path between them. (U)

Stage II - Intermediate CIRS ADP Security

3.21 The ADP security requirements for Phase II of CIRS build on the Phase I requirements. They are essentially those of the TCSEC mandatory labeled security protection (class B1) items with the addition of a minimum length specification on passwords and the deletion of some documentation items. New paragraphs added in this stage will be so designated in the title. New material added to an existing paragraph will be underlined. (U)

Security Policy

Discretionary Access Control

3.22 The TCB shall define and control access between named users and named objects (e.g., documents, files, and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow the OPI to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both. The discretionary access control mechanisms shall, either by explicit user action or by default, provided that objects are protected from unauthorized access. These access controls shall be capable of including or

excluding access to the granularity of a single user. Access permission to an object by CIRS users not already possessing access permission shall only be assigned by the OPI or its designee. (U)

Object Reuse

3.23 When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the subject can obtain no data from any object for which the subject is not authorized access. (U)

Labels (New)

3.24 Sensitivity labels associated with each subject and storage object under its control (e.g., process, file, segment, device) shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB. (U)

Label Integrity (New)

3.25 Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported. (U)

Exportation of Labeled Information (New)

3.26 To ensure that no information shall be exported through a path or to a device not approved to transmit or receive the level of classification (sensitivity) of the

information, the TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device. (U)

Exportation to Multilevel Devices (New)

3.27 When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received. (U)

Exportation to Single-Level Devices (New)

3.28 Single-level I/O devices and single-level communications channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices. (U)

Labeling Human-Readable Output

3.29 The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning

and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB. (U)

Mandatory Access Control (New)

3.30 The TCB shall enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. The following requirements shall hold for all accesses between subjects and objects controlled by the TCB: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in

---

*The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchical categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Note that a subject cannot gain access to an object whose hierarchical security level is higher than the subject's hierarchical session level. (U)

Accountability

Identification and Authentication

3.31 The ETCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the ETCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the ETCB to authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user. The ETCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The ETCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual accessing a CIRS data base. The ETCB shall also provide the capability of associating this identity with all auditable actions taken by that individual. (U)

3.32 If passwords are used as all or part of the authentication mechanism, they shall be a minimum of six alphanumeric characters in length and shall be changed at least once every six months. Passwords shall be distributed by the host responsible for their use in identifying and authenticating the user. (U)

Audit

3.33 The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of CIRS file user-related events: use of identification and authentication mechanisms, introduction of programs and/or files and related material into a user's address space, deletion of all or any part of a file from a data base, and actions taken by computer operators and system administrators and/or system security officers. The TCB shall also be able to audit any override of human-readable output markings. Audit trails shall be maintained to enable tracing the access to or retrieval of any one document by a user. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/ authentication events the origin of request, either a terminal ID or host ID, shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. Audit records shall be maintained in either on-line, off-line, or microfiche form for a period of at least one year from their creation (see Chapter IV, Administrative Controls--Procedures). (U)

Assurance

System Architecture

3.34 The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are access controlled, and audited according to system requirements. (U)

System Integrity

3.35 Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB. At a minimum, these procedures will be performed at every scheduled preventive maintenance period for the hardware. A series of software test drive modules shall be used to exercise all features of the security software to verify correct operation. These tests shall be performed at least daily. (U)

Security Testing

3.36 The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design implementation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB, as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications

initiated by other users. All discovered flaws shall be removed or neutralized and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. (U)

Documentation

Security Features Guide

3.37 A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another. (U)

Trusted Facility Manual

3.38 A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to the security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. In addition, procedures for obtaining and exchanging certification and accreditation data and applicable MOUs with appropriate representative of other organizations identified in the CIRS plan. (U)

Network Security

ADP Security Aspects

3.39 All ADP equipment used in part or whole as a component of a network carrying CIRS information shall be governed by the same ADP requirements stated for CIRS retrieval nodes. (U)

Security-Related Information Content

3.40 Each packet transmitted as part of a user log-on procedure or session shall contain information which will allow unique identification of the individual user who is logged on and of the host and terminal in use for the session, as soon as such information is available. In addition, each packet shall contain the session security level and the packet security level. The level will include both the hierarchical and non-hierarchical designators which apply. (U)

3.41 The security and identification information inserted into a packet by the transmitting entity must be readable by the receiving entity without regard to the transmission path between them. (U)

