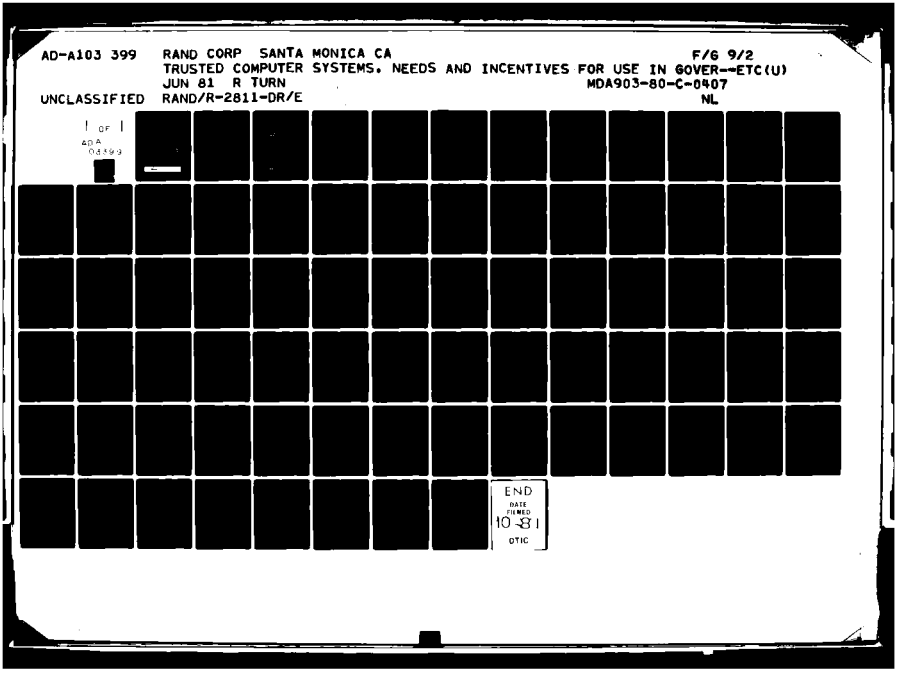

AD-A103 399
RAND CORP SANTA MONICA CA
F/G 9/2
TRUSTED COMPUTER SYSTEMS. NEEDS AND INCENTIVES FOR USE IN GOVER--ETC(U)
JUN 81 R TURN
MDA903-80-C-0407
UNCLASSIFIED
RAND/R-2811-DR/E
NL
1 OF 1
AD A 103399
END
DATE FILMED
10-81
DTIC

(1) LEVEL II

AD A103399

Trusted Computer Systems

Needs and Incentives for Use in Government and the Private Sector

Rein-Turn

June 1981

Rand

The research described in this report was sponsored by the Office of the Under Secretary of Defense for Research and Engineering under Contract NO. MDA903-80-C-0407.

Library of Congress Cataloging in Publication Data

Turn, Rein
Trusted computer systems.

"R-2811-DR&E."
Prepared for the Office of the Under Secretary of Defense for Research and Engineering.
Bibliography: p.
1. Computers--Access control. 2. Electronic data processing departments--Security measures. 3. Operating systems (Computers) I. United States. Office of the Under Secretary of Defense for Research and Engineering. II. Title.
QA76.9.A25T87 658.4'78 81-11995
ISBN 0-8330-0345-3 AACR2

Published by The Rand Corporation

R-2811-DR&E

Trusted Computer Systems

Needs and Incentives for Use in Government and the Private Sector

Rein Turn

June 1981

Prepared for the
Office of the Under Secretary of Defense
for Research and Engineering

Rand
SANTA MONICA, CA. 90406

PREFACE

This report was prepared for the Office of the Under Secretary of Defense for Research and Engineering, as a part of the Computer Security Initiative Program of the Computer Security Technical Consortium. It analyzes the need for trusted computer systems in the civilian agencies of the federal government, in state and local governments, and in the private sector. In addition, it proposes a rationale for the production and marketing of trusted computer systems.

The author is Professor of Computer Science at the California State University, Northridge, and is a consultant to The Rand Corporation.

Other Rand work in this area is reported in the following publications:

Willis H. Ware (ed.), *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*, R-609-1, October 1979.

Rein Turn, *Privacy and Security in Personal Information Databank Systems*, R-1044-NSF, March 1974.

M. Kathleen Hunt and Rein Turn, *Privacy and Security in Databank Systems: An Annotated Bibliography, 1970-1973*, R-1361-NSF, March 1974.

N. Z. Shapiro and M. Davis, *Uncrackable Data Banks*, R-1382-NSF, November 1973.

R. Stockton Gaines, William Lisowski, S. James Press, and Norman Shapiro, *Authentication by Keystroke Timing: Some Preliminary Results*, R-2526-NSF, May 1980.

Paul Baran, *On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations*, RM-3765-PR, August 1964.

H. E. Petersen and Rein Turn, *System Implications of Information Privacy*, P-3504, April 1967.

Dennis Hollingworth, *Enhancing Computer System Security*, P-5064, August 1973.

Dennis Hollingworth, Steve Glaseman, and Marsha Hopwood, *Security Test and Evaluation Tools: An Approach to Operating System Security Analysis*, P-5298, September 1974.

R. Stockton Gaines, *Control of Processes in Operating Systems: The Boss-Slave Relation*, P-5551, November 1975.

Rein Turn and Willis H. Ware, *Privacy and Security Issues in Information Systems*, P-5684, July 1976.

Willis H. Ware, *State of the Privacy Act: An Overview of Technological and Social Science Developments*, P-5756, November 1976.

Willis H. Ware, *Computer Technology: For Better or Worse?*, P-5903, July 1977.

Willis H. Ware, *Computer Security in Civil Government and Industry*, P-6385, September 1979.

Willis H. Ware, *Security and Privacy in the 80s*, P-6492, May 1980.

Willis H. Ware, *Security, Privacy, and New Technology*, P-6606, January 1981.

Willis H. Ware, *Security, Privacy, and National Vulnerability*, P-6628, April 1981.

SUMMARY

Since June 1978 the DoD Computer Security Consortium has conducted a Computer Security Initiative program, with the goal of achieving widespread availability of "trusted ADP systems"* for use within the Department of Defense (DoD), in other government agencies, and in the private sector. For the government, "widespread availability" means the use of commercially developed trusted systems whenever possible. Effective January 1, 1981, the Director of the National Security Agency (NSA) was assigned responsibility for the evaluation of computer security for the DoD and thus will serve as Executive Agent for the Computer Security Initiative. One of his functions will be the compilation of a DoD Evaluated Products List of trusted systems.

To date, the three major activities of the Initiative have been (1) coordination of DoD research and development efforts in computer security, (2) identification of efficient evaluation procedures for trusted operating systems and their uses, and (3) identification of incentives for the computer industry to develop trusted systems as part of its standard product lines. This report addresses the third task. It analyzes the needs for trusted computer systems in the civilian agencies of the federal government, in state and local governments, and in the private sector.

Protection is needed in computer systems to (1) safeguard assets or resources, (2) comply with certain laws and regulations, (3) enforce management control, and (4) assure the safety and integrity of computer-controlled processes or systems. Additional incentives for implementing trusted systems might be to realize operational economies, to achieve marketing advantages, and to enhance an organization's public image.

Protection of programs and data in computer systems involves a variety of physical, personnel, and hardware/software security techniques; administrative and operational procedures; and computer-communication security techniques. The most difficult task to date has been the development of trusted operating systems—a necessity in resource-sharing, multiuser systems to prevent users from interfering with each other and to control access to sensitive data files or process-

*A "trusted" ADP (automated data processing) system is one that employs sufficient hardware and software integrity measures to allow its use for simultaneous processing of multiple levels of classified and/or sensitive information. See the Glossary of Technical Terms in Appendix A for other definitions.

ing operations. The trusted operating systems sought by the Computer Security Initiative Program have a high potential for providing a solution to many of these problems.

In general, the use of current computer security techniques entails some reduction of system throughput, as well as some modification of existing application software or data bases. Some potential users of trusted systems are concerned about these impacts on their existing computer applications. However, there is a clear trend in computer hardware architectures and in software development toward including features that would be very useful for implementing performance-effective trusted systems; thus, performance loss is likely to be far less of a problem in the future. Conversion requirements for application software can also be reduced by designing trusted systems to be compatible with existing operating systems (as has been done, for example, in the KVM and KSOS efforts). A data-base conversion may be necessary (e.g., to include sensitivity-level information), but this is usually a one-time effort.

Computer security is needed in the civilian agencies of the federal government primarily for asset and resource protection and for regulatory compliance. Many agencies are responsible for financial disbursements or collections and thus are subject to attempts to perform unauthorized transactions. Trusted systems with appropriate operational and administrative controls can protect against unauthorized actions, unless these actions are performed by malicious or untrustworthy authorized users. Here, additional controls must be designed into the application programs.

All civilian agencies of the federal government are subject to the requirements for data security and integrity of Transmittal Memorandum # 1 of Office of Management and Budget Circular A-71. Personal information on individual citizens that is maintained by these agencies is also subject to the confidentiality requirements of the Privacy Act of 1974. Trusted operating systems can provide a tool for effectively meeting these requirements.

Protection needs in state and local government computer systems are similar to those in federal government systems, although they are on a smaller scale and there is considerable variation from state to state. Financial disbursements and collections account for a large part of state and local governments' computer use, but regulatory requirements for security are less stringent; indeed, many states have not enacted fair information practices laws, and some do not have laws requiring confidentiality of computerized criminal-history or public health information. Although these state agencies may have less compelling needs for trusted systems and they may be more constrained by economic considerations, trusted operating systems can greatly enhance the controllability and auditability of state and local govern-

ment computer systems, and as a consequence, they could increase public trust in government operations.

In the private sector, business information that is stored and processed in nearly all corporate computer systems is, or represents, a valuable asset that must be protected. The need for effective management control over all operations, particularly those that involve computers, is self-evident. Strong accountability requirements have been established by the Foreign Corrupt Practices Act of 1977, and requirements for ensuring confidentiality of personal employment, medical, and financial information are included in state laws. In addition, federal privacy protection requirements are pending that will affect insurance, health care, and financial industries in the private sector. Thus there is a strong rationale for protection of data and programs in private-sector computer systems. Trusted operating systems could provide that protection, as well as certain collateral benefits in the areas of safety and integrity, marketing, and public relations.

The widespread availability of effective and economical trusted operating systems is predicated on computer system vendors' perceptions of an adequate market for these systems. The government alone cannot provide enough user demand to be attractive; the market must also include the private sector. Thus, the situation is somewhat circular: A market will develop along with availability, but availability is influenced by the size of the market. The trusted system technology has been developed and is now being demonstrated by the Computer Security Initiative, so the technical risk to vendors appears relatively small. However, the perceived need to maintain compatibility between trusted systems that use new architectural and design concepts and the existing equipment and software bases causes vendors to be cautious about undertaking such development efforts.

Given the trend in new operating systems and software packages toward inclusion of stronger controllability and auditability features, it appears that development may evolve naturally toward trusted operating systems. A demonstration of a credible rationale for acquisition and implementation of trusted systems, as attempted in this report, may provide the additional increment of incentive for vendors to submit their systems for evaluation and inclusion in the Computer Security Initiative's Evaluated Products List.

Trusted systems can contribute effectively to the solution of the growing problems of protection of assets and resources, compliance with laws and regulations, assurance of safety and integrity, and implementation of full management control. In addition, trusted systems may provide operational economies, marketing advantages, and public-image enhancement. They are needed in a variety of applications that constitute a market that should be of considerable interest to

vendors and that should strongly encourage participation in trusted system development efforts. Their use could serve the interests of private business and industry, as well as public policy, public safety, and national welfare.

ACKNOWLEDGMENTS

The author wishes to acknowledge the constructive reviews of this report by Bruno Augenstein, Gary Martins, and Willis H. Ware of The Rand Corporation; by Marvin Schaefer of the System Development Corporation; and by Stephen T. Walker of the DoD Computer Security Consortium. Substantial contributions were made by Walter L. Anderson of the GAO; Gary Bearden of Tenneco, Inc.; Louise G. Becker of Congressional Research Service; Sheila L. Brand of HHS; Dennis Branstad of NBS; Harry DeMaio of IBM; Edwin Jacks of General Motors; Seymour Jeffery, formerly of NBS, now at TRW; Paul Karger of Digital Equipment; Theodore Lee of Sperry-Univac; Joseph Millen and Grace Nibaldi of Mitre; Donn Parker of SRI International; Kenneth Pollock of the GAO; Oliver Smoot of CBEMA; and Edward Springer of OMB.

Expert editorial assistance was provided by Janet DeLand.

CONTENTS

I. INTRODUCTION

Trusted Computer Systems

Computer systems have become a necessity in the functioning of a modern, industrialized society. They are used by business and industrial organizations and by government agencies to support daily operations and management as well as long-term planning. They are used in a wide variety of applications, including financial transactions of many kinds, personal information record-keeping systems, research and product design, and the control of manufacturing processes. The users expect these systems to have integrity and security, i.e., correct functioning of programs, correct data values, and assurance that there has been no unauthorized access to or modifications of either programs or data. In other words, they expect their computer systems to be trustworthy.

In a broad sense, a computer system consists of equipment, the operating system and application programs, data files or data bases, data communication networks, facilities, personnel, and users. Threats to system integrity and security may emanate from any of these subsystems, inadvertently or by deliberate design. A variety of protection techniques have been developed to counter these threats. For example, effective techniques exist for controlling physical access to computer systems. It has been much more difficult, however, to implement effective access controls within multiuser, resource-sharing computer systems where sensitive information is processed concurrently with other processing tasks, and where the trustworthiness of all users has not been established.

In the computer itself, the access control function is implemented in the operating system programs, supported by various hardware mechanisms. However, for various design and implementation reasons, no existing conventional operating system is fully secure—unauthorized users can surreptitiously disable or bypass the access control features of any conventional system. One solution to this problem is the rigorous application of formal design and analysis techniques (i.e., formal specification and formal verification) to those portions of the operating system that implement and enforce the desired security policy. The use of these design and implementation principles and techniques will help to assure that a system can mediate all access attempts, consistent with the security policy, and will aid the thorough analysis required for formal evaluation and testing of systems.

