from HIS
to ESD
rec'd 5/30/74

A Proposal for
Multics Security Research
(Project Guardian)

1.0 SCOPE

1.1 Overview

This is a level of effort, cost sharing proposal for an advanced development program to be conducted by Honeywell, Inc. and the Massachusetts Institute of Technology, directed toward the study, design, and evaluation of a certifiably secure computer system based on Multics technology. This program will be in the form of a cost-sharing contract between Honeywell, Inc. and the U.S. Air Force, with Project MAC of the Massachusetts Institute of Technology as a directed subcontractor of Honeywell. Honeywell feels that a cost-sharing contract is justified for the following reasons:

* Honeywell has a substantial commercial interest in Multics, dating from the participation in the initial development of the H645 hardware through its present availability as a fully supported standard product on the H6180.

* Multics systems of considerable value have been delivered to both Government and commercial customers and the system represents a major offering of Honeywell in the large-scale systems area.

In recognition of this fact, Honeywell has funded the Project MAC research effort in secure computer systems for the first half of calendar 1974 in order to provide project continuity and to formulate the basis for the development of a certifiably secure computer system. This research, funded by Honeywell, insured the continuation of a project (funded by the Advanced Research Projects Agency until December 1973) which is clearly in the Government interest.

1.2 Description

The research to be performed will fall into two broad categories, the reduction of hardcore to certifiable size and the study of secure input-output processing. The investigation of the hardcore will be performed primarily by Project MAC and the input-output study primarily by Honeywell, although the effort will be conducted as a single, integrated project, under Honeywell direction. The investigation will continue until June 1975, at which time it is anticipated that a complete understanding of problems involved in developing a certified

system will exist and an outline of their solutions will have been developed. The effort will produce three classes of documents:

* Technology reports, at the system and module levels, which will discuss general technical issues influencing certification.

* Specifications, at the system and module level, which will define specific designs or modifications to Multics required to achieve certification.

* An Integration Plan, which will describe the duration and levels of the various efforts which will be required to implement the technology defined in the reports and specifications.

In addition there will be the usual management reports required of good research and development practice.

1.3 Data Rights

The rights in data developed under this contract shall be identified either as limited or unlimited. Unlimited rights in data shall be granted to the Government for specified items of data and shall enable the Government to have a non-exclusive, transferable right to use such data, as defined in ASPR 7-104.9(a)(3). The Government need not hold in confidence data identified with unlimited rights. Limited rights in data shall be granted to the Government for specified items of data and shall enable the Government to have a non-exclusive, non-transferable right to such data solely for Government use, as defined in ASPR 7-104.9(a)(2). The Government shall hold in confidence all data identified as limited rights data. Honeywell shall have non-exclusive, transferable right to use all data developed under this contract. All data not specifically identified as limited or unlimited, including, but not limited to, all background data, shall remain the exclusive property of Honeywell and shall be held in confidence by the Government, unless this data is already available to the public or is rightfully obtained from another source without restriction.

1.4 Proprietary Data

The Government agrees to grant to the contractor the right to designate those portions of the study results that the contractor may determine to be proprietary. Such data as designated by the contractor to be proprietary and furnished in connection with this contract shall be held in confidence by, and not disclosed outside of, the Government. This restriction does not limit the Government's right to use information contained in the data if it is rightfully obtained from another source without restriction.

Honeywell shall have a transferable right to use such data. The data subject to the restriction shall be marked by the following statement:

> Use or disclosure of the above data is subject to the restriction as contained in Contract _____ between Honeywell Information Systems, Inc. and the Government.

The Government shall include restrictive markings, including copyright notice if any, on all its reproductions, copies, or modifications of such data.

2.0 STATEMENT OF WORK

2.1 Reduction of Hardcore to permit certification.

This work will be conducted in accordance with the proposal submitted by Project MAC to the Advanced Research Projects Agency and the Electronic Systems Division, USAF, dated October, 1973. This work will be done primarily by Project MAC with Honeywell support and direction.

2.2 Secure Input-Output Processing.

This effort will consist of the examination of current Multics practices in the areas of input-output and communications processing with regard to their conformance or nonconformance to the principles of a certifiably secure system. Technology reports and functional specifications will be produced for secure front-end processing and secure input-output processing. This work will be done primarily by Honeywell with Project MAC support.