Stage III - Full Implementation of CIRS ADP Security Features

3.42 The ADP security requirements for Stage III of CIRS continue to build on the security requirements for the first two stages. All previous features are carried forward and new ones are added, primarily in the structuring of the ADP system. The Stage III CIRS requirements meet most of the TCSEC mandatory structured protection (class B2) specifications. (U)

Security Policy

Discretionary Access Control

3.43 The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow the OPI to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both. The discretionary access control mechanisms shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding acces to the granularity of a single user. Access permission to an object by CIRS users not already possessing access permission shall only be assigned by the OPI or its designee. (U)

Object Reuse

3.44 When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the subject can obtain no data from any object for which the subject is not authorized access. (U)

Labels

3.45 Sensitivity labels associated with each ADP system resource (e.g., subject, storage object) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the security level of the data, and all such actions shall be auditable by the TCB. (U)

Label Integrity

3.46 Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported. (U)

Exportation of Labeled Information

3.47 To ensure that no information shall be exported through a path or to a device not approved to transmit or receive the level of classification (sensitivity) of the information, the TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the current security level associated with a single-level communication channel or I/O device. (U)

Exportation to Multilevel Devices

3.48 When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received. (U)

Exportation to Single-Level Devices

3.49 Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process.

However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single security level of information imported or exported via single-level communication channels or I/O devices. (U)

Labeling Human-Readable Output

3.50 The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly* represent the overall sensitivity of the output or that properly* represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly* represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB. (U)

Subject Sensitivity Labels (New)

3.51 The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal

---

*The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to: the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other non-hierarchical categories.

user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label. (U)

Device Labels (New)

3.52 The TCB shall support the assignment of minimum and maximum security levels to all attached physical devices. These security levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located. (U)

Mandatory Access Control

3.53 The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such security levels. The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects: A subject can read an object only if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the object's security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and all the non-hierarchial categories in the subject's security level are included in the non-hierarchical categories in the object's security level. Note that a subject cannot

gain access to an object whose hierarchical security level is higher than the subject's hierarchical session level. (U)

Accountability

Identification and Authentication

3.54 The ETCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the ETCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the ETCB to authenticate the user's identity and to determine the security level and authorizations of subjects that may be created to act on behalf of the individual user. The ETCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The ETCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The ETCB shall also provide the capability of associating this identity with all auditable actions taken by that individual. (U)

3.55 If passwords are used as all or part of the authentication mechanism, they shall be a minimum of six alphanumeric characters in length and shall be changed at least once every six months. Passwords shall be distributed by the host responsible for their use in identifying and authenticating the user. (U)

Trusted Path (New)

3.56 The TCB shall support a trusted communication path between itself and the user for initial login and authentication. Communications via this path shall be initiated exclusively by a user. The communications may be carried by an encrypted

network using trusted ADP systems at its nodes or by dedicated lines under continuous control and approved for use as carriers for CIRS traffic. (U)

Audit

3.57 The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of CIRS file user-related events: use of identification and authentication mechanisms, introduction of programs and/or files and related material into a user's address space, deletion of all or any part of a file from a data base, and actions taken by computer operators and system administrators and/or system security officers. The TCB shall also be able to audit any override of human-readable output markings. Audit trails shall be maintained to enable tracing the access to or retrieval of any one document by a user. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request, either a terminal ID or host ID, shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's security level. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels. Audit records shall be maintained in either on-line, off-line, or microfiche form for a period of at least one year from their creation (see Chapter IV, Administrative Controls--Procedures). (U)

Assurance

System Architecture

3.58 The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. (U)

System Integrity

3.59 Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB. At a minimum, these procedures will be performed at every scheduled preventive maintenance period for the hardware. A series of software test drive modules shall be used to exercise all features of the security software to verify correct operation. These tests shall be performed at least daily. (U)

Trusted Facility Management (New)

3.60 The TCB shall support separate operator and administrator functions. (U)

Security Testing

3.61 The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB, as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found relatively resistant to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification (DTLS). (U)

Design Specification and Verification

3.62 A formal model of the security policy supported by the TCB shall be maintained that is proven consistent with its axioms. A descriptive top- level specification of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface. (U)

Configuration Management (New)

3.63 During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code,

the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. (U)

3.64 Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB. (U)