The DoD Computer Security Initiative program [1-5] defines a "trusted" system as one that "has sufficient hardware and software integrity to allow its use for simultaneous processing of multiple levels of classified and/or sensitive information" [1]. Currently, there are three major efforts in the DoD research and development program that relate to trusted systems:

1. Development and demonstration of trusted computer operating systems, including the Kernelized Secure Operating System* (KSOS-11), the Kernelized VM/370 System (KVM/370) which will be installed in two test sites in 1981, and the Secure Communications Processor (SCOMP). In addition to demonstrating the effectiveness of trusted computer systems to the DoD, these systems should serve as incentives to computer manufacturers to produce similar systems.
2. Development of applications for trusted systems, such as the GUARD systems for permitting interactions between untrusted systems that operate at different security levels, trusted front-end processors for computer networks, trusted message systems, and trusted data-base management systems.
3. Development of technology for trusted system specification and verification.

An important prerequisite for the development and certification of trusted systems is the precise identification of the access policy they implement and of the access control mechanisms used. It is also necessary to establish the criteria for evaluation of the degree of protection these mechanisms can provide. Many technical features can influence the overall integrity of operating system programs and the protection provided. Some features are essential regardless of the type of application or operating environment, but others are essential only in certain specific environments. Therefore, a particular system installed in one environment may provide sufficient security, while the same system in a different environment may be unacceptable. Accordingly, trusted systems can be categorized on the basis of their suitability for use in various operating environments. An important dimension in the categorization is the degree of confidence in the systems' design and implementation.

Within the DoD Computer Security Initiative, initial efforts to quantify protection levels have resulted in a preliminary seven-level structure [1,6]. The structure is cumulative in the sense that at each level the criteria for that level and all lower levels must be satisfied. When a system is evaluated, its rating will be determined by the

*See the Glossary of Terms in Appendix A for further definitions.

highest protection level that is completely satisfied. The categorization criteria were defined so that systems rated at the lowest protection levels must meet certain security policy standards, even if the access control mechanisms are not judged sufficiently strong to counter certain subtle threats. For systems at higher protection levels, the emphasis is on evidence that the software, and ultimately the hardware, is correct. As presently defined, the preliminary protection levels are:

- *Level 0: No protection.* A system that has no demonstrable ability to protect information.
- *Level 1: Limited controlled sharing.* A system in which some attempt has been made to control access, but the controls are limited. For example, login authentication in a Level 1 system is based on passwords. (Most of the current operating systems provide Level 1 protection and are suitable for dedicated-mode operation.)
- *Level 2: Extensive mandatory security.* A system in which minimal protection requirements are satisfied. Assurance is derived primarily from attention to protection during system design; extensive testing, including penetration testing, has been performed. Mechanisms include read and write authorization controls, virtual memory, and virtual machine architecture. (Some recent, mature operating systems provide Level 2 protection and are suitable for benign environments with need-to-know controls.)
- *Level 3: Structured protection mechanism.* A system in which additional confidence is provided through methodical construction of protection-related software components and modern programming techniques, including a top-level specification. (The MULTICS operating system is an example of Level 3 protection in a benign environment with two levels of national-defense security, Top Secret and Secret.)
- *Level 4: Design correspondence.* A system whose protective-mechanism design has been formally specified and verified. Tests are generated from the formal design specifications, and operating system security kernels are used to implement complete mediation. (Examples are the KSOS-6, KSOS-11, and KVM/370 systems.) Level 4 systems are suitable for environments where limited user programming is permitted and three levels of security are allowed (e.g., Top Secret, Secret, and Confidential) in a reasonably benign environment.
- *Level 5: Implementation correspondence.* A system whose protection mechanisms' software design and source-code implementation have been formally specified and verified. Test cases are derived from the formal specifications. Extended provisions are made for blocking covert information leakage paths. There are no examples

of Level 5 systems at the present time. This protection level is suitable for environments where full user programming is permitted and three levels of security are allowed (Top Secret, Secret, and Confidential) in a reasonably benign environment.

- *Level 6: Object-code analysis.* In addition to meeting Level 5 requirements, Level 6 systems include object-code analysis and object-code to source-code correctness proof, as well as additional hardware features such as extensive failure tolerance. Currently, there are no examples of Level 6 systems, and the formal analysis of object-code correspondence is beyond the state of the art of formal verification. Application environments would have full user programming and full multilevel security and would not have to be benign.

A description of security mechanisms provided at each level is still being developed [6], along with specifications of the administrative procedures that must be in place for the mechanisms to be effective, the threats that the systems can counteract, and the associated costs (in qualitative terms). The application areas and operational environments can then be analyzed to determine adequate protection levels, and the appropriate trusted systems can be selected from an Evaluated Products List that will be developed. This process is depicted graphically in Fig. 1.

The protection environment of a trusted system is achieved through hardware and software access control mechanisms, including implementation in firmware or microcode, that control the sharing of information. These mechanisms, which comprise a Trusted Computer Base (TCB) of the system, implement the "reference monitor" concept [7,8] for controlling when and how data are accessed.

In general, the TCB must enforce a given protection policy which describes the conditions under which information and system resources can be made available to users of the system. Protection policies specify precisely the rules for granting access to information in the various sensitivity categories and also cover the handling of such problems as unauthorized disclosure or modification of information, and damage to the system that can result in denial of service to authorized users.

Proof that a trusted system can enforce the desired protection policy requires a formal approach to TCB design, implementation, and verification. This is required to establish credibility of the TCB and to provide evidence of its capabilities. Since the TCB contains all the protection-related mechanisms of the trusted system, proof of its correctness will imply that the rest of the system will also perform consistently with respect to the security policy. Ideally, protection policy and

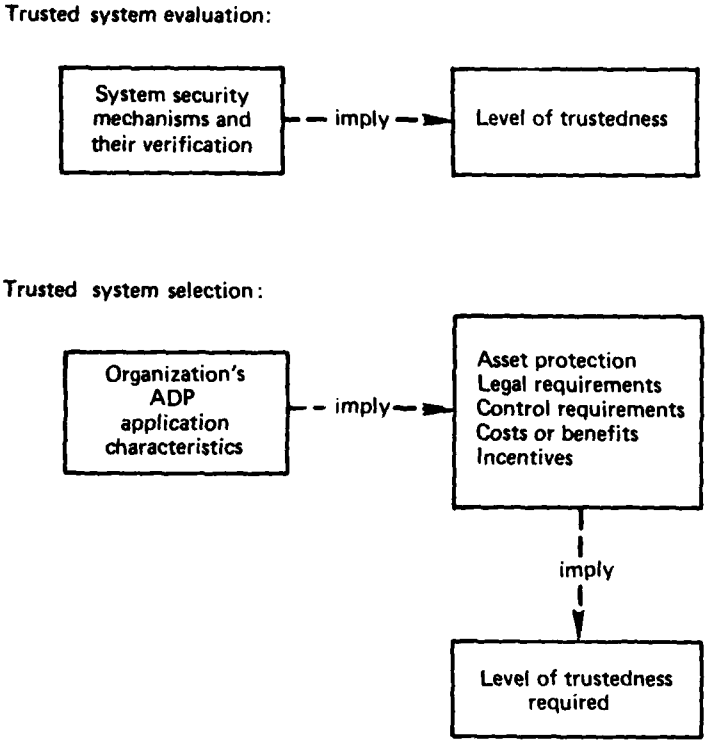


Fig. 1—Trusted system evaluation and selection process

protection mechanisms should be treated separately in the system design, so that the TCB can be flexible and amenable to different environments and will not require rewriting or reverification to accommodate changes in policy. Details of trusted system and TCB design have been described elsewhere [1-8], as have the security principles involved [9].

The Computer Security Initiative

In June 1978 the Assistant Secretary of Defense for Communications, Command, Control and Intelligence established the DoD Computer Security Technical Consortium and initiated the Computer Se-

curity Initiative program to coordinate and encourage the development of trusted systems for applications in the DoD and, through technology transfer, in other agencies of the government and in the private sector [1-5].

The Initiative program has pursued three major activities:

1. Coordination of the DoD research and development efforts in computer security.
2. Identification of consistent and efficient evaluation procedures for determining suitable environments for trusted systems.
3. Identification of incentives for the computer industry to develop trusted systems as part of its standard product lines.

These activities constitute three distinct, sequential phases in the Initiative program. The ultimate goal of the program is the specification of a TCB and the establishment of consistent and systematic criteria by which to evaluate government- and industry-developed computer systems [1]. The intent of the Initiative since 1978 has been to then identify an Executive Agent to carry out the formal evaluations of vendor-produced operating systems. Those that are judged usable as trusted systems in specified classes of applications and specified types of environments will then be placed on an Evaluated Products List. Effective January 1, 1981, the Director of the National Security Agency (NSA) was assigned responsibility for the evaluation of computer security for the DoD and will serve as the Executive Agent for the Computer Security Initiative.

In preparation for the formal evaluation stage, draft specifications and draft evaluation criteria have been distributed to the DoD and to industry for comment. When it has been demonstrated to the computer user community that trusted systems can be built and can be effectively employed in a variety of applications, the development technology will be transferred to the computer manufacturers.

Evaluation Center and Procedures

Central to the development and implementation of trusted systems, and to the compilation of an Evaluated Products List, is the concept of an Evaluation Center for trusted systems. This Center would perform technical evaluations of systems to be used in applications requiring a trusted system. It would also produce documentation for each system evaluated, assigning a protection level to the system, describing its specific protection mechanisms, and ultimately placing it on the Evaluated Products List [10]. The use of a central facility

rather than many small, dispersed facilities should assure that evaluations are as consistent as possible and that qualified technical personnel will be utilized efficiently.

The DoD trusted systems Evaluation Center currently is being established at NSA. It will maintain a staff experienced in computer system design, computer security issues, TCB design, and penetration testing. In addition to evaluating industry-submitted systems, it will be available to DoD agencies requiring security-related consultations on individual products or contracts. The Center will also establish and maintain internal research and development capabilities. Any proprietary information and rights of the developers will be safeguarded.

The evaluation of an industry-developed operating system will be based on the adequacy of each system's TCB design. The evaluation process proposed by the Initiative consists of four sequential steps, synchronized to the computer system development life-cycle phases [10]:

1. *Preliminary evaluation:* Analysis of the TCB of a submitted system to determine the adequacy of the system for use in an environment requiring trusted access controls. The purpose of the preliminary analysis is to determine whether the TCB has been sufficiently well designed and documented to warrant further evaluation. This step can be performed as soon as the proposed system has completed its concept formulation phase.
2. *Interactive evaluation:* An extension of the preliminary evaluation. This review will focus on whether the system satisfies the criteria for the level of protection specified in the preliminary evaluation. It will be based on a series of presentations by the developer and his documentation on the development phase of the system. The developer and the Evaluation Center will interact closely so as to assure that evaluation criteria are met and that discrepancies are found early in the development process.
3. *Final evaluation:* Analysis and testing of the production version of the proposed operating system to determine its strengths and weaknesses relative to the criteria for the specified level of protection. The developers will submit a copy of the production-level system to the Center for evaluation, along with details of the test methods and procedures they have used to evaluate it. This step cannot be undertaken until the initial acceptance testing has been completed and the system is available for field testing. The final evaluation will determine the "actual" protection level of the system and where (and if) it is to be placed on the Evaluated Products List.
4. *Periodic reevaluation:* Required reevaluation of trusted systems on

the Evaluated Products List that have been modified or enhanced. The Evaluation Center and the vendor will jointly analyze all system changes to evaluate the security-related aspects and to determine the extent of reevaluation needed.

The evaluation criteria to be used to determine the eligibility of a system for inclusion in the Evaluated Products List are still being developed [6,11]. Basically, they address two essential aspects of a trusted system: (1) completeness and adequacy of the protection policy that is to be implemented, and (2) verification of adequate implementation. In general, specific techniques or ways of implementation (e.g., in hardware, firmware, or software) will not be prescribed by the Evaluation Center.

Finally, a vendor who has a trusted system on the Evaluated Products List must also assure the integrity of copies of the system it provides to customers (for example, by maintaining the master copy of the system in a physically secure facility). The details of this and many other aspects of the Evaluation Center, the Evaluated Products List, and developer-Center relations are still being worked out.

II. NEEDS AND INCENTIVES FOR THE DEVELOPMENT OF TRUSTED SYSTEMS

The development of trusted computer systems was originally motivated by the security needs of military and defense applications [8,9]. In these applications, access to classified information must be limited to appropriately cleared individuals, as stated in DoD Directive 5200.28 (published initially in December 1972) and the associated manual [12,13].* Thus, the DoD and its component services have been at the forefront of trusted systems research and development.

The need for trusted systems in civilian agencies of the federal government, state and local governments, and the private sector is less clear-cut. However, the need does exist, and in this section we shall discuss five generic classes of needs and incentives for trusted-system implementation:

1. Protection of assets and resources.
2. Compliance with regulations.
3. Management control.
4. Assurance of system safety and integrity.
5. Operational economy.

Protection of Assets and Resources

Nearly every organization that has a data processing system or uses data processing services offered by a commercial vendor maintains computer-based data files that reflect its activities, assets, resources, and/or liabilities. These files are used almost exclusively to support daily operations; hardcopy backup, if any, is maintained primarily for archival purposes and is practically inaccessible for use in an operational sense.

Information itself is an important resource in the operation and management of an organization. Management information systems (MIS) are used both for decisionmaking in daily operation and for long-term organizational planning and guidance. The information used in strategic planning, along with the decisions themselves, is often very sensitive and must be protected against unauthorized access. In highly competitive industries, information on competitors'

*A comprehensive survey of federal security policies is reported in Ref. 14.

long-term development, production, and marketing plans is of great value, and the integrity of MIS data bases is extremely important. Moreover, the presence of inaccurate or deliberately falsified information can lead to decisions having very detrimental consequences.

Trusted systems for MIS applications seem to be a necessity rather than a luxury. Computer files containing sensitive information are subject to clandestine, unauthorized access by legitimate users of the system and, in some cases, by outsiders as well. If unauthorized actions can be detected, it is likely that their effects can be corrected, albeit sometimes at considerable expense and with substantial delays in the availability of correct information. If they are not detected, such actions can result in both the direct loss of assets or resources and the indirect losses that may ensue from operating without knowing that those assets or resources are missing or that the system has been tampered with. Numerous cases of such losses have occurred in the past; the problem is real, and it is serious [15].

