☐ UNCLASSIFIED ☐ INTERNAL USE ONLY ☐ CONFIDENTIAL ☒ SECRET

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Minimum Security Requirements for Multi-Level Computer Systems

FROM: CIA Member Rm 4E38
USIB Computer Security Subcommittee

EXTENSION | NO.

DATE: 27 April 1970

25X1

25X1

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. D/NPIC thru C/DDI Planning Staff 2F-24 Hq.	27 Apr	28 Apr	mwk	DEADLINE: 6 May 1970
2.				
3.				
4. O/DIR 6N212				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Declass Review by NIMA/DOD

FORM 3-62 610 USE PREVIOUS EDITIONS ☒ SECRET ☐ CONFIDENTIAL ☐ INTERNAL USE ONLY ☐ UNCLASSIFIED

27 April 1970

MEMORANDUM FOR: D/OCS
D/CRS
D/OC
D/ORD
DDP, Operational Services Systems Group
D/NPIC Thru C/DDI Planning Staff

SUBJECT : Minimum Security Requirements for Multi-Level Computer Systems

1. The Computer Security Subcommittee has been tasked by the full Security Committee to develop minimum security requirements for multi-level operation of resource-sharing computer systems. In order to obtain optimum input from all possible sources, the attached first draft of these requirements is being widely distributed throughout the CIA and the other USIB Member Agencies.

2. It is requested that the appropriate members of your staff be asked to review and submit written comments on this draft. For example Section IV, Definitions, may generate questions regarding the correctness of the definitions or the completeness of the list itself. There also may be some feeling that a section should be added to include additional or optional features to enhance system security. Specific comments on these aspects would be appreciated.

3. Since the Intelligence Board Security Committee has placed a short deadline date for completion of this project, it is therefore necessary that replies be forwarded to the undersigned no later than 6 May 1970.

Signed

[redacted]

25X1

CIA Member
USIB Computer Security Subcommittee

Attachment

DRAFT I
23 APR 1970

MINIMUM SECURITY REQUIREMENTS FOR MULTI-LEVEL OPERATION OF RESOURCE-SHARING COMPUTER SYSTEMS

I. Purpose:

This paper defines basic USIB policy concerning the security aspects of utilizing remotely-accessed resource-sharing computer systems for the concurrent processing and/or storage of classified information of different security levels and/or certain special access control categories. It specifies the conditions under which such systems may be operated in a multi-security level mode and prescribes minimum security requirements for the operation of such systems. Further, it assigns the responsibility for the security testing and accreditation of such systems to individual USIB members.

II. Background:

A. In view of the high cost of modern computing hardware and of developing the accompanying system software, and because of the trend toward the centralization of computing capabilities, sound management of ADP resources dictates their use in as cost-effective manner as possible within the constraints of good security practices. This is especially true of contemporary systems with large storage capacity, multitasking capabilities, and accessibility not only in the computer center but also from terminals remotely located from the computer itself.

B. While technological advances in the state-of-the-art as well as cost and other operational factors have contributed to the trend toward centralized computer installations with large on-line data bases and a diversified spectrum of users, this centralization when applied to a classified environment has compounded already complex security problems identified in the use of modern information processing equipment and techniques.

C. Fundamental to the exercise of sound security practices in the USIB community has been the concept of "need-to-know" and its accompanying control procedures for the dissemination of classified

25X1

information. This concept has been carried out by compartmenting the distribution of official data in a manner commensurate with its sensitivity. Such compartmentation when applied to the more sensitive materials is more rigidly and usually more formally required by appropriate directives.

D. The traditional "Need-to-Know" concept can become especially vulnerable in the processing of classified data by modern resource-sharing computer systems with their remote accessibility to large numbers of users, unless appropriate measures are taken to provide adequate control of the data resident in these systems. The compartmentation problem in this environment is created by operational requirements to process different groups or levels of data in the system concurrently and by security demands to maintain separation of the levels at output stations.

E. In the case of formally compartmented data this separation is a problem of matching the clearance and access approval level of a given user and terminal with the classification and dissemination restrictions of the data. More broadly, the security problem is one of preventing a user from intentionally accessing groups of data for which he is not authorized and of ensuring against the unintentional spillage from the system of data to a user or terminal not approved to receive such data.

25X1

25X1

Potentially, the spectrum of clearance levels can cover the range from none to Top Secret to several special access approvals; the corresponding data classifications and dissemination restrictions can run from unclassified through the hierarchical national levels (Confidential, Secret, Top Secret) to several special access categories.