2.3 Consistency with Modelling Activities.

Each effort will be monitored by Honeywell personnel familiar with and qualified in the mathematical investigation of certification now underway under Government sponsorship. This will ensure consistency of the proposed technology development activities with the results of the mathematical investigation.

2.4 Integration Plan

Along with the system-level specifications and module specifications, a plan for the implementation of the results of this effort and the integration of that implementation into Multics will be developed. This work will be done jointly by Honeywell and MIT.

3.0 DELIVERABLE ITEMS

3.1 Software

There are no software items specified for delivery under the provisions of this proposal.

3.2 Hardware

There are no hardware items specified for delivery under the provisions of this proposal.

3.3 Technology and Management Reports and Specifications

Honeywell will provide five (5) copies of each document under the provisions of this proposal. Additional copies will be available at additional cost to the Government.

The following documents are deliverable as a result of this effort:

a. A Final Technical Report, which describes the technical issues raised and resolved by this effort in terms of general Multics technology. The Government shall have unlimited rights, as defined in Section 1.3, in the data contained in the Final Technical Report.

b. Technical Reports, which will be issued as required, upon the development of some result of significance. The Government shall have unlimited rights, as defined in Section 1.3, in the data contained in the Technical Reports, except that if a Report is designated proprietary (Section 1.4), the Government shall have limited rights in such data.

c. Monthly Research and Development Management Reports, which will provide in an early issue a plan and milestone chart for the research effort and describe in later issues progress against that plan. The Government shall have unlimited rights, as defined in Section 1.3, in the data in these reports.

d. An Integration Plan, which will provide schedules, milestones, durations and levels of effort for the implementation and integration into Multics of the results of this effort. The Government shall have limited rights in data, as defined in Section 1.3, in the integration plan.

e. A System Specification, which will describe in detail the system effects of the implementation of all of the hardware and software specified by this effort. The Government shall have limited rights in data, as defined

in Section 1.3, in the System Specification.

f. Module Specifications, which accurately describe the functional characteristics of the hardware and software modules to be included or altered as a result of implementing the technology developed by this effort. The Government shall have limited rights in data, as defined in Section 1.3, in these Specifications.

4.0 SCHEDULE OF EVENTS

4.1 The Research Period

This effort represents the continuation of a program funded by Honeywell from January, 1974 to 30 June 1974. The continuation must begin at the end of the original period and will continue until 30 June 1975.

4.2 Design Reviews

The scope and direction of the effort will be reviewed with the Air Force at quarterly intervals near the end of the calendar year quarter, on a mutually agreed upon date and location. Formal approval of the work presented at the design review should be provided within 15 working days. Delays in excess of 15 working days in obtaining approval may cause changes in schedule.

4.3 Report Delivery

The items described in section 3.3 of this proposal will be delivered according to the following schedule:

a. Final Technical Report: A preliminary draft will be submitted on or before 24 January 1975 and a final draft on 30 June 1975.

b. Technical Reports. As Required.

c. Research and Development Management Reports. Monthly.

d. Integration Plan. A preliminary draft will be submitted on or before 11 October 1974 and a final draft on 10 January 1975.

e. System Specification. A preliminary draft will be submitted on or before 24 January 1975 and a final draft on 30 June 1975.

f. Module Specification. As Required.

5.0 Cost Sharing Breakdown

Honeywell feels that the level of effort outlined in Appendix A is most appropriate for the program at this time.

6.0 Additional Contract Clauses

The following contractual clauses are provided to be included if applicable to this study.

6.1 Tax Exclusions

Notwithstanding the provisions of ASPR Clause 7-103.10(a), the contract price excludes all state and local taxes levied on or measured by the contract or sales price of the services or completed supplies furnished under this contract. Taxes so excluded from the contract price pursuant to the preceding sentence shall be separately stated on the contractor's invoices, and the Government agrees either to pay to the contractor amounts covering such taxes or to provide evidence necessary to sustain an exemption therefrom.

6.2 Warranty Exclusion and Limitation of Damages

Except as expressly set forth in writing in this agreement and except for the implied warranty of merchantability, there are no warranties expressed or implied. In no event will the contractor be liable to the Government for consequential damages as defined in the Uniform Commercial Code, Section 2-715 in effect in the District of Columbia as of January 1, 1973, i.e.:

> "Consequential damages resulting from the seller's breach include:
>
> (a) Any loss resulting from general or particular requirements and needs of which the seller at the time of contracting had reason to know and which could not be reasonably be prevented by cover or otherwise: and
>
> (b) injury to person or property proximately resulting from any breach of warranty."