Trade secrets are another type of corporate asset. They are protected by law against unauthorized use by outsiders, provided they have been handled as secrets from the very beginning of their development. If computer systems are involved in the development of trade secrets, protection of programs and data is a requirement; at the very least, trusted systems could be implemented as a demonstration of concern over the security of the trade secrets being developed.

In general, managers tend to be quite skilled at providing adequate protection to manual accountings of assets and resources, using control techniques that have proven effective through years of use. However, these techniques are not directly transferable to the protection of computerized information. Moreover, high-level managers tend to be unfamiliar with protection techniques for computer systems (and with computers and data processing in general), and few have addressed the problem of protecting accountings of assets and resources maintained in such systems.

When trusted systems become available as off-the-shelf items, they can be used to augment the existing administrative controls to provide effective access control and to eliminate at least those vulnerabilities in computer systems that are due to the lack of effective protection mechanisms in current operating system programs. Moreover, individual organizations or agencies will no longer need to design and implement their own protection mechanisms and will be spared the task of protection system evaluation and verification.

Regulatory Compliance

A sizable body of federal and state laws and regulations that affect automated data processing (ADP) systems and their management and control has evolved over the past several years [14]. Collectively, these regulations

1. Prescribe secure processing and storage of certain categories of information (e.g., identifiable personal records on individuals).
2. Require assurances that full management control is exercised over ADP operations and use.
3. Require implementation of security techniques in ADP systems and facilities as indicated by risk assessments.

Compliance with such requirements may necessitate the use of trusted computer systems. For example, in the pharmaceutical industry, FDA regulations require accurate and controlled record-keeping. Trusted systems can strengthen the assurance that the required records are not subjected to unauthorized modifications.

Many suppliers of ADP services assure their customers (both external subscribers and internal users) that their data and programs are fully protected. Failure to provide that protection may lead to legal actions against them involving breach of contract. Trusted systems can provide the means to minimize protection failures and associated losses, thereby reducing management vulnerability to breach-of-contract lawsuits or other claims of negligence and liability, including lawsuits filed by stockholders.

Legal admissibility of computer records as accurate representations of a corporation's financial status or business activity is an important consideration in modern business and industry. If records from a corporate computer system are not considered trustworthy by authorities, they may be ruled inadmissible, and the corporation may have to keep additional records using more expensive manual methods. Trusted computer systems may become a prerequisite for full legal acceptance of computerized accounting systems and reports.

As the use of trusted systems in business and industry expands, such use is likely to become a standard of good practice for management control and protection of computer-based assets, resources, or customer data. Failure to employ trusted systems could eventually be construed by insurance carriers, external auditors, regulatory agencies, customers, contract grantors, and stockholders as management practice that is not prudent and reasonable.

Management Control

Effective management control is required by various laws and regulations, but it should also be an organizational goal in its own right. An organization must have mechanisms in its structure, administrative procedures, and technical operations that minimize the potential for detrimental actions or events and that provide a high level of confidence that such events will be detected, if they do occur. With the advent and increasing use of ADP systems, many of the traditional means of implementing management control have become ineffective. They must be, and have begun to be, replaced by new means of control that take into account the environmental and functional changes brought about by the use of computers [16,17].

It has been necessary to develop internal control and auditing techniques to assure accuracy and completeness of computer-based transaction processing, record maintenance, and reporting, and to provide access control and physical security to computer systems and data files. However, technical hardware and software measures are not sufficient to assure full management control by themselves. They must be supported by clear and consistently applied management procedures and, above all, they must have the full support of top-level management.

Trusted systems can provide the first part of the overall protection system—the technical mechanisms. Management actions and support must, of course, be provided by the organization itself.

The potential benefits of trusted systems are evident, yet certain tradeoffs must be acknowledged: Rigid control can stifle innovation and impair efficient use of computer resources. Moreover, beyond required regulatory compliance, the risk of losses must be weighed against economic pressures on an organization. At times, the risk of loss due to imperfect controls may be small when compared to the risk of not being able to function at all. For example, retail stores will always be subject to a certain amount of shoplifting, since attempts to eliminate it totally—for example, by manually searching every exiting customer—would be excessively costly as well as unacceptable to the customers. A prudent choice among the protection options should help to ensure that a suitable integration of protection and functionality will be achieved.

Assurance of Safety and Integrity

A potential collateral benefit of trusted operating systems development and use relates to system safety and integrity. Computer sys-

tems are being increasingly used to implement control over systems that operate in "real time," i.e., whose operation must be monitored continuously. Computers are used to detect deviations from correct operation and to apply remedial measures immediately in process control in oil refineries and steel mills, automated assembly lines, rapid transit systems and air traffic, onboard applications in aircraft, national-defense systems, and many other applications. All of these real-time control situations are characterized by the possibility of disastrous consequences in the event of failure. Thus it is imperative that steps be taken to assure the safety of personnel, facilities, and equipment. Hardware and software components in such systems must be highly reliable, and their integrity must be assured throughout their life cycles.

High levels of hardware reliability can be achieved by use of various failure-tolerant design techniques. Reliability and continued integrity of software and data bases are more difficult to achieve. Software-engineering techniques can increase software reliability considerably, but full assurance of the reliability of a software module will require formal verification of design correctness and of subsequent implementation as computer object code. Such verification is currently difficult for all but very small programs.

The trusted system development effort is based, in the limit, on full verification of operating system program modules and their interfaces, but a trusted system can also be created by less than full verification (e.g., the MULTICS operating system). Since real-time control systems are essentially special-purpose operating systems, the concepts of trusted systems and their verification are fully applicable. Thus, real-time control systems should be viewed and developed as trusted systems.

The same is true for computer-aided design (CAD) systems whose products affect public safety, and for other computer models that are used to make important design or policy decisions. Construction engineering, nuclear power generation, aerospace engineering, and econometric modeling are examples. In such systems it is necessary to assure that the integrity of the design programs or models is not compromised accidentally or intentionally. Trusted systems or their design and verification techniques can be used here to increase that assurance.

Operational Economies

The use of trusted systems may lead to certain economies in the operation of a computer facility. Whether or not such economies actu-

ally materialize will, of course, depend on specific situations and contexts. For example, an existing system that has been acceptably secure by virtue of "periods processing" (a usually disruptive technique of scheduling sensitive processing to be done at times when the system is closed to other users) could be replaced by a trusted system, which does not require periodic scheduling. Or trusted systems could obviate the need for extensive background investigations (the so-called system-high clearance level mode of operation) for personnel who do not have critical functions in operating the computer system. In these cases, trusted systems permit reductions in special security efforts and thereby reduce associated expenses. In other situations, the cost benefits of using a trusted system may be less clear-cut.

In general, the following operational economies may be achievable through the use of trusted systems:

1. Reduced duplication of data, equipment, or personnel required when dedicated systems are used for processing sensitive data.
2. Reduced requirements for personnel clearances or security procedures (e.g., stringent control of physical access to terminals).
3. Reduced insurance premiums for business risk or liability or management liability (in the private sector).
4. Reduced downtime losses and recovery costs that should result from the better design and implementation of trusted systems.
5. Elimination of the need for a dedicated processing shift (e.g., in private-sector organizations that use proprietary data extensively or that have trade secrets to safeguard).
6. Reduced need for highly trained operators and support personnel to apply access controls and other controls.

Marketing Incentives

Certain organizations that provide services involving their customers' assets—e.g., banks, savings and loan associations, and other financial institutions—must be able to assure that those assets are properly handled and safeguarded. These organizations, particularly the financial institutions, tend to be very competitive and therefore are always seeking new approaches that will give them competitive advantages. The use of trusted systems to reduce risks to customers' assets may give an institution a more favorable image even though all competing institutions may already provide adequate protection of assets through insurance coverage.

Clients of organizations such as computer service bureaus are concerned with the security of the data or programs they submit for

processing or storage and are likely to choose an organization that can provide better safeguards, such as the use of trusted systems.

Finally, all government and private-sector organizations that interact with the public are concerned about their image. Government agencies make special efforts to explain their missions and to publicize the necessity or benefits of their operations. Private-sector organizations likewise expend resources to emphasize their concerns for the welfare of the public. A particularly important area of public concern is the collection and maintenance of personal information about individuals. The safeguards that are implemented to assure that personal information remains confidential and is not accessed or disseminated by unauthorized individuals can greatly enhance an organization's public image. Two or three corporations have already purchased advertising space in national magazines to emphasize their concern and to describe the approaches they are taking to assure confidentiality of personal data. Recent public-opinion surveys, including the Harris Poll directed by Alan Westin in 1978 [18], have demonstrated that there are strong public sentiments in favor of assuring confidentiality of personal information commensurate with individual privacy rights.

Public-image concerns also arise in the area of asset and resource protection. No organization wants publicity resulting from fraud or other substantial losses or because of having being victimized by a computer crime. The use of trusted systems can reduce the possibility of adverse publicity by reducing the probability of occurrence of such events.

Other Considerations

The question of whether or not trusted operating systems will be cost-effective must be addressed, along with the related question of utility, even if they are not excessively costly. These questions deal with performance capabilities and the impacts of trusted systems on the computer systems and applications being examined.

A trusted system that is acquired to be used in an environment of weak physical, administrative, personnel, or communications security may not be fully effective. It needs an appropriate foundation in the form of physical and administrative security.

A trusted operating system may also show poorer performance than a conventional one (although hardware enhancements may compensate for this penalty). In order to be certifiable, a trusted system will have to avoid shortcuts that improve software performance, and higher-level trusted systems, at least, will have to provide complete authentication and breach-of-security checks of all processing and

data access requests. These factors may substantially reduce the processing rate. Appropriate hardware support will be essential—additional or more powerful equipment may be required to offset performance losses—and this may limit the types of installations that can acquire efficient trusted systems. A security risk assessment must be made to establish the relative priorities of trustworthiness and performance. However, as trusted systems technology advances, the two attributes will become increasingly compatible.

Additional possible considerations in the use of trusted systems include the following:

- It may be necessary to maintain interoperability with existing software and/or data bases to an extent that discourages making the changes needed to comply with trusted system requirements. For example, if in a trusted system all protected objects have to be labeled with security classification indicators, such labeling may be expensive in an existing software base or in existing data files.
- While DoD security policy is quite general in that it provides for both mandatory and discretionary security and for (limited) data-integrity controls, it is possible that trusted systems that implement the DoD security policy model might not be fully suited to support some types of organizations and their security policies.
- The denial-of-service threat to computer security is not completely handled by trusted systems and should not be the primary reason for their acquisition. System robustness is increased by incorporating fault-tolerance techniques.

III. APPLICATIONS IN CIVILIAN AGENCIES OF THE FEDERAL GOVERNMENT

The federal government is the largest single user of computers in the United States. In fiscal year 1980, it operated 15,142 computers (an increase of nearly 80 percent over the 8,649 used in fiscal year 1975) [19]. The civilian agencies of the government currently operate 3,020 computers, many of which are minicomputers. The principal application areas are in the administration of federal programs and of the federal government itself.

Personal information records on individuals are maintained by all federal agencies for their own employees and for individuals associated with their missions and programs. The *Annual Report of the President on the Implementation of the Privacy Act of 1974* for calendar year 1979 [20] provides statistics on record-keeping by civilian agencies of the federal government. The major record-keepers are listed below:

Agency Name	Total Number of Computer Systems	Total Number of Individual Records (millions)
Department of HEW	497	1,033
Department of the Treasury	547	780
Department of Commerce	95	431
Department of Justice	186	200
Veterans Administration	53	157
Postal Service	75	105
Office of Personnel Management	17	91
Selective Service System	8	54
Department of Agriculture	236	33

In 1979, agencies of the federal government (including noncivilian agencies) had 5,843 systems of records containing 3.529 billion individual records. The record-keeping focus in other systems maintained by the Department of Labor, the Securities and Exchange Commission, the Small Business Administration, and others is on business enterprises.

Needs for Trusted Systems

Most civilian agencies of the federal government deal with financial disbursements or collections, confidential or personal information, and enforcement of policies or regulations. These agencies are likely to be subject to attempted or successful unauthorized transactions to establish eligibility for disbursements, alter amounts to be collected, or avoid enforcement sanctions. While agencies are striving to provide effective protection to the information processed in their computer systems, to apply strong management controls, and to assure compliance with legal and regulatory requirements, incentives to use trusted operating systems are often lacking. Some agency personnel have argued that there are many security discrepancies at levels far below the sophistication of a trusted operating system which should be rectified before turning attention to computer-system security. Physical security often tends to be inadequate, administrative controls are weak, and funds are often not provided to agencies for upgrading computer security and other aspects of management control, even though regulations require such upgrading of controls.*

Even though a trusted operating system is implemented on a relatively weak physical security framework, it can still provide substantial protection against unauthorized activities within the computer system that would be undetectable and unpreventable otherwise. For example, by manipulating computer records, an unauthorized individual can siphon resources from an untrusted system with very little risk and can falsify accounts or payments. With a trusted system, on the other hand, tight access controls and audit trails can be set up to both detect and discourage unauthorized actions in the computer system. Other kinds of threats may still continue to exist, but one class of unauthorized actions that are especially difficult to protect against would be effectively eliminated.

Protection of Assets and Resources

Several studies, congressional hearings, and GAO audits have scrutinized fraud and abuse in the disbursement of benefits in federal programs, and improper purchase, handling, and disposition of federal resources and property (reports of these investigations are listed in Appendix B). "Abuse" has been broadly defined as the improper utilization of a benefit or a benefit system; "fraud" constitutes abuse in which the utilization of the benefit is also illegal. The federal benefit programs surveyed have included all the major programs of the De-

*These regulations include Transmittal Memorandum #1 to Office of Management and Budget (OMB) Circular A-71, discussed in detail on pp. 20-21.

partments of Agriculture, Health and Social Services, Housing and Urban Development, Education, and Labor, as well as the Small Business and Veterans Administrations. The following (paraphrased) conclusions were reached in one of these reports [21]:

1. A "delivery at all costs" philosophy has pervaded agencies that manage benefit programs. Even when controls are in place, many program personnel either overlook or circumvent them to expedite processing of caseloads.
2. The type of enforcement mechanisms available and their effectiveness are basic to achieving control. While there has been a dramatic increase in the quantity and variety of control strategies employed, there has been little evaluation of the individual or aggregate value of such strategies in reducing fraud and abuse.
3. Fraud in most of the programs surveyed was committed by recipients (misrepresentation of eligibility), third-party providers (misrepresentation of services provided and overcharges), auxiliary providers (misrepresentation of services provided under contract), and agency administrative personnel (kickback payments, misrepresentation, overpayments, other falsification of information).
4. Proof of the seriousness of fraud and abuse has been obscured by inconsistent and inadequate data and by emotional media reports. The meager evidence currently available supports the finding that fraud and abuse extend into all types of benefit programs and are committed by a large cast of actors either singly or in collusion. Losses due to fraud and abuse in the 15 programs reviewed could amount to between $80 billion and $100 billion over the next ten years.

