//

IBSEC-CSS-R-6
19 January 1971

COMPUTER SECURITY SUBCOMMITTEE

OF THE

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

MEMORANDUM FOR: Chairman, United States Intelligence Board
Security Committee

SUBJECT : Guidelines for the Security Analysis, Testing, and Evaluation of Resource-Sharing Computer Systems

REFERENCES : a. Joint Memorandum from Chairman, Security Committee and Chairman, Intelligence Information Handling Committee for Chairman, United States Intelligence Board dated 23 April 1970, Subject: Controlled Multi-Level Security Test of DIA Analyst Support and Research System (IHC-D-132/1; USIB-D-71.9/1);

b. Secretary's Notes, United States Intelligence Board Minutes dated 14 May 1970 (USIB-M-570)

1. Paragraph 9.d of reference a. recommended that USIB request the Security Committee to submit for the Board's approval minimum security requirements for multi-level operation of computer systems in a controlled Top Secret environment and guidelines for the security testing of such systems. This recommendation was approved by the Board on 12 May 1970 as recorded in reference b.

2. Minimum security requirements for the multi-level operation of computer systems were prepared by the Computer Security

Subcommittee and approved by the Director of Central Intelligence with the concurrence of USIB on 7 January 1971 as DCID No. 1/16. This memorandum forwards guidelines for the security analysis, testing, and evaluation of resource-sharing computer systems in response to the second part of the tasking mentioned in paragraph 1 above.

3. These guidelines have been developed by the Computer Security Subcommittee acting in staff capacity as the special USIB group most knowledgeable of the subject. The report, therefore, is not meant to be a coordinated Community paper.

4. It should be noted that the guidelines were prepared to assist individual USIB organizations in the process of testing and evaluating their computer systems from a security standpoint as a basis for security accreditation. The paper is not to be interpreted as directive in nature. The problems of implementing its content are complex and involve the availability of manpower and expertise; in producing the report, the Subcommittee deliberately did not address these problems, since their consideration might have seriously impaired the quality of the product. Lack of technical expertise to conduct certain phases of the security analysis, testing, and evaluation process might have suggested omission of such phases from the guidelines despite their security importance.

[redacted] STAT

Chairman
Computer Security Subcommittee

both productive and stable. The process should be scheduled for a period in which, for example, the system is not undergoing any major software, hardware, or procedural modifications. Changes taking place in the system during the process should be separately evaluated in the light of their impact on both system security and the status of the testing process.

4. In many cases, due to operational requirements, the analysis, testing and evaluation process must be a discrete though recurring activity. On the other hand the advantages of continuous analysis and testing should be recognized, since almost any system is constantly undergoing change.

5. It is acknowledged that system configurations, capabilities, locations, and procedures vary widely among organizations which may use these guidelines. It is essential that insofar as possible the analysis and testing process be based upon these guidelines in conjunction with applicable regulatory guidance. These guidelines are meant therefore to suggest a method for matching the environment of a given system with the security requirements demanded for information it is to process and store. System security analysis is requisite to the testing process; both the analysis and testing phases provide the groundwork for system evaluation. While all three may be independent phases, they are not mutually exclusive. They all may contribute to a feedback loop serving to identify security deficiencies, initiate remedial action, and in turn permit further testing and re-evaluation.

TEST PLAN:

6. Judicious application of these guidelines in the security analysis, testing, and evaluation of a specific system dictates the need for an orderly approach to the process including the preparation of a test plan as a first step. Development of this plan for testing and evaluating a specific system should include predetermination of the criteria under which the results will be considered acceptable. In some respects these criteria will consist of the presence of required security features; in other cases, however, acceptability will be determined quantitatively in terms of the probability of failure in the systems overall security posture.

SYSTEM SECURITY ANALYSIS:

7. The security analysis of system operation consists of the following:

a. Description of the security environment in which a given system is intended to operate;

b. Identification of protective hardware, software, personnel, physical, and procedural security features.

c. Determination of the presence or absence of such features and procedures required by appropriate regulatory issuances;

d. Documentation as to how these features are applied to the hardware, software, and operating conditions of the specific system under review;

e. The ordering of these safeguards into a framwork showing the manner and degree to which they are designed to guard against possible security vulnerabilities; it is desirable, although not universally practical, to attempt the application of quantitative methods including statistical probability to this phase of the process.

