SECRET

CENTRAL INTELLIGENCE AGENCY (CIA) COMMUNITY ON LINE INTELLIGENCE SYSTEM (COINS) SECURITY PROCEDURES

3 October 1968

SECRET

CENTRAL INTELLIGENCE AGENCY (CIA) COMMUNITY ON LINE INTELLIGENCE SYSTEM (COINS) SECURITY PROCEDURES

TABLE OF CONTENTS

ATTACHMENTS

A. Time Sharing System IBM 360/50 Hardware Configuration

B. Core Layout

C. User Partitions and Associated Terminals

D. Example of LOGON Procedure

E. Flow Diagram of Procedures Required to Retrieve or Modify Data from a Remote Terminal

F. Security Standards for Conduit Installation

3 October 1968

Central Intelligence Agency (CIA) Community
On Line Intelligence System (COINS)
Security Procedures

I. Introduction

1. CIA COINS security procedures consist of a combination of physical security, communications security, and computer software (programming) techniques which are designed to operate the CIA portion of the COINS network at the Top Secret, Comint level compatible with security controls applicable to that compartmentation level. The adoption of a combination of procedures provides some safeguards to maintain security control even if, for some unanticipated reason, one aspect of the security structure momentarily fails, i.e., if an unauthorized individual was able to obtain access to a CIA COINS terminal, he would not be able to use it unless he had been trained in the query procedure and had also been given access to several passwords required to make the system available.

2. In general, however, the security procedures developed for the CIA COINS system are designed to operate the system in a non-hostile environment, i.e., the procedures are based on the following assumptions:

a. Employees without a need-to-know will be denied access to the system.

b. Cleared employees will not actively attempt to access non-COINS files

c. Users will report receipt of data which is not responsive to a COINS query (e.g., accidental spillage of non-COINS data).

Next 2 Page(s) In Document Exempt

Approved For Release 2005/08/18 : CIA-RDP80B01139A000100100012-9

Operating System (OS/360). Although there were a number of advantages in adopting OS/360, there were also some serious drawbacks, primarily in the security area. OS is a generalized operating system which was designed with little or no regard for security safeguards in a multitasking on-line environment.

b. The approach followed then, in developing the Time Shared System was:

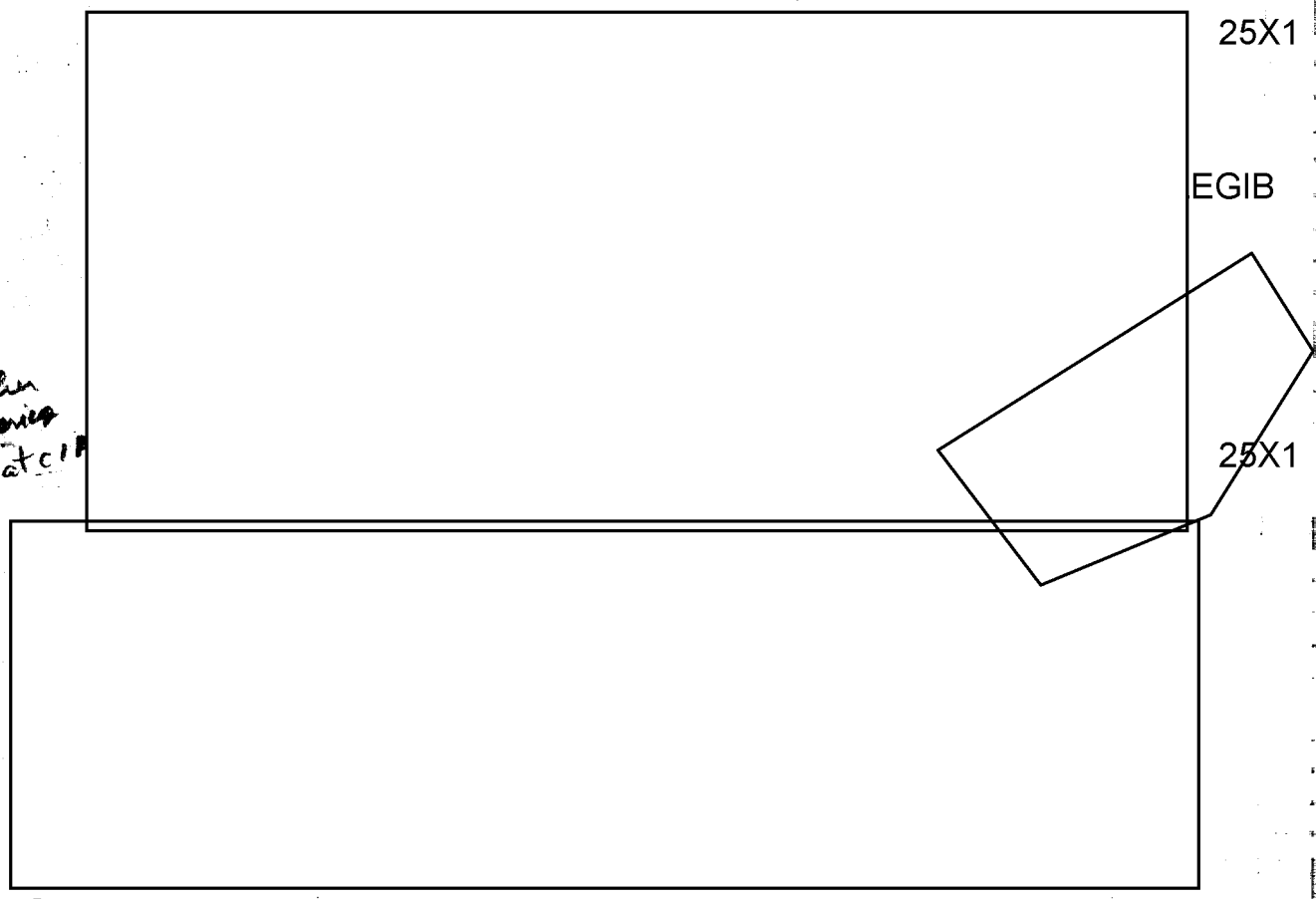
1) to integrate as much software protection as possible in the basic design and circumvent known OS/360 deficiencies, and

2) to prevent users of the system from interfacing directly with the various program modules of OS/360 and, in particular, prohibit them from directly accessing any I/O devices.

c. The software security of this system, as currently implemented, is based on the premise that all users interact, via remote devices, with debugged systems programs and have no direct interface with any of the OS/360 modules. These programs are written and implemented by OCS programmers.

d. Assuming that all these programs are error free, there would be no fear of the system being compromised and consequently, no need for any elaborate software safeguards. However, when operating in a time sharing environment, it is not possible to test all program paths or combinations thereof and hence, it is impossible to guarantee that these programs would be 100% reliable at all times. Therefore, a number of other software security safeguards have been built into the system to significantly reduce the probability of a security compromise and to give us more control in order to guarantee a more secure system. Below in sections 2-7

is an explanation of the additional security safeguards that have been incorporated.



How are other agency queries handled etc?

2. Partitioned System

In the Time Shared System, memory is partitioned such that each remote user is allocated a fixed block of core associated with a specific terminal. Conceptually, all user partitions can be visualized as separate computers that share a main processor, re-entrant routines, I/O buffers, and direct access storage devices. The partitioned core allocated to a remote terminal is not accessible by other terminals. See attachment B, 'Core layout - Model 50' and attachment C, 'Time Shared Users Partitions and Associated Terminals.'