There is a clearly a need for improved protection of assets and resources in the computers of agencies that administer benefit programs or maintain other sensitive information in computer files. The use of trusted systems by these agencies has the potential of substantially decreasing the incidence of unauthorized and/or fraudulent use, manipulation, or disclosure of information.

Regulatory Compliance

A number of statutes and regulations require security mechanisms (physical, technical, and administrative) in civilian agencies of the federal government, although they seldom specify the method that is to be used. The major legislation is described briefly below.

The Paperwork Reduction Act of 1980 (chap. 35 of Title 44, United States Code, January 3, 1980). This Act charges the OMB with, inter alia, coordination of the Federal Information Policy, including aspects

dealing with management control and unauthorized uses of systems. The OMB is required:

> (5) to ensure that automatic data processing and telecommunications technologies are acquired and used in the Federal Government in a manner which improves service delivery and program management, increases productivity, reduces waste and fraud, and, wherever practicable and appropriate, reduces the information processing burden for the Federal Government.
>
> (6) to ensure that the collection, maintenance, use and dissemination of information by the Federal Government is consistent with applicable laws relating to confidentiality, including section 552a of title 5, United States Code, known as the Privacy Act.

These requirements are implemented by the Office of Information and Regulatory Affairs within the OMB. The Director of this Office is charged with a "privacy function" which includes [3504(f)]:

> (1) developing and implementing policies, principles, standards, and guidelines on information disclosure and confidentiality, and on safeguarding the security of information collected or maintained by or on behalf of agencies;
>
> (2) providing agencies with advice and guidance about information security, restriction, exchange, and disclosure;
>
> (3) monitoring compliance with section 552a of title 5 of the United States Code, and related information management laws.

In addition, the Office of Information and Regulatory Affairs reviews all federal agencies' information collection requests and reviews the information practices of all federal agencies (on a three-year cycle).

The Paperwork Reduction Act requires avoidance of duplication with other agencies in information storage and collection and promotes increased sharing of information and centralized information collection. Potential conflicts may arise here with the intent, if not the actual wording, of the Privacy Act of 1974.

Transmittal Memorandum #1, OMB Circular A-71 (July 27, 1978). The subject of the Memorandum is security of federal automated information systems. It establishes requirements for each agency of the federal government to implement a computer security program and defines a minimum set of controls to be incorporated into each such security program. It assigns to the head of each agency the responsibility for providing

> physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations as well as national security data.

This responsibility includes assuring that automated processes operate effectively and accurately, and establishing personnel security policies for screening individuals participating in the design, operation, or maintenance of federal computer systems or having access to data therein. Several levels of personnel screening, from minimal to full background investigation, are to be established commensurate with the sensitivity of the data handled by each agency and with the risk and magnitude of loss or harm that could be caused by misuse.

Applicable GSA Regulations. In accordance with the requirements of Transmittal Memorandum #1 of Circular A-71, the General Services Administration (GSA) formed a task group to codify the Transmittal Memorandum itself in the Code of Federal Regulations. The GSA issued or modified the following Federal Property Management Regulations (FPMRs) which address computer system or facility security requirements and, at least indirectly, should be considered in assessing needs for trusted systems:

1. FPMR 101-35.3, "Security of Federal ADP and Telecommunication Systems" (August 11, 1980). This FPMR establishes the policy that all federal agencies must ensure that an adequate level of security is provided for all ADP and telecommunications systems and services, including those provided by contractors. In particular, federal agencies are required to establish security programs that (a) ensure safeguarding of sensitive data from unauthorized disclosure, (b) provide for operational reliability of ADP systems, and (c) provide for asset integrity and prevention of losses due to natural hazards, fire, etc.

As a part of this security program, agencies are required to (a) develop security specifications for new and modified sensitive applications to meet users' requirements, (b) describe potential threats to the system and measures needed to protect against them, (c) conduct tests to demonstrate the adequacy of security provisions to meet the requirements of the applicable federal policies, regulations, and standards, and (d) develop procedures for certification of systems after the completion of the acceptance tests. Also covered are personnel screening, risk analysis, and contingency planning.

2. FPMR 101-36.7, "Environmental and Physical Security" (August 11, 1980). This FPMR discusses (a) computer system environmental factors such as temperature, humidity, cleanliness, electrical services, and fire safety, (b) authorizing and controlling access to ADP facilities, and (c) development of contingency plans to deal with events that could prevent normal operation.

3. Federal Procurement Regulation (FPR) 1-4.1107-21, "Computer Security Requirements" (October 6, 1980). This regulation requires that all solicitations for acquisition of ADP equipment, software, maintenance services, and supplies where sensitive applications are

involved must include computer security requirements as established and certified by the agency pursuant to Transmittal Memorandum #1 of OMB Circular A-71 and GSA FPMRs.

The solicitations are to include, whenever applicable:

a. Agency rules of conduct that contractor employees must follow.
b. A list of anticipated threats and hazards that contractors must guard against.
c. Descriptions of safeguards that user agencies require contractors to provide.
d. Testing methods and procedures to monitor and verify correct operation of the safeguards, and to discover and counter any new threats or hazards.
e. Any requirements for periodic risk assessment and for advising users of the security level of the system.

Evaluation of solicitations will include, when applicable, how well the solicitations have addressed security concerns, the presence of safeguards, and other security-related requirements.

Statutes with Security Requirements. A number of federal laws and agency regulations contain requirements for ADP system security. These security requirements are usually stated in very general terms, with implementation choices left to the discretion of the agencies and/or their ADP system managers. Laws and regulations containing ADP security requirements include the following:

1. The Privacy Act of 1974 (P.L. 89-306, December 31, 1974) requires federal agencies that maintain identifiable personal information about individuals to

> establish adequate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm to any individual on whom information is maintained . . . .

A pending amendment to the Privacy Act of 1974 (H.R. 1049, January 22, 1981) would alter the security requirement slightly, requiring in section (e)(1)(E) that each federal agency that collects or maintains individually identifiable records must

> establish reasonable administrative, technical and physical safeguards to assure the integrity, confidentiality and security of such individually identifiable records so as to minimize the risk of substantial harm, embarrassment, inconvenience, or unfairness to the individual to whom the information pertains.

The Act's security requirements are further elaborated in a supplement to OMB Circular A-108 [22] and in National Bureau of Standards FIPS PUB 41 [23].

The general requirements for personnel record-keeping systems, including access control, security, and accountability requirements, were issued by the Office of of Personnel Management on September 30, 1975, as revisions of Chapters 293 and 297 of the Federal Personnel Manual (described in FPM Letter No. 297-1, October 31, 1975, and attachments).

2. The Brooks Act (P.L. 89-306, October 30, 1965), which provides for efficient and economical management of federal ADP resources, contains an implicit requirement for management control.

3. The Crime Control Act of 1973 (P.L. 93-83) amends the Omnibus Crime Control and Safe Streets Act of 1968 to specifically require privacy and security of arrest records in federally supported state criminal-justice systems.

4. The Freedom of Information Act (5 USC 552, 1966) defines certain classes of personal and other information that may not be revealed publicly and that thus require access control safeguards. Examples are:

a. National security information that is classified and information specifically exempted by statute.
b. Trade secrets and commercial or financial information obtained from a person and required to be maintained as privileged or confidential.
c. Personnel and medical files and other files the disclosure of which would constitute a clearly unwarranted invasion of privacy and confidentiality.
d. Geological and geophysical information and data, including maps, concerning wells.

In addition, several specific types of ADP applications in federal agencies are subject to statutory requirements for protecting the confidentiality of data and providing security against unauthorized access or disclosure. For example, the Bureau of the Census must maintain data confidentiality under 13 U.S.C. 8, the National Center for Health Statistics under 42 U.S.C. 242m, and the Internal Revenue Service under the Tax Reform Act of 1976 (I.R.C. Sections 6103, 6110).

Management Control

Management control requirements in civilian federal agencies are similar to those discussed in Sec. II. Accountability must be established for disbursements of funds, processing and storage of regulatory information, determinations of eligibility for program benefits, acquisition of supplies and materials, and so forth. Agencies are increasingly using automated systems for payments, maintenance of invento-

ries, and disposition of surplus materials. The need for stronger management control over these systems and their operators has been emphasized in several GAO reports (listed in Appendix B).

An essential ingredient of management control in computer-based systems is internal control over access to or modifications of operational data. This control is implemented via the system software, especially that of the operating system. A trusted operating system can form a basis to which effective external controls can be added.

Safety and Integrity

Air traffic control computer systems operated by the Federal Aviation Agency (FAA) are an example of computer systems whose operations affect human safety and in which reliability and integrity are essential. As discussed in Sec. II, trusted systems and/or their development and verification methodologies can provide vital safeguards in this area.

Federal agencies also use, develop, and sponsor development of various computer models that can affect population safety. For example, the Nuclear Regulatory Agency operates models of nuclear reactor safety. The integrity of the models in these applications is critically important and could benefit from trusted system application.

Operational Economies

The potential for achieving operational economies through the use of trusted systems may vary widely among federal agencies. As discussed in Sec. II, expectations for such economies are based on trusted systems strengthening internal access controls and thereby permitting reduction of external controls.

In the absence of strong internal controls, external controls require additional security personnel, background investigations of users beyond the needs of their work assignments (i.e., operation at system-high clearance level), or the use of dedicated processing periods which reduce system efficiency. The recurrent costs of such external controls probably outweigh the recurrent costs of trusted systems (e.g., the reduction in performance that results from implementation of a trusted operating system). To date, experimental trusted operating system prototypes, such as KSOS-11, have been considerably slower than untrusted versions, but performance improvements can be achieved by the use of hardware or firmware features and by redesigning rather than emulating the operating system's programs.

Other Considerations

In general, security requirements in computer systems tend to be viewed by some operational personnel and management as hindrances to fulfilling the agency's mission and to performing their jobs efficiently. Security threats tend to be viewed as highly exaggerated. In particular, the following observations have been made:

1. Requirements for federal agencies to implement computer system security, such as those stated in Transmittal Memorandum # 1 of OMB Circular A-71, are not supported by appropriate funding. Agencies are expected to take funds from other areas of their budgets, which they are very reluctant to do, especially since implementation of these requirements is seldom enforced.

2. Agencies view the meeting of mission requirements and goals as the overriding objective. Security systems are perceived as reducing efficiency, interfering with operations, providing an overkill of protection, and costing too much. In agencies responsible for timely disbursement of benefit program funds, there is a tendency to tolerate overpayments or payments to ineligibles in order to avoid underpayments or the withholding of payments to eligibles. If denial-of-service threats became serious and could be averted by the use of trusted systems, acquisition of such systems would be much more likely.

3. Potential performance degradation due to the "complete mediation" of access requests in trusted systems is a concern in agencies where access request traffic is heavy. For example, one of the Social Security Administration's systems has over 1,500 terminals and over 20,000 users. However, while a trusted system may reduce the throughput of such facilities, these are precisely the high-risk/high-exposure institutions in which enforcement of management control is difficult and in which trusted systems will be required.

4. Some agencies feel that much improvement is still needed in physical and administrative security and in increasing employee security awareness, and that it would be futile to install trusted systems on the present weak physical security base.

5. Nearly all fraud in agency systems is in the form of unauthorized manipulation of input data, which is not perceived as controllable by a trusted system. But unauthorized use of applications programs, which also accounts for a substantial part of overpayments, could be controlled by trusted systems.

To summarize, most of the perceived reluctance to consider acquisition of trusted systems in civilian agencies of the federal government seems to stem from concern over potential losses of performance or efficiency, views that existing physical security is too primitive to warrant installation of trusted systems, and lack of budgetary support

or strong enforcement of security requirements. However, increased emphasis by the Administration on the curtailing of fraud in federal disbursements of funds could greatly reduce the the current inertia. Civilian agencies are not likely to sponsor the development of trusted operating systems even though these systems could be tailored to their security needs. But they would probably acquire trusted systems if they were available off-the-shelf and were fully supported, efficient, and inexpensive.

IV. APPLICATIONS IN STATE AND LOCAL GOVERNMENT

Computer applications are as extensive in state and local governments as in the federal government, but the number of computers used is considerably smaller. According to the National Association of State Information Systems (NASIS) [24], 681 computer systems were in use in state governments in July 1978. California was the largest user, with 49 computers; Mississippi was the smallest, with 2. (Civilian agencies of the federal government were using 2,118 at the same time.) The number of computers in state governments increased by more than 50 percent between 1973 and 1978 (from 421 to 681), and this rate can be expected to continue into the 1980s. In local governments, more than 90 percent of the cities with populations over 50,000 and counties with populations over 100,000 were using ADP in some form in 1975 [25], and of these, 78 percent owned their own computers.

The areas in which computers are most heavily used are, in descending order, accounting, law enforcement, treasury and collections, utilities, budget and management, personnel, and purchasing. Very few of these applications require security safeguards equivalent to those needed for classified national-defense information; certain types of investigative information related to organized crime, however, may require high levels of protection.

State and local computer systems maintain and disburse smaller amounts of resources than federal systems, but the relative impacts of losses of those resources due to computer fraud or penetration are likely to be just as great.

Collectively, state record-keeping systems probably maintain as much personal information on individuals as do federal systems. Much of this is public information, as defined by Public Records or Freedom of Information laws, which vary from state to state. However, an increasing proportion of personal information is becoming subject to privacy protection and associated security requirements.