Documentation

Security Features Guide

3.65 A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another. (U)

Trusted Facility Manual

3.66 A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a

new TCB from source after modification of any modules in the TCB shall be described. In addition, procedures for obtaining and exchanging certification and accreditation data and applicable MOUs with other members of CIRS shall be described. (U)

Network Security

ADP Security Aspects

3.67 All ADP equipment used in part or whole as a component of a network carrying CIRS information shall be governed by the same ADP requirements stated for CIRS retrieval nodes. (U)

Security-Related Information Content

3.68 Each packet transmitted as part of a user log-on procedure or session shall contain information which will allow unique identification of the individual user who is logged on and of the host and terminal in use for the session, as soon as such information is available. In addition, each packet shall contain the session security level and the packet security level. The level will include both the hierarchical and non-hierarchical designators which apply. (U)

3.69 The security and identification information inserted into a packet by the transmitting entity must be readable by the receiving entity without regard to the transmission path between them. (U)

(BLANK PAGE)

IV. SECURITY FEATURES PROVIDED BY ENVIRONMENTAL AND ADMINISTRATIVE CONTROLS

SCOPE

4.1 This section of the CIRS security plan addresses the COMSEC, documentation, personnel, physical, procedures, and TEMPEST considerations in the eight basic security areas covered by this plan. It is important to make these areas an integral part of the full CIRS security effort. These controls should not and cannot be omitted, because they provide security in depth to cover temporary system failures or data of high sensitivity, alternate security when planned hardware or software security features are under development, and fulfill mandatory requirements within the traditional areas of security. (U)

ENVIRONMENTAL CONTROLS

Communications Security (COMSEC)

4.2 COMSEC requirements for CIRS will be as follows:

- Communications links between all peripheral devices connecting them to other peripheral devices, to CIRS user terminals, or to CIRS hosts shall be accredited for the transmittal of TS/SCI.
- CIRS component communications networks shall include a network control station capable of furnishing to the COINS or DODIIS (as appropriate) Network Security Officer (NSO) such information as is required to monitor the security aspects of their respective network operations. (U)

Physical Security

4.3 The CIRS host sites, networks, and communications links, along with their personnel and environs, shall comply with "US Intelligence Community Standards for Sensitive Compartmented Information Facilities," dated 13 April 1981. (U)

4.4 When physical access to a terminal authorized for CIRS use cannot be restricted to those having clearances for all CIRS compartments and CIRS need-to-know access approvals, at least two independent identity verification mechanisms (e.g., password and badge reader or password and fingerprint scan) should be used before permitting a person to log on. (U)

Emanations Control/TEMPEST

4.5 Each CIRS component and communication link processing or carrying CIRS information in clear-text form must be in compliance with all applicable sections of NACSIM 5100A. If critical cryptographic functions are being performed, the KAG 30 emanation control standards must be met. Methods used to meet these standards must be in accordance with DOD Directive S-5200.19. (U)

ADMINISTRATIVE CONTROLS

Documentation

4.6 Each CIRS component shall prepare a system security plan for approval by the appropriate security and system approving authorities. This plan brings together all applicable regulations and special procedures into a single source document for the system. The document will be reviewed and revised as appropriate whenever hardware, software, configuration or usage changes are made which have an impact on security. (U)

Central Point of Contact for Security-Related Information

4.7 The IHC member or other designated official representing each Intelligence Community organization acting as executive agent for the operation of a CIRS component shall, on an annual basis, certify to the IHC that each CIRS component for which their organization is responsible is in compliance with the minimum security criteria contained in the CIRS security plan. In the event that any CIRS component is operating under a waiver of any of the minimum security criteria, such certification shall also include notice of the terms and conditions of any such waiver. In addition, the same responsible officials shall also certify that each such CIRS component is in compliance with any unique security requirements or information handling restrictions contained in any agreements entered into between their organization and the various OPIs concerning data being processed under the CIRS plan. These certifications will be maintained by the IHC staff and may be made available to the IHC members representing the OPIs for data being processed on systems which are the subject of any such certification under such terms and conditions as may be stipulated in each such certificate. The IHC staff will also act as a coordination point, if needed, to make available CIRS security related audit data maintained by CIRS components to the extent required to construct a complete audit of CIRS security related events down to the level of an individual user. (U)

