DRAFT

STATEMENT OF WORK

Attachment to HISI/MIT Research Contract

February 25, 1974

The work plan under this research agreement is based on the document "Proposal for Engineering of a Computer System for which Security can be Certified by Auditing", submitted to Honeywell Information Systems Inc., in October, 1973. That document proposed a level of activity based on a budget about 50% greater than that of the current research contract, and therefore this statement of work anticipates a rate of progress something less than two-thirds the rate implied in that proposal. In most cases, during the calendar year 1974, the tasks described here will proceed only through initial design; some implementation may begin but will probably not be completed within calendar year 1974. In such cases, the work result will consist of memoranda detailing initial design proposals. It is recognized that in the course of work on each task it may be discovered that some variation on the task is appropriate, that work in the area should be postponed until another task area is completed, or that the task should be abandoned as not feasible. The following tasks are those on which progress is expected during 1974. (Further details on the tasks will be found in the referenced proposal.):

1. Reviewing, verifying, and updating the list of outstanding implementation mistakes of Multics which affect security.

2. Update and publication of a survey "Ongoing research and development on information protection". This survey was originally undertaken to identify and coordinate with other security research projects; its publication is intended to enhance communication among workers in the field.

3. Restructuring the Multics Dynamic Linking facility to not require supervisor privileges. This task is currently estimated to eliminate 10% of the current supervisor entry points. Its main technical difficulty involves dynamically linking across protection ring boundaries without use of special privileges.

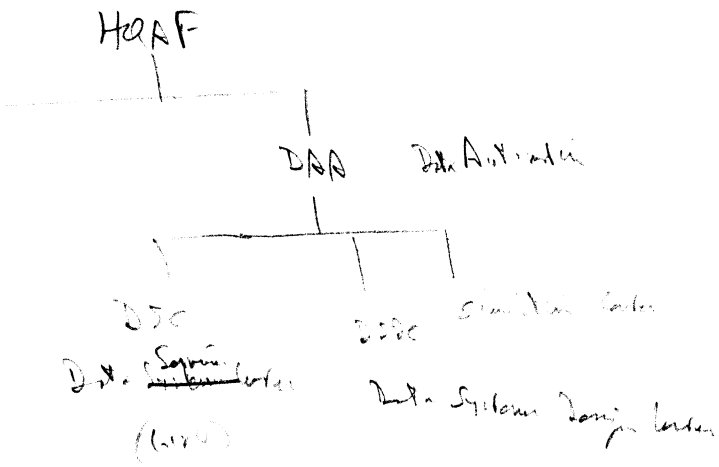
4. Restructuring the Multics address space management to not require supervisor privileges. This task involves removing the "Known Segment Table" from the supervisor and placing it under control of the user instead.

5. Revising the Multics initialization strategy to do more work at the time of system generation (when a rich environment is available,) and less in the primitive environment of system bootstrapping.

6. Development of alternative implementations of the Multics page removal selection and processor scheduling algorithms, which are simpler in structure and which are more compartmentalized, using parallel processes and multiple protection rings, if feasible.

7. Reimplementation of the metering interface of Multics so that the ability to measure the system is not coupled with the privileges of system programming and unlimited read access to supervisor data bases.

8. Development of simpler, yet more effective, buffering strategies for the ARPA network interface. This modification is expected to significantly reduce the size of one of the largest protected modules of Multics.


HQAF
DAR