Local governments maintain large personal information record-keeping systems, including property tax files, student school records, criminal justice and law enforcement files, and local welfare and medical care files. This information is also becoming increasingly subject to privacy protection.

Needs for Trusted Systems

The needs for trusted systems in civilian agencies of the federal government are broadly applicable to computer systems and applications in state and local government as well. There are some differences, however, especially in the area of regulatory compliance. Only a few states have enacted privacy protection or fair information practices laws, and there are no state directives comparable to Transmittal Memorandum #1 of OMB Circular A-71.

There is a trend in state and local legislative bodies to install or to contract for the use of computers to support legislative business—to maintain information on the status of active bills, calendars on committee meetings, vote tallies, and the like. Despite the public nature of legislative business, these ADP systems must have access controls and data integrity. Clearly, unauthorized manipulation of a bill's text could have far-reaching consequences. The need for a trusted system is especially evident when the legislative computer system must be shared with other state agencies or commercial clients.

As in other organizations, state and local government computer systems lack proper security measures. Moreover, an "it can't happen here" state of mind seems to exist in some state governments, as far as computer-based fraud and abuse is concerned [25]. To counteract this, organizations such as NASIS have developed computer security guidelines for state computer systems and have drafted model legislation for combating computer crime.

Protection of Assets and Resources

Information is an important resource in state and local legislative management information systems, as well as in administrative systems. It is especially important to maintain data integrity where data are used for actions that can have important economic consequences. Various groups may attempt to influence decisions in their favor by unauthorized data manipulation in decision support systems. Frauds have in fact been discovered in state-operated health care support programs and in welfare programs. However, as in the federal systems, these frauds have involved falsified input data rather than manipulations of records within the computer systems. Nevertheless, better security is needed in this area.

Regulatory Compliance

Each state has complete jurisdiction over the computer systems and applications of its state agencies, and also over some local government and private-sector computer systems. For example, fair information

practices (privacy protection) laws have been enacted in 10 states and are pending in several others.

The Federal Privacy Act of 1974 does not appear to extend to the state and local governments' record-keeping systems. However, certain state-operated benefit programs that involve federal funds are required to comply with data confidentiality and individual privacy requirements set forth in authorizing federal legislation. Furthermore, general legislation that is pending in Congress—H.R. 1061 (January 22, 1981), the Privacy of Public Assistance and Social Services Records Act of 1981—would require in Sec. 2(a)1 that each state

> shall provide, by one or more fair information practices statutes or laws, for such privacy and confidentiality of records used in and maintained by any State or private agency administering the program as the Secretary of Health and Human Services determines ....

The federally enacted Family Educational Rights and Privacy Act of 1974 (20 U.S.C. 1323g) is applicable directly to the local level without the need for a state law. It gives students and their parents the right to inspect the student's records (with some exceptions) but limits access by third parties, also with some exceptions. The disclosure limitation requires that confidentiality of records be provided and, by implication, imposes a requirement for access control and security mechanisms.

The state fair information practices and privacy statutes tend to be similar to the Privacy Act of 1974 in the privacy rights provided to individuals. In general, they apply to both state government agencies and local government entities in the state. These laws also contain the following data security requirements [26]:

1. The Arkansas Information Practices Act (16-801 through 16-810 of the Arkansas code) establishes an Information Practices Board with authority to prescribe, inter alia, "policies and procedures to insure the security of personal information systems including ... mechanics, personnel, processing of information, site design, and access ...."
2. The California Information Practices Act of 1977 (Title 1.8, chap. 1, section 1798.21) requires that "each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury ...."
3. The Connecticut Personal Data Act (CGSA Section 4-190) requires that each state agency "... take reasonable precautions to protect

personal data from dangers of fire, theft, flood, natural disaster, or other physical threats ...."

4. The Indiana Fair Information Practices Act (IC 4-1-6-1) states that all state agencies are required to "... establish appropriate administrative, technical and physical safeguards to insure the security of the information systems and to protect against any anticipated threats or hazards to their security and integrity ...."
5. The Massachusetts Fair Information Practices Act (C. 66A) requires that every holder maintaining data must "... take reasonable precautions to protect personal data from dangers of fire, theft, flood, natural disaster, and other physical threat ...."
6. The Ohio Personal Information Control Act (Revised Code, Sections 1347.01-10, and 1347.99) states that every state or local agency that maintains personal information shall "... take reasonable precautions to protect personal information in the system from any anticipated threat or hazard to the security of the system ...."
7. The Utah Information Practices Act (Section 63-30-10 and Section 63-2-68, Laws of Utah) requires that "... emphasis will be placed on the data security requirements of computerized files which are directly accessible by means of telecommunications, including security during transmission ...."
8. The Virginia Privacy Protection Act (chap. 26, Title 2.1, Code of Virginia) requires any agency maintaining an information system to "... establish appropriate safeguards to secure the system against any reasonably foreseeable threat to its security ...."

Fair information practices acts are also in force in Nebraska and North Dakota, and bills to enact similar statutes have been introduced in Alaska, Hawaii, New Jersey, New York, Rhode Island, and Wisconsin.

Various states have enacted legislation to provide confidentiality of medical, public health, income tax, and educational records maintained by state and local governments. Freedom of information and public records acts exempt various categories of information from disclosure, including, in some states, motor vehicle ownership and registration information.

Nearly all states have established regulatory authorities to oversee the collection, maintenance, access to, and dissemination of criminal-justice information. As of 1979, the following types of statutes or executive orders regarding handling of criminal-justice information were in effect [27,28]:

Type of Legislation	Number of States
Privacy and security councils	11
Dissemination controls	41
Data-quality requirements	42
Dedicated computer system	3
Access for research purposes	14
Separation of investigative and intelligence files	10
Security requirements	31
Transaction of logging	27
Freedom of information, except criminal-justice information	19

The level of detail in criminal-justice information legislation varies considerably from state to state. Privacy and Security Councils in some states have developed in-depth guidelines for criminal-justice information security. For example, the Georgia Crime Information Center requires participating local criminal-justice agencies to execute an agreement that sets up security requirements, including requirements for security features in system software. Security in computerized message-switching networks is emphasized.

In general, law-enforcement and criminal-justice agencies maintain that security can be assured only by using dedicated systems, completely isolated from outside users. However, very few states can afford the expense of a dedicated criminal-justice computer, and trusted systems can provide the required security in shared computer systems.

Management Control

Most state and local government computer systems operate under a centralized coordinating authority, typically in the Department of Finance. In some states, the authority is all-inclusive, and all data processing for state agencies is performed in a single facility [24]. Other states may have several facilities that service different agencies, and a few states do have a separate, dedicated computer system for criminal-justice data processing.

Centralized data processing has been the predominant mode in local governments, but a trend toward distributed processing is now developing as the result of increasing dissatisfaction with services provided by central systems. The maintenance and servicing of data and programs of many government agencies by the same system also increases the potential for unauthorized access.

Computer systems shared by many organizations that strive to control access to and use of their own programs and data have a special need for effective management control. Trusted systems appear to be an effective way to implement this control.

Safety and Integrity

Safety questions in state or local government computer systems primarily concern rapid transit systems (e.g., BART in the San Francisco area, and the Metro system in Washington, D.C.). Reliability and integrity are achieved in these systems by various techniques, although formal correctness proofs such as those used in trusted systems development are not used.

Correctness and continued integrity of computer models for evaluating design safety must be assured. Software for future real-time control systems or for safety-related modeling should therefore be based on trusted system development technology or should actually use a trusted system.

Operational Economies

State and local governments have not made substantial expenditures for computer security, except in criminal-justice and law-enforcement information processing systems. Personnel background investigations and clearances for access to sensitive information are virtually nonexistent. Thus, installation of trusted systems would not provide immediate cost savings. However, as data security requirements become increasingly important, trusted systems may provide a means to avoid future security-related expenses.

Other Considerations

State and local governments can be expected to find the costs of trusted systems—both acquisition costs and possible performance degradation—an important consideration in their acquisition. Managers of service-bureau-type state computer operations may be especially reluctant to sacrifice system throughput and efficiency for improved security. Thus, installation of trusted systems will require strong backing by top management.

Proposals to increase state and local government computer system security by installing trusted systems may even meet with criticism from public-interest groups. A recent study of local government computer applications [29] states that there is "mounting evidence that

systems implementation has made municipal agencies more costly to run, less responsive to the public and less equitable in meeting the needs of particular population groups." The study also states that these systems are operated by elitist groups which maintain tight control over information and use it to promote their own goals. Thus, increased security might be viewed by some as a further step toward increased secrecy in government. Hence, appropriate public-relations activities should be initiated as a part of a unified security-enhancement program to explain to the public the benefits of increased security measures.

V. APPLICATIONS IN THE PRIVATE SECTOR

Computer applications in the private sector of the United States encompass nearly every area of business and industry activity. In addition, "personal computing," which includes computers in small enterprises as well as computers in the home, is growing rapidly. More than 200,000 "regular" computers, over 1 million personal computers, and several million programmable pocket calculators are currently in use. These numbers are becoming extremely difficult to estimate.

Computers are used to handle personnel administration and payroll, accounts payable and receivable, inventories, production, sales, marketing, advertising, planning, financial management, regulatory reporting, research and development, and a multitude of other functions. Enterprises that provide services to clients—financial institutions, health care services, insurance carriers, private educational establishments, investment institutions, credit-granting organizations, and the like—maintain records on services being provided and on the clients who receive them. Electronic funds transfer systems (EFTS), electronic mail, and office automation are new, rapidly growing application areas. Most service-providing organizations depend on the accuracy and integrity of their computer programs and data files for successful operation and have a recognized need for access control and other computer security techniques.

Co[illegible]ers are also being used increasingly in the control of real-ti[illegible]ocesses, e.g., in oil refineries and automated assembly lines. Very high reliability and operational integrity are essential in these systems to minimize safety hazards to people, facilities, and equipment.

Needs for Trusted Systems

The definition of security and the requirements for it in the private sector tend to differ from those in the government. A recent analysis summarizes the need for computer security in private business and industry, especially in corporate management and operations systems based on ADP, as follows [30]:

1. Computers have become a basic resource in the operation of a business. The exception today is the *non-use* of computers in

business function, not the use of computers. The end effect of this is an extensive business dependency on computer systems.

2. The concern in business and industry is with the consequences of interruptions of ADP support, including security failures: loss of production, loss of assets, loss of confidentiality, and loss of customer services, as examples.
3. The broad business incentive is the prevention of failure of the information-system portion of business systems. From the ADP management point of view, the security objective is to provide business managers with trusted information systems.
4. Security may be defined as knowing your business procedures, being confident of their correctness and completeness, and being sure that they are in place. In general, the DoD trusted system concepts are necessary but not sufficient for private-sector information security.

There are no standard security requirements or personnel clearance levels in the private sector, nor is there a consensus that these are needed. Various industry associations have developed security standards for their own members, however. The security function, like any other business function, is regarded by top management as an economic one—*certain losses are viewed as tolerable if their prevention* is too expensive or if loss prevention interferes excessively with business operations. However, because of federal or state laws, certain aspects of security are mandatory.

As in government agencies, trusted systems are needed in the private sector for the protection of assets and resources, regulatory compliance, maintenance of management control, and safety and integrity. Additional incentives may stem from potential improvements in operational economies, marketing advantages, and enhancement of public image.

Protection of Assets and Resources

Nearly every organization in the private sector that uses a computer system has automated its payroll, accounting, and inventory systems and is likely to use various MIS features as well—for financial planning, product development, market research, production scheduling, and so forth.

The assets that are stored in the computer system and thus exposed to security risks include financial records, information necessary for business functions, trade secrets, and marketing data. They are subject to internally perpetrated fraud, industrial espionage, and vengeful actions by disgruntled employees or others who may object violently to an organization's policies or activities. The data base on such

computer-related crime in the private sector is thought to be substantial [15] (although most reports have been challenged as unverifiable [31]).

One study in 1975 of computer-related crime [15] shows 375 cases with an average loss of $450,000 (excluding the Equity Funding fraud which was committed by larcenous management and involved total direct and indirect losses of nearly $1 billion). About 20 percent of these cases were reported to have involved operating system integrity, time-sharing service use, or application program use; the rest, poor control, operating procedures, data entry management, and physical security. In total, they present an argument for better protection of assets and resources.

Regulatory Compliance

Privacy, confidentiality, and security requirements in federal and state laws regulate the type or functions of ADP applications in various private-sector organizations. Corporations are regulated by state corporation laws, and publicly owned corporations (i.e., those that have issued stock certificates) must abide by federal Securities and Exchange Commission (SEC) regulations. These regulations do not all contain explicit requirements for computer system security, but the need for security is generally implicit.

Personal Information Record-Keeping. In principle, personal information that is maintained in private-sector record-keeping systems is subject to the same privacy protection requirements as are provided in government systems. However, the federal and state privacy legislation has evolved toward "area by area" coverage of the private sector, rather than covering all parts in a single "omnibus" law. As a result, only a few areas are covered by federal legislation, and relatively few state laws have been enacted.

The following federal record-keeping legislation affecting the private sector has been enacted or is pending in the Congress:

1. The Fair Credit Reporting Act of 1969 (15 U.S.C. 1687 et seq.) applies to organizations that collect, maintain, and make available for a fee creditworthiness information on individuals. The Act focuses on individual rights. Disclosure to clients is the credit bureaus' business; thus, prevention of unauthorized access is mainly intended to maintain data integrity (a requirement of the Act) and prevent data thefts. Bills to amend the Act and broaden its coverage to depository institutions (H.R. 1046) and to insurance carriers (H.R. 1047) are pending.
2. The Family Educational Rights and Privacy Act of 1974 (20 U.S.C. 1232g) applies to any educational institution that receives federal

funds from the Department of Education. It grants certain privacy rights to students and their parents and restricts disclosure of educational records to third parties. Amendments to the Act are pending (H.R. 1048). Security provisions are needed in computer systems where student records are stored concurrently with other data, including student schedules, and in systems that are also used by students in course work. H.R. 1048 addresses the use of student records for research purposes and requires that "... adequate safeguards to protect the record or information be established and maintained by the recipient, including a program for removal or destruction of identifiers."

