IPC Committee
USIB
IHC - DCID

18 NOV 1970

MEMORANDUM FOR: CIA Member of the USIB Computer Security Subcommittee

SUBJECT : Guidance for the Security Analysis, Test and Evaluation of Resource-Sharing Computer Systems

REFERENCE : Your memo for the Information Processing Coordinator/DDS dtd 13 November 1970; same subject

1. The deadline you established for comments about the draft guidance was too short to permit a very careful or thorough consideration of the proposal. A hasty review leads to the conclusion that the proposal is totally impractical. The time, cost, and relative lack of resources required to analyze, test, and evaluate all user programs would cause computer systems to founder from the weight of their own overhead. I wonder whether any effort has been made to assess the magnitude of the task that would be involved, how long it would take how many people to do it at what cost, and evaluate that in terms of the risk of not doing it in order to get some notion of its worth. Perhaps a more practical and direct approach would be simply to take particular care to guarantee the reliability, in the personnel security sense, of systems programmers.

2. There is a statement in paragraph III that the "security analysis, test and evaluation should be conducted when the system is operating...." There is nothing to say what happens if the systems fail to pass the test and evaluation, but presumably it means that they would have to be redesigned and reprogrammed. I have no way of guessing how many existing programs or programs yet to be developed would pass the test but the failure of any of them resulting in a need to start over again would impose an unbearable burden on the systems people and cause the alienation of users and managers at all levels of the organization.

3. The scope of the paper says that the guidance applies "to all community intelligence functions using resource-sharing computer systems support for which special handling controls have been established." The use of the word "all" presumably applies whether the systems function in a totally intra-agency environment or an inter-agency exchange. Perhaps this requires some clarification.

4. The statement of the scope says the guidance applies to the intelligence functions for which special handling controls have been established. "Special handling" presumably means codeword, and "intelligence functions" presumably do not include functions with which we are primarily concerned in the Support Directorate. We have established special handling controls for many of our systems that deal with Security, Personnel, Financial, and Budgetary information which are extremely sensitive but are not intelligence functions and do not fall within any codeword system. I interpret the language in the statement of scope to mean, therefore, that the guidance proposal would not apply to systems in the Support Directorate. This is the interpretation I would prefer and I would appreciate confirmation that the Guidance does not apply to Support functions.

5. The word "should" is used throughout the paper with never a specification of who "should", and there is nothing to say what the consequences will be if all of those things which "should" be done are not. The paper says that systems should be accredited but we do not know who is authorized to do the accrediting. The combination of the effort to analyze, test, and evaluate systems should be a positive or negative recommendation for accreditation but there is no way of knowing to whom the recommendations are to be submitted.

6. The editorial style of the paper is troublesome throughout. One example from page 2: "A. Security Analysis - This process will encompass the accumulation of all conceptual approaches and features for providing security protection of information...." Perhaps the problem is self-evident, but what is a conceptual approach? How does one accumulate conceptual approaches? How does a process encompass the accumulation?

7. Pages 8 through 11 discussing security testing seem, in a hasty review, to be almost exactly duplicative of pages 2 through 7 describing security analysis. I should think that a careful editorial review would make it possible to improve the organization of the paper significantly and shorten it appreciably.

[redacted] 25X1A

DD/S
Information Processing Coordinator

DDS/SSS/RHW:sd (18 November 1970)

Distribution :
Orig & 1 - Addressee
1 - SSS Subject
1 - SSS Chrono
1 - [redacted] 25X1A