8. The analysis should be oriented toward determining whether system security features meet the requirements of regulatory issuances, and/or collectively provide the degree of protection adequate for the needs of the information being stored or processed in the system.

SECURITY TESTING:

9. This process includes the examination and attempted subversion of all system security features and procedures, singly and in combination, to determine whether they are efficient and cohesive in providing the desired data security control. The extent and duration of this phase of the process will depend on the complexity of the system involved, and the sensitivity of the data.

(2) Separation of Data By Storage Medium: Similar to memory protect, except that data separation is normally not additionally dependent upon software protection; this separability must be reviewed to determine its presence and reliability.

(3) Protection State Variables: Any one or more variables included in the execution state of a processor which determine the interpretation of instructions executed should be identified in the security analysis phase. The actual ability of the processor to access locations in primary memory should be tested to insure that all original and modified capabilities are known, understood, and adequately controlled.

(4) Security Labels: The presence and efficacy of security classification and other required control labels in the files of the system and the reliability of the software utilizing these labels should be checked in both the analysis and testing phases.

(5) User Identification/Authentication: Although user identification/authentication features will primarily apply to remote users of resource-sharing systems, all persons accessing any part of a system should be identified and controlled in some manner. If the control mechanisms are based on software and/or hardware, their adequacy must be examined and tested. If manual control procedures are used, their efficacy should be taken into consideration in the analysis phase of the overall process.

(6) System Supervisor: It is imperative to examine the functional dependability of and the security control over the system supervisor, which acts as the overall control of system operations. This portion of the software (also known as the executive or the monitor) internally manages job flow through the computer, allocates system resources to job, and controls data

flowing to and from files and terminals. Since it represents a critical element in the security of system operation it is worthy of close scrutiny in the analysis and test phases. This scrutiny should determine that rigid controls are exercised to limit access to the supervisor to authorized personnel, especially for the purpose of changing it in any way.

(7) Privileged Instructions: The analysis and testing phases should determine that the architecture of the system provides a capability for privileged instructions and protection thereof. This capability for controlling all input/output commands, and commands to change memory boundaries and protection barriers should be verified. Moreover, it should be determined that the supervisor program alone can operate or provide access to these privileged instructions. The testing phase should attempt to ascertain any user access to such instructions. An actual test of these instructions should be performed within various software systems to verify their reliability from a security and data integrity standpoint.

(8) Separation of User/Supervisor Modes of Operation: The analysis and test process shall determine the separation of the user and executive modes of system operation and insure that a program operating in user mode is prevented from performing unauthorized executive functions. After analysis of system documentation, the test should be oriented toward the verification that application/user programs are incapable of any alteration to the supervisor. This test may reveal a necessity for investigation of all user programs in this regard.

(9) Residue Cleanout: The security analysis and testing phases should verify the presence of instructions for performing residue cleanout which system or user programs can execute under the following conditions:

(a) Upon system initiation;

(b) Either upon job completion, before allocation, or after deallocation of any assigned permanent user storage area;

(c) Whenever determined necessary by the system security officer.

Further, measures should be identified and their efficiency tested to insure that memory residue from terminated user programs is made inaccessible to unauthorized users.

(10) Audit Trails: The presence and reliability of the system's security audit trail must be examined in the analysis and testing phases. It should be determined that this feature contains sufficient information to permit a regular security review of system activity and that the audit trail is in fact reviewed for this purpose, and not generated solely as a record of system transactions. During the testing of the audit trail software feature, special care should be used to confirm that access and security authorization violations and incidents are detected and recorded. For this purpose, special "spy" programs or routines which attempt to violate the security controls of the system should be exercised to determine the effectiveness of this feature.

b. Other Controls:

(1) Personnel Security: During the analysis, a determination should be made that all personnel having unescorted access to the system have been appropriately cleared and approved to receive data stored or processed by the system.

The test process should also insure that all other personnel are properly escorted and monitored during