3. Time Sharing Monitor

a. The Time Sharing Monitor (TSMON) is a problem program designed to run in the top partition of a two partition multiprogrammed Operating System. TSMON replaces interrupt locations of OS/360 in order to gain control of the system environment allowing implementation of an equal-priority, time-slicing, multiple partition, multiprogramming system utilizing Operating System facilities.

b. During the initialization phase of TSMON operations, user partitions are defined, allocated core storage, and linked to a specific remote terminal; re-entrant routines are loaded; task control blocks are generated for each partition; and the 'LOGON' program is loaded into all user partitions to control those tasks until the user has successfully logged on. The system clock is set to a time slice interval which insures a reasonable response time for all tasks. When the initialization phase is complete, control is passed to the task dispatcher which passes control successively to user tasks which are active.

4. Logon

same Q 6.

a. This procedure applies only to the internal CIA system - it is not applicable to a query originating from another agency.

b. To gain access to the computer system, a user from a CIA terminal initiates a 'LOGON' procedure. Name, office designation, telephone number, and the system password must be supplied. Only two attempts are allowed to enter the password correctly. If unsuccessful, the entire 'LOGON' procedure is reinitialized. The system password is changed periodically by the system operator.

?

c. After the system password has been internally verified, the program then logs the following information on the operator's console:

1) User's terminal #

2) Date

3) Time of day

4) User's name

5) User's office designation

6) User's telephone number

The system operator must validate this logon request from his console before the user can proceed, if the user is unauthorized to use the terminal, the operator can cancel the request.

25X1

e. It is the responsibility of the user to log off his terminal, but, in addition, the operator has the capability to log off any

terminal from his console. The LOGOFF program prints the following information on the operator's terminal:

1) Terminal # logged off

2) Date

3) Time of day

See attachment D, for an example of 'LOGON' procedure.

5. System Log

Time sharing programs record pertinent information in a data set known as the 'System Log.' Such information as log-on attempts, password failures, program loading, and data set initialization are recorded and may be displayed at the operators terminal or listed on the printer. Standard information within each log entry includes: time, date, user, and terminal.

6. Data Set Protection

a. This procedure applies only to the internal CIA system - it is not applicable to a query originating from another agency.

b. All classified data sets within the system are password protected for both read and write access. Whenever a data set is specified, a password is requested, verified, and the following information is logged on the operator's console:

1) User

2) User's terminal #

3) Date

4) Time of day

5) Directory name

6) Data set name

7) Program in control

An optional feature of the system, when requested, requires operator intervention before the data set can be opened and processing continues. For a flow diagram of procedures required to retrieve or modify data from a remote terminal, see attachment E. 25X1

[redacted]

d. To insure the security of data previously written on scratch storage, all free blocks on direct access storage media will be written over before any new allocation is made.

25X1

[redacted]

Next 2 Page(s) In Document Exempt

Approved For Release 2005/08/18 : CIA-RDP80B01139A000100100012-9

ATTACHMENT 'B'

CORE LAYOUT

	P1	PØ								
MFT Nucleus (OS/360)	BATCH PARTITION	TSMON	TP PARTITION	DISK PARTITION	USER PARTITION #1	USER PARTITION #N	Work Area (Access Method)	Task Control Block	I/O Buffers (PAM)	Link Pack Area

MFT Nucleus - Operating System - Resident monitor Multi-programming fixed # of tasks

P_1 Batch Partition - runs normal OS/360 jobs

$P_Ø$ TSMON - Time sharing monitor

TP - Teleprocessing partition - controls polling of all remote terminals

DISK Partition - initiates all I/O for Direct Access Devices
(NOTE: The TP and DISK partitions require no core but are specified as partitions so they may be allocated a quantum of time the same as all user partitions. Programs that are run during this time are located in the Link Pack Area.

USER Partitions
Work Area used by access methods - work space not shared but allocated to specific partitions
Task Control Block - control blocks for all TS partitions - serves as commutation list for TSMON.
I/O Buffers - buffer pool used by Paging Access Method which services all TS User Partitions.
Link Pack Area - contains all common re-entrant routines.

Next 4 Page(s) In Document Exempt

Approved For Release 2005/08/18 : CIA-RDP80B01139A000100100012-9