3. The Financial Privacy Act of 1980 (12 U.S.C. 3401) applies to banks and restricts access to depositors' bank transaction records by government agencies. Pending is a bill, H.R. 1046, which in part also addresses Electronic Funds Transfer Systems (EFTS) but includes no statements on EFTS security requirements. These systems are certain to be subject to future federal legislation.

Pending federal laws and enacted or pending state laws apply to records maintained in several types of private-sector enterprises:

1. A large fraction of the clients of public-assistance and social service organizations are covered by state or federal benefit programs. Laws related to these programs apply to the private programs as well, including requirements related to data privacy, confidentiality, and security. A federal law to amend the existing personal-information-related legislation (H.R. 1061, Privacy of Public Assistance and Social Services Records Act of 1981) is pending in Congress. This law requires privacy protection and record confidentiality, including controlled, selective access (see section 3(5)).
2. Medical and public health records are regarded as confidential in nearly every state, and therefore access to them must be restricted. The following general security principle for medical records has been formulated [32]: "Because of the sensitivity of the personal information stored in a health data system, security measures must be taken to limit access by personnel within the organization to those who need to see particular information items in a record, to monitor data uses in order to detect unauthorized conduct, and to protect files against outside penetration."
3. Pending in Congress is H.R. 1059, the Privacy of Medical Information Act of 1981, which would establish privacy protection and confidentiality requirements on health care institutions treating Medicare or Medicaid patients. The legislation covers hospitals, nursing facilities, intermediate care facilities, home health agencies, and

health maintenance organizations. Data-security requirements are not stated in this bill, but they are clearly implied by the requirements for medical information confidentiality and disclosure limitations. Another pending bill, H.R. 1061, would require safeguards to prevent unauthorized disclosure of personal medical information that is maintained for statistical and research use.

4. Federal legislation related to personal information privacy protection and confidentiality presently does not cover the insurance industry. However, H.R. 1047, pending in Congress, would amend the Fair Credit Reporting Act to provide privacy and confidentiality in record-keeping systems maintained by insurance carriers, with particular emphasis on medical information. In 1980, bills were pending in eight states to apply fair-information-practices principles to insurance records.
5. Financial and credit information is covered by the Federal Fair Credit Reporting Act and also by 16 similar state laws. Limitations on disclosure for other than credit determination purposes are specified and in turn imply requirements for access control and security.
6. Confidentiality of employment records is required by law in five states. Most of these laws provide access rights to employees and limit disclosures, thereby implying access controls and security. Further discussion of employment-record confidentiality and privacy requirements is found in Ref. 33, which points out the need for access controls in any data base that also contains other records and in computer systems where employment records may be processed concurrently with other data-processing tasks.

The report of the Privacy Protection Study Commission [34] contains detailed data and specific recommendations regarding privacy protection and confidentiality of credit, financial, insurance, employment, medical, welfare, and educational records maintained by federal and state agencies and by organizations in the private sector.

Accountability Requirements. The Federal Securities and Exchange Act of 1934 (15 U.S.C. 78) defines certain accounting requirements for publicly held corporations. These corporations are required to establish internal controls to safeguard assets against loss and to provide reliable financial records for internal use and for external reporting purposes. Similar requirements are established in state corporation codes. The internal control and auditing procedures implemented to comply with these statutes usually involve the following elements:

1. Competent, trustworthy personnel with clear lines of authority and responsibility.

2. Adequate segregation of duties.
3. Proper procedures for authorization.
4. Adequate documentation and records.
5. Proper procedures for record-keeping.
6. Physical control over assests and records.
7. Independent (internal) checks on performance.

In organizations that use ADP, these controls are applied to programs and data bases; to data acquisition, storage, and processing; to report generation; and to data communication software, hardware, and personnel. Development of effective controls and auditing procedures is still a difficult problem, but progress is being made [16,17]. The use of trusted computer systems promises considerable enhancement of control effectiveness.

The Federal Foreign Corrupt Practices Act of 1977 (P.L. 95-213) amends the Securities Exchange Act of 1934 by inserting Title I to strengthen the accounting and accountability requirements. Section 102 of Title I, Accounting Standards, states that:

> (2) Every issuer which has a class of securities registered pursuant to section 12 of this title and every issuer which is required to file reports pursuant to section 15(d) of title shall—
>
> (A) make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transitions and disposition of the assets of the issuer; and
>
> (B) devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that—
>
> (i) transactions are executed in accordance with management's general or specific authorization;
>
> (ii) transactions are recorded as necessary to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and to maintain accountability for assets;
>
> (iii) access to assets is permitted only in accordance with management's general or specific authorization; and
>
> (iv) the recorded accountability for assets is compared with existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

The impact of this Act on publicly held corporations is to require further strengthening of internal control and accountability along the lines described above. In 1980, the SEC proposed (and then withdrew) a set of rules [35] which discuss internal control and explain the notion of "reasonable assurance" as follows:

> The concept of reasonable, as opposed to absolute, assurance is incorporated in the proposed rules in recognition that it is not in the interest

> of shareholders for the cost of internal accounting control to exceed the benefits thereof. Such benefits, and in many cases such costs, are not likely to be precisely quantifiable. Therefore, many decisions on reasonable assurance will necessarily depend in part on estimates and judgments by management which are reasonable under the circumstances.

Improved internal control may bring about not only quantitative benefits, such as reduced exposure to theft of assets, but also qualitative benefits, including preservation of the good reputation of a company and its management.

International Laws and Regulations. Within the last 8 years, privacy and data protection laws have been enacted in several European countries and in Canada [36]. In addition, a convention on privacy protection is being ratified by the member countries of the Council of Europe [37], and a set of voluntary privacy protection guidelines has been completed by the Organization for Economic Cooperation and Development (OECD) [38], which includes the United States, Japan, Canada, and Australia.

The foreign data protection laws and international agreements contain requirements for privacy protection, data confidentiality, and data security in international data transfers, especially when personal information on either natural or legal persons is involved. They affect so-called multinational corporations and the data processing networks that provide services in Europe using U.S.-based computer systems.

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, September 1980 (Annex, Part 2, sec. 11), state that "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure." The United States has voted to approve the OECD Guidelines and U.S. private-sector organizations that are affected have been urged to voluntarily abide by them.

Data-protection laws have been enacted in Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, and Sweden and are pending in several other countries. The Austrian Data Protection Act (1978) applies to natural and legal persons. It requires that "the processor shall, having regard to economic feasibility and technical possibilities, introduce organizational, staff, technical and structural security measures. Such measures shall, having regard to the type of data and technical facilities and to the scale of processing, [ensure] that data are not unlawfully disclosed or brought to the knowledge of third parties and cannot be consulted, processed or disclosed by unauthorized persons."

The French Act on Data Processing, Data Files, and Individual Liberties (1978) states: "Any person processing personal data or ordering such processing shall thereby undertake, vis-à-vis the persons con-

cerned, to see that all necessary precautions are taken to protect the data and in particular to prevent these from being distorted, damaged or disclosed to unauthorized third parties."

The Federal Data Protection Act of the Federal Republic of Germany (1977) spells out the security requirements in considerable detail:

> Where personal data are processed automatically, appropriate measures suited to the type of personal data to be protected shall be taken to ensure observance of the provisions of this Act:
>
> a. Unauthorized persons shall be refused admission to data processing facilities which process personal data that are restricted (admission control);
> b. Persons employed in the processing of personal data shall be prevented from removing storage media without authorization (leakage control);
> c. Unauthorized input into the memory and the unauthorized examination, modification or erasure of stored personal data shall be prevented (storage control);
> d. The use by unauthorized persons of data processing systems from which or into which personal data are disseminated by means of automatic equipment shall be prevented (use control);
> e. It shall be ensured that persons entitled to use a data processing system have access by means of automatic equipment only to the personal data to which they have a right of access (access control);
> f. It shall be ensured that it is possible to check and to establish to which bodies personal data can be disseminated by means of automatic equipment (dissemination control);
> g. It shall be ensured that it is possible to check and establish what personal data have been input in data processing systems, by whom and at what time (input control);
> h. It shall be ensured that personal data processed on behalf of other parties are processed strictly in accordance with the instructions of the principal (control of processing on behalf of other parties);
> i. It shall be ensured that data cannot be read, modified or erased without authorization during their dissemination or during transport of relevant storage media (transport control); and
> j. It shall be ensured that the internal organization of authorities of enterprises is suited to the particular requirements of data protection (organization control).

Nearly all the cited laws require the organizations that are affected to obtain some form of prior licensing or approval by data-protection authorities, who examine and evaluate the security features of the systems being examined. The use of trusted systems may satisfy many of the above requirements for internal access controls.

Management Control

As in government agencies, management control is necessary in any activity of a private-sector organization, particularly in computer

systems and where stored data and data processing can be examined only indirectly. For example, it is not readily apparent from observing an employee interacting with a computer at a terminal that he is performing only authorized operations.

The internal control functions and procedures and the internal auditing techniques have the following purposes:

1. To establish a foundation for maintaining discipline and enforcing administrative procedures and policies.
2. To maintain accountability of employees and the capability to assign responsibilities meaningfully.
3. To provide confidence in the system, in the data integrity it provides, and in the information it produces.
4. To reduce the risk of fraud or other unauthorized activities.
5. To ensure that a prudent course of action has been taken in the system's operation.

Since the principal foundation for implementing management control in computer systems is operating system procedures, these procedures must be verified to be correct. The trusted operating systems described in Sec. I will be correctly designed and implemented and will be certified. Thus, they will form a reliable base for effective management control.

Safety and Integrity

Computers are used for process control in oil refineries, the chemical industry, the steel industry, and automated assembly lines, to name but a few private-sector applications of real-time control systems. Because these systems require high levels of reliability and continued integrity of control programs and data, they are suitable candidates for the use of trusted systems or their design concepts and methodology. Failure to take due care in the design and operation of automated control systems is likely to involve financial liability and generate problems with regulatory agencies, even if no disastrous events take place.

Design automation is proliferating, especially in the aerospace industry, where computer models are used to assist in design decisions, planning, etc. Likewise, computations of structural strength in civil engineering applications are often based on structural analysis programs, as are subsequent specifications of construction details. Errors can be costly, or even disastrous, particularly in sensitive applications such as nuclear power plants. Users must have assurance of correct design and implementation and continued integrity of these models. Trusted systems and their development methodology are applicable.

Operational Economies

The use of trusted operating systems in private-sector computer applications could result in

1. Reduced costs of personnel security procedures.
2. Elimination of the need to operate duplicate systems or maintain redundant data bases.
3. Easier auditability, with resultant cost savings.
4. Reduced security enforcement, training, and education costs.
5. Savings on insurance, bonds to protect client data, and bonding of employees.

Cost savings are always important in private-sector organizations. If a proposed trusted system cannot reduce costs related to security, management, and/or control, an acquisition decision may still reasonably be based on the potential for loss avoidance, which could be determined roughly by applying security risk assessment techniques [39,40].

Marketing Advantages

Numerous business firms in the private sector, e.g., banks and other financial institutions, mutual funds, and investment companies, hold and manage their customers' assets. They must provide financial returns to the customers, and the customers must have confidence that their assets are being properly handled and safeguarded. These institutions are continually seeking new ways to gain competitive advantage. The use of trusted systems would be very attractive to customers who are particularly concerned over the safety of their assets.

Customers of other organizations such as computer service bureaus who are similarly concerned with the security of the data or programs they submit for processing or storage are also likely to choose an organization that provides better safeguards, such as the use of trusted systems.

Enhancement of Public Image

Nearly all private-sector organizations are concerned about their image in the marketplace and in society at large. They wish to be perceived as being concerned over the well-being and rights of their customers and over societal needs in general, as well as being providers of excellent services or products.

Organizations that handle large amounts of personal information on individuals, such as financial and credit-granting institutions, insurance companies, health care organizations, and credit bureaus, expend resources to emphasize their concerns for customers' and public welfare. They focus on safeguards they have implemented to assure that customers' personal information is not accessed or disseminated to unauthorized parties, and that data integrity is maintained. The IBM Corporation and the Aetna Life Insurance Company have recently published advertisements in national magazines on the privacy protection safeguards they have voluntarily implemented in their systems.

Organizations are also concerned with their public image regarding asset and resource protection. Clearly, no organization welcomes the publicity that results from computer fraud or losses or from having been victimized by a computer crime. The reluctance to report suspected computer crimes attests to this. The use of trusted systems could reduce the possibility of adverse publicity by reducing the probability of occurrences.

Other Considerations

The all-important issues in the private sector are business economics, ability to remain competitive in the marketplace, and making a return on stockholders' investments. Acquisition of computer systems or any other equipment is a business decision made in view of these issues. Thus, there is a natural tendency in the private sector to view the acquisition of a trusted computer system also as a purely dollars-and-cents question. In addition, a trusted system either must be shown to be cost-effective in comparison with other security techniques that could achieve a comparable level of protection or it must provide additional benefits that justify any additional cost. The impact of trusted system implementation on the performance of the corporate computer system and any requirements to modify existing applications software or data bases are of particular concern. It is not surprising, therefore, that some private-sector ADP system managers are skeptical about the need for trusted systems in their organizations and about the cost-benefit aspects of trusted systems.

However, as discussed extensively in this section, the acquisition of a trusted system is not just a matter of business economics. There are numerous important considerations—protection of assets and resources, regulatory compliance, public image, management prudency—that are likely to be the deciding factors. In more technical terms, it is certainly true that while a trusted computer system can reduce

the need for the more conventional security techniques, it does not eliminate entirely the need for physical, administrative, personnel, or communication security techniques, nor can it fully handle a denial-of-service threat by authorized users or system personnel. But it provides a trustworthy base for implementing sets of discretionary protection mechanisms for monitoring denial-of-service threats and generating tamperproof evidential audit-trail records.

Concerns over performance or efficiency losses resulting from the use of trusted systems and the need to justify what some people see as a "deliberate reduction of service" are valid and understandable, as are concerns over possible large-scale conversions of applications software or data bases. Many performance concerns are based on a single, experimental data point—the preliminary results in KSOS-11 development, where emulation of the UNIX operating system on PDP-11 computers resulted in a substantial performance slowdown on the untuned system. However, in KSOS-6, implementation of the UNIX emulator on the SCOMP hardware (a specially modified Honeywell Level 6 minicomputer) has resulted in a much smaller performance slowdown. There is a general trend in the development of applications software to include features that are also very useful for implementing performance-efficient trusted systems; thus, performance loss is likely to be much less of a problem in the future, and there is some reason to believe that the performance costs of trusted systems will be negligible, or even nonexistent, as the experience base grows.