Personnel

4.8 The system, its personnel, and environs shall comply as appropriate with "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," dated 1 September 1983 (still known as DCID 1/14). In addition priority shall be given to the

reinvestigation of all personnel employed in key security sensitive positions (e.g., security officer, all persons granted access privileges to the TCB, all systems software and hardware maintenance personnel, and all persons responsible for COMSEC equipment or key maintenance). In no case shall the 5-year limit on reinvestigations prescribed in DCID 1/14 be exceeded. In all departments and agencies with policies sanctioning the use of the polygraph for personnel security purposes, the following practices shall be complied with: (a) the polygraph shall be utilized as a part of the investigation of personnel being initially employed to fill any key security sensitive position, and (b) personnel who have previously not been polygraphed as a part of their original investigation and who may subsequently be assigned to any key security sensitive position shall be the subject of a reinvestigation utilizing the polygraph at the earliest practicable date. (U)

4.9 All CIRS users shall be cleared to TOP SECRET and clearable for SCI access. All users accessing hosts operating in system-high mode shall be cleared for all categories of SCI contained in the sytem. All users accessing hosts operating in compartmented mode shall be cleared for all compartments to which they have been granted access. There shall be no access by foreign nationals to any files included in the CIRS plan. (U)

4.10 All routine maintenance functions performed by hardware and software specialists must be performed by personnel who have been investigated and approved for access at the highest level of information the system is accredited to process. They shall be authorized to access only the resources necessary to perform their maintenance tasks. (U)

Procedures

4.11 The following procedures shall be observed in relation to the accreditation of all CIRS components:

- Each CIRS component shall maintain records showing the current accreditation status, the classification(s) and compartment(s) of intelligence data contained in the system, and the range of clearance characteristics of the system users.
- Each CIRS component shall comply with the protection mechanisms identified in "Security Policy for Sensitive Compartmented Information," dated 28 June 1982 (formerly DCID 1/19); "Security Policy Manual for SCI Control Systems, dated 18 June 1982; and with "Security Policy on Intelligence Information in Automated Systems and Networks," dated 4 January 1983 (formerly DCID 1/16).
- Each CIRS component shall be accredited for operations on a yearly basis by an appropriate authority.
- Each IHC member representing an organization responsible for operating a CIRS component (or his designated authority) shall certify on an annual basis that the systems and networks operated by their respective agencies in accordance with the CIRS implementation plan are in compliance with the minimum requirements identified in the CIRS security plan. (U)

4.12 The following procedures shall be observed in relation to access to the intelligence data included in any CIRS file located on any of the CIRS hosts:

- Unencrypted dial-up communications lines shall not be connected to any of the CIRS component systems which has CIRS information on-line.

- o Access by a subject (i.e., person, process, or device) to an object (e.g., record, file, program, printer, or network node) shall be controlled based on access authorization approvals specified by an approval authority which will usually be the OPI for the data involved. (U)

This approval authority shall be specified in the certification process and such authority shall be clearly identified. (U)

4.13 The following procedures deal with the protection of security-related software:

- o All security-related software (e.g., password files, access control processes, and auditing functions) used during classified processing shall be continuously protected commensurate with the requirements for the highest level and most restrictive category of classified information processed by the system, even when the software is not in the system, until the software is no longer used during classified processing. Such security-related software, whether obtained from outside sources or developed within the system facility, shall be protected from the earliest feasible time that it is in the custody and control of the system concerned.
- o Duties and responsibilities of the system support staff shall be allocated so as to prevent one person from having complete control of the system security software and its operation. Procedures shall be established for each system to segregate associated programming and system operation functions. As far as is practicable, personnel should be prohibited from both programming and operating the security features of a given system. (U)

4.14 The following procedures address removable storage media and the use of CIRS terminals capable of information storage:

- Removable information storage media used with computers and other automated information handling systems shall bear external markings clearly indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination limitations. Examples of such media include magnetic tapes, hard and soft (floppy) disks and paper tape.
- Intelligent terminals and personal computers may be used as CIRS terminals if the cognizant authority at the terminal location certifies that all personnel using such terminals are specially briefed as to the unique security problems involved and that security control measures appropriate to their use are in place. (U)

4.15 Audit files for security-related events occurring within CIRS shall be retained for a period of one year. The retention medium or media may be chosen to suit the site operations methods. Individual records relating to a specific security investigation may be requested for indefinite retention. (U)

(BLANK PAGE)

V. IMPLEMENTATION TASKS AND RESOURCES

COMPONENT ENHANCEMENTS

5.1 (TO BE WRITTEN) [redacted] 25X1

RESOURCE ESTIMATES

5.2 (TO BE PROVIDED WHEN DATA IS AVAILABLE) [redacted] 25X1

MILESTONES

5.3 The following major milestones for the implementation of the three stages of the CIRS Security Plan are scheduled for specific calendar year quarters. Further development and refinement of implementation schedules by the individual CIRS component organizations will expand and may modify this list.