25X1

25X1 [redacted]

III. Scope:

A. The provisions of this paper are applicable to the utilization within the USIB community of resource-sharing remotely-accessed computer systems for the concurrent processing and/or storage of classified information of different security levels including SI, TKH,

25X1 and [redacted] compartmented intelligence data. Its provisions are equally applicable to contractor and non-USIB government systems handling intelligence data in a multi-security level mode of operation.

B. Since the paper prescribes minimum security requirements for multi-level operation of resource-sharing computer systems, it does not inhibit an individual agency from requiring additional protection features or procedures in the multi-level operation of its own systems.

25X1 [redacted]

IV. Definitions:

A. Resource-Sharing Remotely Accessed Computer Systems: Modern information processing computer systems having a capability for multi-processing, i.e., concurrently handling more than one job utilizing time-slicing or other techniques, which are accessible for input or output purposes not only in the immediate area of the computer center but also from terminals located at a distance from the central processing unit which may vary from several feet to several thousand miles.

B. Multi-Security Level Mode of Operation: Utilization of resource-sharing computer systems for the concurrent processing of two or more tasks whose security classification or access control levels are different and where system access from local or remote terminals is afforded personnel holding different levels of security clearances or access approvals.

C. Benign Environment: A resource-sharing computer system which is secured and controlled from a physical, technical, and personnel security standpoint at the minimum requirements for the processing and handling of Top Secret material; in such an environment all personnel accessing the system holding a minimum of a final Top Secret clearance; all communications links are protected and approved for the transmission

of Top Secret data; the computer center and the areas housing all remote terminals on the system are afforded physical security protection as required for Top Secret material.

D. System Certification: Endorsement of a given computer system that it meets all security requirements and established standards for its utilization in processing classified information of a specific level.

E. System Accreditation: Approval by responsible authority for a given computer system to be utilized for the processing of classified material of a given level or levels, e.g., to permit its use in a multi-security mode of operation covering classified material through Top Secret including certain groups of compartmented data.

F. System Security Officer: The individual assigned responsibility to monitor the security aspects of the utilization of a given computer system.

V. Policy:

A. The current state-of-the-art in computing technology does not provide to resource-sharing multi-level systems having on-line remote access capabilities any guarantee against deliberate unauthorized intrusion into system files from and against unintentional spillage of system data to remotely located ancillary devices. Further, the state-of-the-art cannot even afford sufficient safeguards against intrusion and spillage to permit on a calculated risk basis the operation of such a system in a multi-security level mode covering the full spectrum of clearance/classification levels existing in the USIB environment.

B. However, when cogent cost and operational factors deem it necessary, a sufficient degree of security can be achieved to allow the operation of remotely accessed resource-sharing systems on a multi-security level basis if such systems are limited to a benign environment as defined above and provided that at least the minimum protection features and procedures of this paper are made a part of system operation. The features outlined represent basic requirements; the use of additional system security procedures and techniques are to be encouraged.

C. Judicious implementation of the basic requirements outlined in this paper suggests a need to test and evaluate their effectiveness when applied to a specific system as a basis for multi-level

certification or accreditation of that system. The Senior Intelligence Officer in each USIB organization has the responsibility for conducting such testing and evaluation and has the authority to certify that specific systems meet the requirements specified by this paper as a means for initial multi-level accreditation. This accreditation should be subject to periodic review of the security of system operation and on the occasion of major hardware and/or software modification to retesting, reevaluation, and recertification procedures as deemed appropriate.

VI. Minimum Requirements:

A. Personnel Security and System Access Control:

1. Computer Center: Access to the area housing the computer center must be limited to personnel holding Top Secret clearances and approved for access to all compartmented data being processed by the system. Where deemed necessary by cognizant authority area access logs should be maintained as a record of who enters computer center area and when.

2. Remote Terminal Sites: Access to the immediate area of a remote terminal should be limited to personnel holding a Top Secret clearance and access approved for compartmented data designed for input and output at that terminal. Direct use of remote terminals should be controlled by a monitor assigned responsibility for the security of that remote device.

B. Physical Security Protection:

1. Computer Center: Physical security requirements for the temporary or permanent storage of classified material will be followed in determining the degree of protection needed for the computer center. Since the system will probably be processing information classified through Top Secret and including compartmented data, it is envisioned that secure area or vault construction requirements will be necessary. It must be remembered that such

requirements must be defined in terms of the highest classification level or most demanding compartmented information standards involved in system operations.