Any sizable application software or data base conversions that are required by the acquisition of a trusted system are certainly cause for concern. However, if the TCB is compatible with an existing (untrusted) operating system, software that ran under the operating system can be run on the trusted operating system with only minimal conversion. Such compatibility was a design goal for the KVM/370 and KSOS and has been successfully demonstrated with the KVM system. If the TCB and the existing operating system are not compatible, the conversion could be a significant part of the price of having a trusted application.

In general, concerns over performance losses or software conversion have been expressed whenever important innovations have been introduced, including the present-generation operating systems, with their resource-sharing capabilities. However, as vendors have become more experienced, many of the perceived problems have either failed to materialize or have been solved effectively and efficiently. It is highly likely that this will be the case in trusted systems development as well.

VI. THE PROSPECTS FOR AVAILABILITY OF TRUSTED SYSTEMS

Whether or not trusted operating systems will be widely available within the next 3 to 5 years in a sufficient range of protection levels and hardware bases to satisfy the needs of government and the private sector will depend on the computer industry's perception of the size of the potential marketplace; the costs of developing trusted systems, having them certified, and maintaining them (in the sense that software is maintained now); and the profits that manufacturers and distributors can expect to make.

The Potential Market

System software vendors are primarily concerned with whether or not a proposed system will have a sufficiently large market to justify its development costs. We must make a distinction here between (1) large vendors of computer systems and associated software and (2) software houses. The trusted system development decision is much more complex for large vendors, because they must consider the issue of compatibility of new software with existing applications, systems, and equipment, and that of maintaining compatibility in the future. The introduction of a new operating system (or a family of operating systems) is more difficult to justify for an organization whose existing software base is large. Software houses, on the other hand, are likely to have less stringent requirements for maintaining across-the-board compatibility with their existing products, but they are more dependent on vendors' changes of hardware bases.

We have not attempted to determine the quantitative marketing opportunities for trusted systems, but we can make some qualitative observations. First, there seems to be a consensus among vendors that the government (federal, state, and local) does not in itself constitute a sufficiently large market to support the development, certification, and maintenance of trusted systems. However, the market is not insignificant, and if future RFPs require the use of trusted systems, vendors may be compelled to produce them in order to remain viable in the government marketplace.

Second, most of the market for trusted systems in the civilian agencies of the government and in the private sector will probably be for Level 1 through Level 4 systems (as defined on p. 3). Some organiza-

tions in which asset protection or safety is very important may need higher-level systems. Some of the latter will be developed to satisfy the DoD needs once the state of the art permits such development, regardless of other markets. In all cases, the important aspect is that these systems have been *certified* to provide the specified level of protection.

Production of Trusted Systems

The trusted operating system concept involves the establishment of a completely separate, or virtual, environment within the computer for each concurrent user. Most existing operating systems are modifications of earlier batch-processing designs, updated to accommodate multiprogramming and time-sharing. In these systems, the mechanisms to accomplish shared concurrent use are scattered throughout the operating system, making the TCB very complex, and are not completely isolated from users. Thus, these operating systems are not currently secure, and it may be infeasible to upgrade them to the point where they become demonstrably secure (or reach a higher level on the Evaluated Products List).

Computer vendors recognize the implications of this problem—it affects much more than just the security aspects of a system—and they are gradually developing system architectures that can create fully isolated processing environments. But the need to maintain compatibility with existing systems weighs importantly against drastic changes, as does a certain inertia of designers who are familiar with existing architectures and design principles and therefore are reluctant to change. Users' system programming staffs have the same sort of inertia, and as a result, the few operating systems that do use virtual machine concepts, Honeywell's MULTICS and IBM's VM/370, have until quite recently found relatively little use even though they have been available for ten years.

The compatibility problem is not entirely untractable, however. The virtual machine concept permits each user to run his own operating system under the control of the virtual machine monitor (VMM), which is essentially transparent to users. This generality will necessarily result in some loss of performance, but the loss can be compensated by the faster hardware that is becoming available. The increasingly clear-cut needs for the capabilities that only trusted systems can provide will lead to greater user acceptance—and demand—which should provide a strong incentive for vendors to incorporate the necessary architectures in their new operating systems. For example, the VM/370 maintains many compatibilities for users of IBM systems.

Three trusted-system development prototypes, sponsored by the

DoD Computer Security Initiative, are now being tested to demonstrate the feasibility of design, implementation, verification, and operational use of trusted systems [1]. As the marketplace for trusted systems expands, uncertainties such as the compatibility question will be resolved and vendors should begin to incorporate trusted systems technology into their new product lines.

Evaluation and Certification

Certifiable trusted systems are difficult to develop unless the criteria for certification are unambiguous, reasonable, and clearly stated. Three sets of factors have thus far been identified by the Initiative program [6,11]: protection policy, mechanisms, and assurance. While the policy may vary from user to user, the mechanisms and assurance tend to employ a common set of technical approaches. The protection policies, too, form a hierarchy, since the goals of each are the same, and differences are those of degree only. A basic trusted system framework can be "customized" to satisfy the user's protection policy by applying appropriate mechanisms. Certification will then be based on the embedded policy.

A protection policy specifies the conditions under which information and computer resources may be shared, typically placing controls on the disclosure and modification of information. Given a clear and concise formal statement of protection goals, it will be possible to evaluate whether or not the system meets those goals.

To be effective, the hardware and software mechanisms that enforce the protection policy must be complete and verifiable. They must also be self-protecting against unauthorized actions or inadvertent intrusions by users or their programs. Operating systems that are poorly designed will not only fail to confine users to their authorized actions and data, but they may also undermine discretionary protection mechanisms provided by the users in applications programs. Thus, evaluation must necessarily concentrate on operating systems and their related software and hardware controls, particularly those relating to detection and prevention of policy violations, recovery from errors, and system operations and maintenance.

Absolute assurance that implemented mechanisms can provide the protection that they promise will never be possible, but steps can be taken in the design, implementation, and validation phases of a trusted system's development to raise confidence to a high level. Such techniques include top-down design, structured programming, and other techniques collectively known as "modern programming practices."

Support

Computer software tends to be a complex commodity in that throughout its life cycle, numerous changes are inevitably made to meet modified design requirements, to increase efficiency, and to improve user interfaces. These changes are usually the vendor's responsibility, and an operating system typically moves through a series of "releases." Any new release of a trusted system that involves changes of critical portions of the TCB will require reexamination of the previous certification. In such cases, if the system is to keep its rating, the Evaluation Center and the vendor must jointly analyze the changes and the extent of recertification needed. Clearly, it is important for the vendor to minimize changes in the TCB (but changes in the non-security-relevant portions of the system can be made as needed, since they will not involve recertification).

VII. CONCLUDING REMARKS

The DoD Computer Security Initiative program is now demonstrating the feasibility of designing and implementing trusted computer systems that can provide high levels of protection to data, programs, and processing in certain constrained operational environments. Ultimately, full, multilevel secure operation will be possible in unconstrained operational environments. But, of course, physical, administrative, personnel, and communications security will always be required.

An Evaluation Center for trusted systems is being established for the DoD at NSA. This Center will maintain an Evaluated Products List of systems submitted to it. Before an Evaluated Products List can be of practical value, however, the need for trusted systems in the government and the private sector must be sufficiently great for system vendors to perceive a marketplace beyond national-defense requirements that warrants submission of their systems for evaluation.

Trusted systems can contribute effectively to the solution of the growing problems of protection of assets and resources, compliance with laws and regulations, assurance of safety and integrity, and implementation of full management control. In addition, trusted systems may provide operational economies, marketing advantages, and public-image enhancement. They are needed in a variety of applications that constitute a market that should be of considerable interest to vendors, and that should strongly encourage participation in trusted system development efforts. The use of trusted systems is in the interest of private business and industry, as well as of public policy, public safety, and national welfare.

Appendix A

GLOSSARY OF TECHNICAL TERMS*

access. The ability and the means necessary to store or retrieve data or to communicate with (i.e., provide input or retrieve output from) or otherwise make use of any resource in a computer system.

access control. A strategy and mechanisms for protecting data, programs, and other items from unauthorized access.

access mode. A distinct operation recognized by the computer's protection system as a possible operation on an object (for example, *read*, *write*, and *append* are possible modes of access to a file; *execute* is a mode of access to a program).

accountability. The property that enables violations or attempted violations of system security to be traced to individuals who may then be held responsible.

accreditation. The final acceptance of a system to be used in a specific operational environment.

activity principle. A security model rule which states that once an object is made inactive, it cannot be accessed until it is made active again.

administrative security. The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide an acceptable level of protection to sensitive information outside the computer system.

ADP. Automated data processing (used synonymously with EDP, electronic data processing).

assurance. A measure of the degree of confidence that can be placed in the protection mechanisms, both hardware and software, in a trusted system.

audit. An independent review and examination of system records and activities, performed to test the adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend indicated changes in controls, policy, and procedures.

audit trail. A chronological record of system activity which is sufficient to enable reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

auditability. The property that enables effective audit and generation of audit trails.

authenticate. To confirm the identity of a person (or any other agent external to the protected system) making an access request.

authorize. To grant a subject access to a certain object in a certain specified access mode.

backup. Provisions made for the recovery of data files or program libraries and for restart of processing or replacement of ADP equipment after a system failure or a disaster.

*Based, in part, on a glossary developed by the Mitre Corporation for the DoD Computer Security Initiative Program and in part on the definition of terms in Army Regulation AR 380-380.

benign environment. An operating environment protected from external, hostile elements by physical, personnel, and administrative security mechanisms; a controlled mode of operation in which the system is protected at the system-high level and all users are cleared to the highest level but do not necessarily have a need-to-know for all data.

certification. The application of policy doctrine and examination of technical evidence about a system to determine the prudence of its use in a particular operating environment for a particular application that requires security.

classification. See *security classification.*

clearance. An authorization allowing an individual access to classified information; it indicates the maximum classification level the individual may access as well as the need-to-know categories.

communications security. The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunication messages.

complete mediation. Checking of every access request within the computer system for authority of the subject making the request to access the requested object in the requested access mode.

compromise. The disclosure of classified information to persons not authorized access thereto.

computer abuse. A general term that refers to any uses of computers for fraudulent or illegal purposes or for perpetrating a computer crime, as well as to unauthorized actions against a computer system itself (such as destruction of the system or its components).

computer crime. Use of computers to perpetrate fraud, extortion, or other crimes; malicious unauthorized access to and use of a computer system or its resources (a general definition being used in state computer-crime laws).

computer security. See *security.*

confidentiality. A status afforded to private and/or sensitive data that requires limiting access to these data.

confinement. Allowing a process executing an arbitrary program to have access to sensitive data while ensuring that the data cannot be misused, altered, destroyed, or released by the process.

confinement property. See *security *-property.*

controlled security mode. A mode of system operation in which some users have legitimate access to the system but have neither a security clearance nor a need-to-know for all classified material contained in the system. Internal hardware and software must be provided and approved for maintaining isolation of data and users with different classifications and clearances, respectively.

correctness proof. A verification by formal methods that the implementation of a system fully corresponds to its specification. Once a system is proved correct, it can be anticipated to perform as specified but not necessarily as originally envisioned if the specification was incomplete or inappropriate.

data protection. A term used in foreign laws to denote privacy protection afforded to individuals vis-à-vis personal data about them in computerized record-keeping systems.

data security. Protection of data against accidental or deliberate modification, destruction, or disclosure.

dedicated processing mode. In government installations, a mode of operation in which the computer system, its connected peripheral devices, and

remote terminals are exclusively used and controlled by specific users or groups of users who have security clearances and need-to-know for all classified material contained in the computer system.

denial of service. The prevention of authorized access to computer resources, or deliberate delaying of time-critical operations.

design verification. The use of verification techniques, usually computer-assisted, to demonstrate a mathematical correspondence between an abstract security model and a formal system specification.

discretionary access controls. Access controls to computer data or programs that may be changed by their creator/owner. More generally, mechanisms in the computer system which allow a user to decide, at his own discretion, which of his own access rights to give to any other user.

discretionary security. "Need-to-know" security requirements which may be developed and applied locally.

DoD. The U.S. Department of Defense.

DoD security policy. The complete body of law, regulations, and policy concerning the safeguarding of national security information. The basic policy establishes three classification designations and several categories of non-discretionary access control and requires that anyone accessing controlled information have an appropriate personnel security clearance level and a need-to-know for the information in question.

DoD security policy model. A version of the Bell-LaPadula model, which is an access-control-type model based on state-machine concepts. In the model, the entities are subjects (active entities such as processes) and objects (information containers). Every subject and object must be assigned a security level. The notion of a "secure" state is defined, and an inductive proof of the system security can be given: The initial state is shown to be secure, and every state transition is shown to preserve this property. A system state is defined as "secure" if the only permitted accesses of subjects to objects are in accordance with specified security-level restrictions: A subject is permitted read-access to objects that have security levels equal to or less than its own security level (the "simple security condition") and to write data into objects with security levels equal to or greater than its own level (the "security *-property"). State transitions preserve the secure state in accordance with the tranquility, erasure, and activity principles. Also included is an integrity model which incorporates a "simple integrity principle" and an "integrity *-property."

emulator. A combination of hardware and software that permits programs written for one computer to be run on another computer.

environment. See *operational environment.*

erasure principle. A security model rule stating that information containers (objects) must be purged of all residual information before being activated or reassigned to another subject.

Evaluated Products List. A list of all computer systems that have had their protection mechanisms evaluated.

evaluation. Determination of the protection level of a computer system.

Evaluation Center. A government facility established for the purpose of evaluating the security mechanisms of computer systems, assigning protection levels to systems, and maintaining the Evaluated Products List. Such a facility is being established at the National Security Agency for the Department of Defense only.

fair information practices. Procedures mandated by law to assure that individuals can exercise their privacy rights vis-à-vis record-keeping organizations that maintain personal information about them.

formal specification. The unambiguous description of hardware or software in a language with a well-defined syntax and semantics. These specifications give a precise mathematical description of the behavior of the system being specified. Computer-readability of these specifications allows for automation of various phases of the verification.