6.3 Contractual Terms

In the event that this proposal is favorably considered, Honeywell Information Systems, Inc. reserves the right to negotiate with the Government mutually satisfactory contractual terms and conditions for inclusion in any contract resulting herefrom.

7.0 Related Efforts

7.1 GCOS/Multics File Transfer Facility

(Contract F30602-73-C-0327 Rome Air Development Center)

This project, which is now in process, involves development of software to transfer all standard GCOS file types from the GCOS environment to the Multics environment. The project also covers design and implementation of software to transfer specially formatted data into logical data base files on the Multics system.

This project also will prepare a user handbook giving instructions for transfer of GCOS files into the Multics file system and for the subsequent conversion of these files into a logical data base form. A second user reference manual will be prepared to describe the data base implementation package that Rome Air Development Center has developed, and to guide the user in its application.

Particular attention is being paid to the security related aspects of this file transfer facility and to provision of a more secure tape I/O capability.

7.2 Security Design Analysis

(Contract F19628-73-D-0087 Air Force Data Services Center)

A joint Security Design Analysis was conducted by a team composed of representatives of groups active in the computer security field. Team members participating represented USAF AFDSC, USAF ESD, Mitre Corp., Honeywell CISL, and Honeywell DSO (MSP). The analysis was conducted to evaluate the requirements for providing a two level security system on Multics. The result of the Analysis is contained in the final report written by Multics Special Projects personnel. The report covers a high level design for modifications to the Multics system to support a two level security environment.

7.3 Secure Data Management System (RFQ F30602-74-Q-0163)

This project has been quoted to RADC but the award has not yet been made. The project involves the study and design of an open use, multilevel, secure data management system. The data management system is to be constructed under Multics and is to utilize the security characteristics of Multics to the greatest degree possible. It is also to utilize the Data Base Management System Implementation Tool recently developed by RADC. The project involves construction of a model of the data management system, proving the correctness of the model, and then

transfering the model into a design for an implementable data base management system.

7.4 Secure 6000 Environment (Unsolicited Proposal to RADC)

This unsolicited proposal will be submitted to RADC in the near future. It covers the analysis, study, and design of a Secure 6000 Environment to be constructed within Multics. The goal of the Secure 6000 Environment project is to provide a means for the execution of any 6000 program, including the GCOS Operating System and privileged slave programs, under the control of the Multics system. Multics interprocess security would then be extended to the 6000 programs operating under each environment.

8.0 Personnel

William Earl Boebert, Manager, Multics Special Projects

Education: BS, Mathematics, Stanford University, 1967

Current Responsibilities:

In his current capacity he has responsibility for consultation, education, and special subsystems development for the Multics system.

Prior Experience:

Mr. Boebert has been involved with the Multics system since November 1970, when he performed a technical evaluation of the system. Since that time, he has implemented several applications and subsystems and supervised investigations of Multics features, analysis of Multics performance, and the preparation of specifications of new Multics features.

Previous to this, Mr. Boebert was part of the design team for the radar landmass subsystem of Honeywell's successful Undergraduate Navigator Training System (UNTS).

Mr. Boebert has also been a software design consultant in the Electronic Data Processing Division of Honeywell, where he performed operating system and compiler design and evaluation duties.

Prior to joining Honeywell, Mr. Boebert was an Electronic Data Processing Officer in the United States Air Force, where he had both technical and managerial responsibility. He was awarded the Air Force Commendation Medal in 1966 for his contribution to a major system conversion.

Organizations: Association for Computing Machinery

Publications:

Boebert, W.E., "Toward a Modular Programming System", Honeywell Computer Journal, 1968.
Boebert, W.E., "The Eagle Squadrons", Journal of the American Aviation Historical Society, 1965

Charles T. Clingen, Manager, Cambridge Information Systems Laboratory

Education: BS Physics, Rensselaer Polytechnic Institute, 1958

Current Responsibilities:

Mr. Clingen is the Manager of the Cambridge Information Systems Laboratory. He is responsible for leading the development of the Multics system.