Date	Milestone
1984, 4Q	C- and D-SAFE accept delivery 2 of software, containing initial security features.
1985, 1Q	D-SAFE accepts delivery 3 software, completing features of single user login and full audit trail recording.
2Q	C-SAFE accepts delivery 3 software, as above.
4Q	COINS/DODIIS gateway IOC.
4Q	NSA provides first full service from the WINDMILL machine under Stage I security requirements.

1986, 2Q	FTD/CIRC joins CIRS under Stage I security requirements. Operations are limited initially to 8 hours per day.
4Q	COINS/DODIIS gateway FOC in compartmented mode.
4Q	CIRS IOC.
4Q	D-SAFE joins CIRS under State I security requirements.
1987, 4Q	NSA/WINDMILL completes upgrade to Stage II security requirements.
4Q	FTD/CIRC completes upgrade to Stage II security requirements and begins full-time service to CIRS users.
4Q	NPIC INS joins CIRS under Stage II security requirements.
1988, 4Q	Stage III compartmented mode operations begin at NSA/WINDMILL, FTD/CIRC, D-SAFE, and NPIC INS.
1990, 4Q	C-SAFE joins CIRS under Stage III security requirements.
25X1 4Q	CIRS FOC.

VI. REFERENCES

1. DCID 1/7, Control of Dissemination of Intelligence Information, 4 May 1981

2. DCID 1/4, Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, 1 September 1983

3. DCID 1/16, Security of Foreign Intelligence in Automated Data Processing Systems and Networks, 6 June 1978

4. DODD 5200.1-R, Information Security Program Regulation, August 1982

5. DIDD C-5200.5, Communications Security (COMSEC) [redacted], (Confidential), 15 April 1971 25X1

6. DODD S-5200.19, Control of Compromising Emanations [redacted] (Secret), 10 February 1968 25X1

7. DODD 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, revised April 1978

8. DODD 5200.28-M, ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, revised June 1979

9. DOD CSC-STD-001-83, Department of Defense Trusted Computer System Evaluation Criteria, 15 August 1983

10. DIAM 50-4, Security of Compartmented Computer Operations [redacted] (Confidential), 24 June 1980 25X1

11. NBS FIPS Publication, Password Usage Standard (Draft)

(BLANK PAGE)

VII. ACRONYMS AND DEFINITIONS OF TERMS

ACRONYMS

ADP	Automatic Data Processing
CIRC	Central Information Reference and Control
CIRS	Community Information Retrieval System
COINS	Community On-Line Information System
COMSEC	Communications Security
CSEC	Computer Security Evaluation Committee
CY	Calendar Year
DCID	Director of Central Intelligence Directive
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DTLS	Descriptive Top Level Specifications
ETCB	Extended Trusted Computing Base
FOC	Final Operational Capability
FTD	Foreign Technology Division
HAS	Host Access System
ID	Identifier
IDHSC	Intelligence Data Handling System Communications
IHC	Information Handling Committee
INS	Improved NPIC System
I/O	Input/Output
IOC	Initial Operational Capability
LIMDIS	Limited Distribution
MOU	Memorandum of Understanding
NAS	Network Access System
NFE	Network Front End
NOFORN	No Foreign
NPIC	National Photographic Interpretation Center
NSA	National Security Agency
NSO	Network Security Officer
OPI	Office of Primary Interest
ORCON	Originator Controlled
SAFE	Support for the Analyst File Environment
SCI	Sensitive Compartmented Information
SI	An SCI Compartment
SWG	Security Working Group
TAS	Terminal Access System
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Center
TEMPEST	Electromagnetic Emanations Control Program
TK	An SCI Compartment
TS	Top Secret
US	United States

DEFINITIONS

Access - A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Accreditation - The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

Audit Trail - A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

Authenticate - To establish the validity of a claimed identity.

Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Bandwidth - A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second.