2. Remote Terminal Areas: Physical security protection of a given remote terminal area must be in accordance with the requirements specified for the level(s) of data designed for input or output at that terminal. In the case of compartmented data this means approval of the site at least as a working area for the compartmented data involved.

C. Communications Security: The communications links between remote terminals and the computer will be secured in a manner appropriate for the transmission of Top Secret codeword material. Regardless of any limitation on the classification level of material being transmitted on a given link. Protection of these links may be provided by encryption or special physical security isolation of cleartext distribution lines within controlled areas.

D. Emanations Security Aspects: The vulnerability of system operations through electromagnetic radiation will be considered in the process of system certification for multi-level operations. Evaluation of the on-site risks at the computer center and in the remote terminal areas will be accomplished by cognizant authority within the appropriate

25X1

agency. Cleartext distribution lines to terminals should be afforded at least the protection of conduit installation.

E. Software Controls: Compartmented data of different security levels being stored and/or processed in the system may be based on the following factors and procedures. These factors are outlined as minimum requirements and must be present in any system operating in a multi-security level mode.

1. Security Flags: All data and programs stored or processed by the system will be identified as to appropriate security classification, special category controls and codewords, dissemination caveats, and downgrading grouping. This identification must be insured not only internally for the data but also upon output regardless of the output medium. The question of to what level data should be so identified should depend upon the utilization of the file involved. It is foreseen that in many cases these security flags will be carried at the file level only; but in some case there may be a necessity to maintain such identification at the record or even field level.

The purpose of identifying data in this manner is not only to provide the security level of the data to a user who might

25X1

25X1

25X1

assimilate its content in the preparation of a new document, but also to indicate to the user that upon receipt in hard copy of such material he must implement required dissemination control numbers. Further identification of compartmented material may serve as an alert mechanism to personnel who accidentally receives such data when they are not access approved for it.

2. User Identification/Authentication: The system must have a software (or software/hardware) based user-oriented identification and/or authentication mechanism. This feature should be a part of the log-on routine of the system whereby a person attempting to access the system from a remote terminal cannot gain access without identifying himself and providing a unique authorized code recognizable by the system for the purpose of insuring that he is the person so identified.

The purpose of this user/oriented identification/authenticated mechanism is based on the need to assign security responsibility to a specific individual when a given terminal is open to the system. Terminal oriented identification mechanisms are considered inadequate in that the security responsibility in a sense is assigned to a portion of the hardware.

25X1

25X1

3. Access Control: Each system will have an access control software feature to limit user entry to selected files, groups of files, data, or programs, and if necessary to control read and/or write authority. This access control protection may be exercised by the use of keywords or user access listing techniques; however it should be recognized that keyword utilization provides a significantly higher degree of security to the system.

4. Audit Trail Capability: Each system will have a capability of maintaining in as secure a fashion as possible an audit trail which will serve as a log of system transactions including a complete listing of personnel gaining access to the system, the files they access, the date and time. In addition the log should reflect a complete record of invalid log-on attempts and [redacted] system security violations.

The audit trail will be regularly reviewed by the system security officer and appropriate portions thereof will be reviewed by terminal monitors.

The audit trail serves not only as a check against individual system use for security purposes and an inspection of invalid log-on attempts or breeches of access limitations, but it also remains as

25X1

a record for potential subsequent review in the event that security flaws in system operations are later identified.

5. The above listed software features, viz. security flagging, user authentication, access limitation, and audit trail capabilities, will be contained in an appropriately determined executive portion of the system software and should be modifiable only under the control of the system security officer. Such control is necessary for the protection of these features, such as the tables utilized for authenticators and keywords.

F. Individual Security Responsibilities: All users of the system must be advised of the need for exercising good security practices in protecting the data stored and processed by the system. Users should be informed of their responsibility to protect the authenticator assigned to them and the keywords needed for system access to the security level of the data to which these indicators provide access. Users are also responsible for meeting the requirements in the handling of hard copy output, including the assignment of control numbers and the maintenance or dissemination logs on such material as promulgated by appropriate regulations. Users should also be informed of the fact that the system

25X1

[redacted]

is operating in a multi-security level mode and that any receipt by them of data which they have not specifically requested should be reported immediately to the system security officer.

DRAFT

25X1

[redacted]