Prior Experience:

Prior to this, Mr. Clingen was manager of the Multics Development Unit at CTSL where he was responsible for the quantitative and qualitative evaluations of Multics.

Before this, he was involved in advanced product planning for the General Electric Computer Department.

Organizations: Association for Computing Machinery

Publications:

"The Multics Virtual Memory: Concepts and Design" (co-author) CACM, May 1972
"Multics: The First Seven Years" (co-author) SJCC, 1972

Dr. Eric K. Jaede, Staff Mathematician, Multics Special Projects

Education: B.S. Mathematics and Physics, Rensselaer Polytechnic Institute, 1961
Ph.D. Statistics, University of Minnesota, 1967

Current Responsibilities:

Dr. Jaede is currently responsible for studies and research in the field of certifiably secure computer systems.

Prior Experience:

Dr. Jaede pioneered use of corporate modeling techniques in Honeywell. One project supported the successful bid and price decisions for the largest computer procurement ever undertaken by Honeywell. Another project aimed at refining computer pricing strategies and the characteristics of various market segments. This project led to development of an integer programming optimization model which supported the existing simulation models.

Earlier, Dr. Jaede managed the evaluation of a time-shared inventory control system for the distribution industry. Software was developed to simulate the performance of the system in the subject firm's inventory environment. This allowed comparison with historical performance.

Prior to that, Dr. Jaede managed a study program to develop a procedure for construction of computer data entry systems. The study resulted in an integer programming formulation of the problem and a branch and bound solution algorithm. The algorithm permitted the economic solution of practical problems.

Earlier, as a Principle Research Scientist with another Honeywell division, Dr. Jaede developed the first experimentally verified, economically feasible computer simulation of the shaped charge jet formation process as a compressible fluid. He also had general responsibility for the simulation of hydrodynamic events through Eulerian difference equation techniques. He also developed a variance reduction procedure for the improvement of computational efficiency for a class of algorithms for the time-constrained truck routing problem.

In earlier Honeywell employment, he furnished consultation in usage of linear programming techniques for a classified resource allocation problem. He also developed a model and a program for simulation of a mine/tank duel. He also did checkout and evaluation of a linear programming application package.

As an employee of Grumman Aircraft, he developed routines for matrix inversion, eigenvalues, root finding, polynomial fitting,

predictor-corrector methods for ordinary differential equations, and Monte Carlo methods for elliptic partial differential equations.

Teaching: Assistant Professor, University of Minnesota Extension Division, teaching mathematics and statistics, 1967 - 1969.
Instructor, Honeywell Evening Education Program, teaching operations research, 1969.

Randall R. Spitzer, Project Leader, Multics Special Projects

Education: B.S. Mathematics, University of Illinois, Urbana, Illinois 1964
M.S. Mathematics, Harvard University, Cambridge, Massachusetts 1966

Current Responsibilities:

Mr. Spitzer is responsible for insuring that the multiple technical activities leading to a certifiable secure system are comprehensive and correct. In discharge of this responsibility Mr. Spitzer conducts technology reviews, design analysis, and technical coordination.

Prior Experience:

Mr. Spitzer provided technical guidance for the system definition and installation of Multics at the Air Force Data Services Center. Previous to that he participated in the design of a general purpose multiprocessor operating system, performed product design for a service bureau serving the insurance industry, and directed an ARPA project to develop a low-cost time-sharing system.

Stanley Curtis Vestal, Senior Systems Analyst

Education: BA, Mathematics, University of Kansas, 1968
MS, Computer Science, University of Kansas, 1969

Current Responsibilities:

Mr. Vestal is currently a member of the Multics Special Projects staff of Data Systems Operations and is located in Rome, New York. His primary responsibility is that of Project Leader for the GCOS/Multics File Transfer Facility effort which is ongoing at Rome Air Development Center. In that capacity, Mr. Vestal provides technical leadership to a staff of systems programmers located in Minneapolis, Cambridge and Rome. He is also responsible for Multics maintenance and support, and customer interface at the Honeywell 645 Multics installation at Rome Air Development Center. In addition, Mr. Vestal participates in the design and implementation of enhancements to the Multics System, proposal preparation for contracts, delivers lectures on the features of the operating system, and is active in user education.