Certification - The technical evaluation of a system's security features, made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Channel - An information transfer path within a system. May also refer to the mechanism by which the path is effected.

Covert Channel - A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also: Covert Storage Channel.

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Data - Information with a specific physical representation.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Descriptive Top-Level Specification (DTLS) - A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Domain - The set of objects that a subject has the ability to access.

Dominate - Security level S_1 is said to dominate security level S_2 if the hierarchical classification of S_1 is greater than or equal to that of S_2 and the non-hierarchical categories of S_1 include all those of S_2 as a subset.

Extended Trusted Computing Base (ETCB) - The totality of protection mechanisms within a computer system, or within two or more cooperating computer systems linked by a network or networks--including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system or combination of cooperating computer systems.

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Low Water Mark - Of two or more security levels, the least of the hierarchical classifications, and the set of intersection of the non-hierarchical categories.

Mandatory Access Control - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, security labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: data bases, documents, records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, network nodes, etc.

Object Reuse - The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media must contain no residual data from the previously contained object(s).

Output - Information that has been exported by a TCB.

Password - A private character string that is used to authenticate an identity.

Process - A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

Read Access - Permission to read information.

Security Label - A piece of information that represents the security level of an object and that describes the sensitivity of the data in the object. Security labels are used by the TCB as the basis for mandatory access control decisions.

Security Level - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model - An information presentation of a formal security policy model.

Security Testing - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Verification.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Session Security Level - The security level of a session is the low water mark of the security levels of: the user, the terminal, a level specified by the user, and the system from which the session originates.

Single-Level Device - A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, security labels do not have to be stored with the data being processed.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

Subject Security Level - A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the session security level. This interpretation clarifies the least upper bound of the subject security level in cases where either, the user security level dominates the terminal security level, the user security level dominates the system security level, or the user desires to lower his maximum security level for a session.

TEMPEST - The study and control of spurious electronic signals emitted from ADP equipment.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system, or within two or more cooperating computer systems linked by a network or networks--including hardware, firmware, and software--the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides user services required for a trusted computer system or combination of cooperating computer systems.

Trusted Path - A mechanism by which a person at a terminal or another TCB can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software.

User - Any person who interacts directly with a computer system.

Verification - The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated.

Write - A fundamental operation that results only in the flow of information from a subject to an object.

Write Access - Permission to write an object.

(BLANK PAGE)

Declassified in Part - Sanitized Copy Approved for Release 2012/08/21 : CIA-RDP95-00972R000100100004-6

APPENDIX A - TCSEC COMPUTER SECURITY DIVISIONS

The Computer Security Evaluation Center has established four major divisions of computer security criteria describing systems ranging from those with essentially no security features to those containing features offering high levels of protection for the information they contain and process. The CIRS requirements do not refer to the D or A divisions described below, but these are included for completeness. Likewise, Class B3 is not addressed in the CIRS requirements.

The four divisions and their classes are:

- o D: Minimal Protection

  This division contains only one class. It is reserved for those systems which have been evaluated, but failed to meet the requirements for a higher class.

- o C: Discretionary Protection

  The two classes in this division provide increasing levels of discretionary (need-to-know) protection and for the accountability of subjects and the actions they initiate.

  - C1: Discretionary Security Protection

    This class provides separation of users and data to protect project or private data and keep other users from accidentally reading or destroying their data. The environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

- C2: Controlled Access Protection

  Systems in this class enforce a more finely grained access control than C1 systems, making users individually accountable for their actions.

o B: Mandatory Protection

  The controls applied in this class are implemented through applying sensitivity labels to the major data objects, preserving their integrity and enforcing a set of mandatory access controls through the use of these labels.

- B1: Labeled Security Protection

  Systems in this class must contain all features required for Class C2. In addition, data labeling and mandatory access control over named subjects and objects must be present as well as accurate labeling of exported information.

- B2: Structured Protection

  These requirements extend the B1 controls to include all subjects and objects in the ADP system. Covert channels are addressed. Formal definition of the security policy model used, as well as documentation of and configuration control over the ADP system is required.

- B3: Security Domains

  Systems in this class build on the B2 requirements, but are required to be more tightly designed, documented and tested. In addition a number of operational support features are specified.

o A: Verified Protection

  This division adds complete formal design and verification methods to the operational requirements of Class B3. Extensive documentation and testing is also specified.

(BLANK PAGE)