Prior Experiance:

Prior to joining Honeywell, Mr. Vestal was attached to the United States Military Academy Academic Computer Center. He served as a programmer/analyst in the Instructor Group of that facility. His primary responsibilities were the design, implementation and maintenance of a student programming assistance package modeled after the Dartmouth TEACH Subsystem.

Before that, Mr. Vestal served as a teaching assistant with the University of Kansas, Department of Computer Science, and as an applications programmer/consultant with the Computation Center there.

Organizations: Association for Computing Machinery

Publications:

Isaacs,R., Moore,D., Tuggle,F.D., Vestal,S.C., "Computer Solution of Verbal Analogy Problems", Journal of Computer Studies in Humanities and Verbal Behavior, 1973

Vestal,S.C., "Highlights of Multics in an Associative Processing Testbed Environment", 1972, Proceedings of the 1972 Sagamore Computer Conference on RADCAP and its Applications.

Jerold C. Whitmore, Senior Principal Systems Engineer

Education: A.A., Electronics, Pasadena City College, 1961
B.S., Electronic Engineering, California State Polytechnic College, 1965
B.S., Mathematics, California State Polytechnic College, 1965
M.S., Management, Massachusetts Institute of Technology, 1971, Information Systems and Computer Applications.

Current Responsibilities:

Mr. Whitmore is currently a member of the Multics Special Projects office of Data Systems Operations and is located in Cambridge, Massachusetts. He is actively involved in the analysis, design and implementation of security features on Multics and recently acted as project leader of a task group to provide military security access controls for the system. Mr. Whitmore has been a technical consultant to Multics subsystem writers and has developed and presented several Multics technical courses. Mr. Whitmore has been associated with Multics since mid 1971 when he was involved in Multics standard product planning and marketing.

Prior Experience:

Mr. Whitmore worked as a System Engineer and Consultant for Data Technology Inc., Massachusetts, where he designed and implemented an Engineering Management Information and Budget Analysis system on a DEC PDP-10 time sharing system.

Previous to that, Mr. Whitmore worked as a Senior Electrical Engineer, Systems Development, for Itek Corporation, Massachusetts, where his duties included development of system proposals and procurement specifications.

Before that, Mr. Whitmore was a Captain in the USAF at Hanscom Field, Massachusetts, where he supervised the Electrical Engineering Section of the Airborne Research Engineering Branch. His duties included design, implementation and flight testing of systems for applied research programs.

Affiliations: Institute of Electrical and Electronic Engineers
Association for Computing Machinery

Appendix A
Budget Proposal

A.1 Proposed Funding for Project Guardian

Honeywell	$297,970
Government	297,970
Total Funds	$595,940

Expenditures for Project Guardian

Honeywell	$97,970
Subcontractors	497,970
Total Expenditures	595,940

A.2 Proposed Contractor Budget

Period 1/1/74 to 6/30/75

Direct Labor	3700 manhours	
	2200 manhours at $9.86	$21,692
	1500 manhours at $10.40	15,600
		$37,292
Burden at 89%		$33,190
Labor and Burden		$70,482
G&A Expense at 39%		$27,488
Total Proposed Budget		$97,970

A.3 Proposed Subcontractor Budget

Period 1/1/74 to 6/30/75

Salaries and Wages	Number	Full-Time Equivalent	Cost
Faculty	5	1.0	$56,775
Staff	5	1.7	60,900
Graduate Students	6	1.6	40,380
Undergraduate Students	5	.5	9,360
Support Staff (Clerical)	3	.5	11,085
Total			$178,500
Overhead at 63%			112,455
Employee Benefits at 17.3% (excluding students)			22,275
Total Salaries and Wages			$313,230

Computer Time (at MIT Information Processing Center)

$7,500 per month for 18 months		$135,000
Other		
Terminals	$25,000	
Travel	6,000	
Reproduction	7,500	
Telephone	4,500	
Misc.	6,740	
Total "Other"		$49,740
Proposed Total Budget		$497,970

A.4 Other Contributions

The Government shall provide guidance and direction for this program, including technical results in related areas, such as certification modeling techniques and secure communications design issues. The Government will also provide, on a GFE basis, up to 7,000 hours of computer time and up to 70,000 page-months of storage on a Multics system.

Honeywell shall provide engineering resources, on an unfunded basis, for review, evaluation, and consultation during the period of the program. Honeywell will also provide the most recent, operational, maintained version of the Multics software to be used as the basis for the development activities.