GAO. The U.S. General Accounting Office.

GUARD. A trusted computer system that acts as an interface between two computers at different security levels and allows data to flow between them in a secure and controlled manner.

hardware security. Computer equipment features or devices used to prevent unauthorized access to data or system resources.

identification. The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to the computer system.

implementation verification. The use of verification techniques, usually computer-assisted, to demonstrate mathematical correspondence between a formal specification and its implementation in program code.

inadvertent disclosure. Accidental exposure of sensitive or classified information to a person not authorized to have access. This may result in a security compromise or, in benign environments, a need-to-know violation.

integrity. The assurance, under all conditions, that a system will reflect the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and the consistency of the data structures and accuracy of the stored data. In a formal security model, integrity is interpreted more strictly to mean protection against unauthorized modification or destruction of information.

internal controls. Management controls, including administrative security procedures, implemented within an organization.

isolation. The containment of users, data, and resources in an operating system in such a way that users may not access each others' data and resources and may not manipulate the protection controls of the operating system.

kernel. *See security kernel.*

KSOS. Kernelized Secure Operating System. A project to strengthen the UNIX operating system with a security kernel to make it suitable for multilevel secure operation.

KSOS-6. The KSOS implementation on Honeywell, Inc., SCOMP hardware (a modified Honeywell Level 6 minicomputer) for communications front-end processor applications.

KSOS-11. The KSOS implementation on the Digital Equipment Corporation (DEC) PDP-11/45 and PDP-11/70 computers.

KVM/370. Kernelized VM/370 operating system. The kernelized version of the IBM virtual machine operating system, VM/370, for the Series 370 architecture, being built and verified by the System Development Corporation.

management control. Administrative procedures and technical mechanisms that assure that management's directives are followed and that management is fully aware of the organization's activities.

management information system. A computer-based system that contains information on an organization and its activities, and on the environment in which it operates, for the purposes of planning, decisionmaking, and operational control.

mandatory security. See *non-discretionary access controls.*

MIS. Management Information System.

MULTICS. Multiplexed Information and Computing Service. A general-purpose time-sharing system developed for a number of computers in the Honeywell Information Systems, Inc. (HIS) line, among them the HIS 643 and 6180 computers. MULTICS has been enhanced to allow limited multilevel operation and is presently used in the Air Force Data Services Center in a security mode where not all users are cleared for all the data in the system (see *controlled security mode.*)

multilevel security. A mode of operation permitting data at various security levels to be concurrently stored and processed in a computer system where at least some users have neither the clearance nor the need-to-know for all classisfied material contained in the system. Separation of users and material on the basis of security level and clearances is accomplished by the operating system and associated system software or hardware.

NASIS. National Association for State Information Systems.

need-to-know. A user's job-related requirement for access to specific information. Need-to-know implies discretionary access control to information, even though the users in question may have all the necessary clearances.

non-discretionary security. That aspect of the DoD security policy which restricts access on the basis of security classification levels. A security level may be composed of a classification level and a category restriction. To access an item of information, a user must have a clearance level greater than or equal to the classification level of the information and must also have a category clearance that includes the access categories specified for the information.

object. In a formal security model, an identifiable resource, data container, or related entity of the system; the counterpart of subject. Examples are software-created entities such as files, programs, and directories, and hardware resources such as memory blocks, disk tracks, terminals, and tapes.

OECD. Organization for Economic Cooperation and Development. An international organization located in Paris, of which the United States is a member.

operational environment. The sensitivity/classification levels of the information being processed, the clearance levels of users and personnel, the capabilities of the users of the system, the nature of the facility, the security-related features at the location, the security modes employed, and physical, administrative, and personnel security mechanisms being employed.

password. A protected word or a string of characters that identifies or authenticates an authorized user, a specific resource, or an access mode.

penetration. The successful, repeatable, unauthorized extraction of recognizable information from a protected computer system, or the capturing of control of the computer system.

penetration testing. Attempts by special teams to penetrate a computer system for the purpose of identifying any security weaknesses.

periods processing. In computer installations, a mode of processing in which a specific security mode is temporarily established during a time interval for processing sensitive information. The computer system must be purged from all information before the transition from one period to the next whenever there will be new users who do not have clearance and need-to-know for some information processed during the previous period.

personnel security. The policy and procedures established to ensure that all personnel who have access to sensitive data have been determined to be eligible for such access.

physical security. The use of locks, guards, badges, and similar measures to control access to a computer and related equipment. Also the measures required for the protection of the structures housing the computer and their contents from damage by accident, fire, or other environmental hazards.

policy. Administrative decisions which determine how certain security-related concepts will be interpreted as system requirements. All such policy decisions must eventually be interpreted formally and implemented in the system.

privacy. Rights of individuals regarding collection, storage, processing, dissemination, and use in decisionmaking of personal information about themselves. Also, the ability of individuals or organizations to decide whether, when, and to whom personal or organizational information is released.

privacy protection. The granting of privacy rights to individuals through legislative or voluntary means.

process. The active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. A process consists of unique address space containing accessible program code and data, a program location for the currently executing instruction, and periodic access to the processor in order to continue. Also, in general, any program in execution.

protection. Generally, the provision of security. More technically, the use of mechanisms in a computer operating system to control access of executing programs to stored data.

protection level. An indication of the degree of trustedness of a system, as determined in an evaluation of its internal protection mechanisms.

protection mechanism. A feature of a computer system that, together with other such features, enforces the protection policy. Protection mechanisms may include algorithms, data bases, and protection hardware. To be effective, a protection mechanism must be complete, correct, and self-protecting.

protection policy. See *policy*.

public information. Information which by law must be available for public access and examination.

real-time operation. Use of a computer system in applications where results must be available very quickly to be useful for controlling a dynamic system (e.g., an oil refinery or an automated train).

reference monitor. An access-control concept in which an abstract machine mediates access to protected data or programs by users or processes. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base.

reliability. A measure of the ability of a computer system to function within specified error tolerances.

resource sharing. In a computer system, the concurrent use of a resource by more than one user, job, or process. Examples of such resources are input output devices, memory, central processor, and programs.

risk. The probability or likelihood that a threat can be successfully launched against a particular system, facility, or vulnerability. Also the measurable uncertainty of loss, expressed as the product of an annual threat occurrence

rate and the expected amount of loss (estimated in dollars) due to a single occurrence of a threat.

risk analysis. The systematic quantification of system security capabilities, vulnerabilities, probable threats, and loss exposures.

robustness. A generic term representing a computer system's reliability, fault tolerance, survivability, and capability for recovery.

safeguards. See *security safeguards.*

sanitize. To delete sensitive material from a file or communication in order to permit lowering its classification level.

SCOMP. Secure Communications Processor. The Honeywell Level 6 minicomputer, modified to increase security capability by the addition of four protection rings along with user-initiated input/output to direct-access memory devices. SCOMP is the hardware base for the KSOS-6 operating system.

secure operating system. An operating system that effectively controls hardware and software functions to provide the level of protection appropriate to the value of data and resources managed.

security. In the most general sense, the totality of mechanisms and techniques that protect resources (including data and programs in computer systems) from accidental or malicious access, modification, destruction, or disclosure. The term includes physical security of the computer installation, administrative security, personnel security, data security, and communications security. Used more narrowly in a verification context, security denotes the protection of information in a computer system from unauthorized disclosure.

security classification. A designation for information requiring protection against unauthorized disclosure in the interest of national security (see *security level.*)

security kernel. A localized mechanism, composed of hardware and software, that controls the access of users (and processes executing in their behalf) to repositories of information resident in or connected to the system. The correct operation of the kernel along with any associated trusted processes should be sufficient to guarantee enforcement of the access contraints.

security level. In the context of formal security modeling, the fundamental security attribute of subjects and objects. Security levels combine a classification designation (e.g., Confidential, Secret, Top Secret) and a set of need-to-know categories.

security mechanism. See *protection mechanism.*

security mode. A DoD term for "authorized variations in the security environments and methods of operating ADP systems that handle classified data." The DoD ADP security policy (DoD Directive 5200.28) defines four modes: dedicated, system-high, controlled, and multilevel secure.

security policy. See *policy.*

security safeguard. See *protection mechanism.*

security violation. See *violation.*

security *-property. A security model rule allowing a subject write-access to an object only if the security level of the object is the same as or higher than the security level of the subject.

simple security condition. A security model rule allowing a subject read-access to an object only if the security level of the object is the same as or lower than the security level of the subject.

software security. The implementation of protection mechanisms in operating system programs or in applications programs.

specification. Generally, a description of the input, output, and essential functions to be performed by a system or by a component of a system. The specification is produced by the organization that is to develop the system; hence at the top level it can be thought of as the contractor's interpretation of the requirements.

spoofing. The deliberate inducement of a user or a resource to take an incorrect action.

subject. An active user of a computer system, together with any other entity acting on behalf of a user or on behalf of the system; for example, processes, jobs, and procedures may all be considered subjects. Under certain circumstances, certain subjects may also be considered objects of the system.

system-high clearance. Security clearance level and categories that are sufficient to access the highest-security-level material in the system.

system-high security mode. A mode of operation in which the computer system and all of its connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest security level of material contained in the system at that time. All personnel and users having computer system access must have the security clearance, but not a need-to-know, for all material contained in the system.

TCB. Trusted Computer Base.

threat. That which has the potential to menance, abuse, or harm by utilizing existing vulnerabilities of the system.

time-sharing. Operating a computer system in a resource-sharing mode by periodically providing each concurrently operating user or process a fixed amount of time for using the system's resources.

tranquility principle. A security model rule stating that the security level of an active object cannot change.

Trusted Computer Base. The totality of protection mechanisms for an operating system, including both a basic protection environment and the additional user services required for a trustworthy turnkey system. TCBs have been implemented as security kernels and trusted processes.

trusted computer system. A computer system that has sufficient hardware and software integrity to allow its use for simultaneous processing of multiple levels of classified and/or sensitive information.

trusted operating system. An operating system that has been evaluated and assigned a protection level.

trusted process. A process in a position to affect system security, sometimes but not always endowed with privileges to override kernel-enforced rules (e.g., the security *-property). A trusted process requires reliable confirmation that its protection capabilities or characteristics comply with stated requirements (e.g., through formal verification).

trusted system. See *trusted computer system.*

unauthorized disclosure. See *violation.*

UNIX. A general-purpose time-sharing operating system designed and built by the Bell Telephone Laboratories and intended originally for use with DEC PDP-11 series computers. Secure system developments have been based on UNIX (e.g., KSOS-6, KSOS-11), and UCLA and the Mitre Corporation have designed secure UNIX prototypes.

untrusted process. A process that can be incorrectly or maliciously executed without affecting system security. Verification is usually not applied to untrusted processes.

validation. The collection of evaluation, integration, and test activities carried out at the system level to ensure that the system being developed satisfies the requirements of the system specification.

verification. Informally, a clear and convincing demonstration that the system design, especially the software, is correct with respect to well-defined criteria, such as a security model. In a formal context, verification refers to the mathematical demonstration of consistency between a formal specification and a security model (design verification) or between the formal specification and its program implementation (implementation verification). The phrase "formally verified" is now beginning to imply that computer-assisted techniques have been employed in the verification effort.

violation. Some form of security breach.

vulnerability. A weakness or a flaw in a computer system; the state of being open for abuse or indiscriminate use through the circumventing or disabling of some security mechanism in the system.

Appendix B

FEDERAL GOVERNMENT REPORTS ON COMPUTER SECURITY NEEDS

General Accounting Office (GAO) Reports

1. FGMSD-76-5, *Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government*, April 23, 1976.
2. FGMSD-76-27, *Computer-Related Crimes in Federal Programs*, April 27, 1976.
3. FGMSD-76-40, *Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities*, May 10, 1976.
4. LCD-76-115, *Safeguarding Taxpayers' Information—An Evaluation of the Proposed Tax Administration System*, January 17, 1977.
5. FGMSD-77-14, *Problems Found with Government Acquisition and Use of Computers from November 1965 to December 1976*, March 15, 1977.
6. LCD-77-102, *Vulnerabilities of Telecommunications Systems to Unauthorized Use*, March 31, 1977.
7. FGMSD-77-32, *Computer Auditing in the Executive Departments: Not Enough Is Being Done*, September 28, 1977.
8. HRD-77-110, *Privacy Issues and Supplemental Security Income Benefits*, November 5, 1977.
9. FGMSD-76-82, *New Methods Needed for Checking Payments Made by Computers*, November 11, 1977.
10. FPCD-77-64, *Proposals to Resolve Longstanding Problems in Investigations of Federal Employees*, December 16, 1977.
11. LCD-76-102, *Challenges to Protecting Personal Information in an Expanding Federal Computer Environment*, April 28, 1978.
12. CED-78-84, *Problems Persist in the Puerto Rico Food Stamp Program, the Nation's Largest*, April 27, 1978.
13. FGMSD-78-27, *Inadequacies in Data Processing Planning in the Department of Commerce*, May 1, 1978.
14. HRD-78-116, *Procedures to Safeguard Social Security Beneficiary Records Can and Should be Improved*, June 5, 1978.
15. LCD-78-123, *Automatic Systems Security—Federal Agencies Should Strengthen Safeguards over Personal and Other Sensitive Data*, January 23, 1979.

16. FGMSD-80-38, *Wider Use of Better Computer Software Technology Can Improve Management Control and Reduce Costs*, April 28, 1980.
17. AFMD-81-16, *Most Federal Agencies Have Done Little Planning for ADP Disasters*, December 18, 1980.

Federal Information Processing Standards (FIPS)

18. FIPS PUB 31, *Guidelines for ADP Physical Security and Risk Management*, June 1974.
19. FIPS PUB 41, *Guidelines for Implementing the Privacy Act of 1974*, May 30, 1975.
20. FIPS PUB 46, *Data Encryption Standard*, January 15, 1977.
21. FIPS PUB 48, *Evaluation of Techniques for Automated Personal Identification*, April 1, 1977.
22. FIPS PUB 65, *Guidelines for Automated Data Processing Risk Analysis*, August 1, 1979.
23. FIPS PUB 73, *Guidelines for Security of Computer Applications*, June 30, 1980.

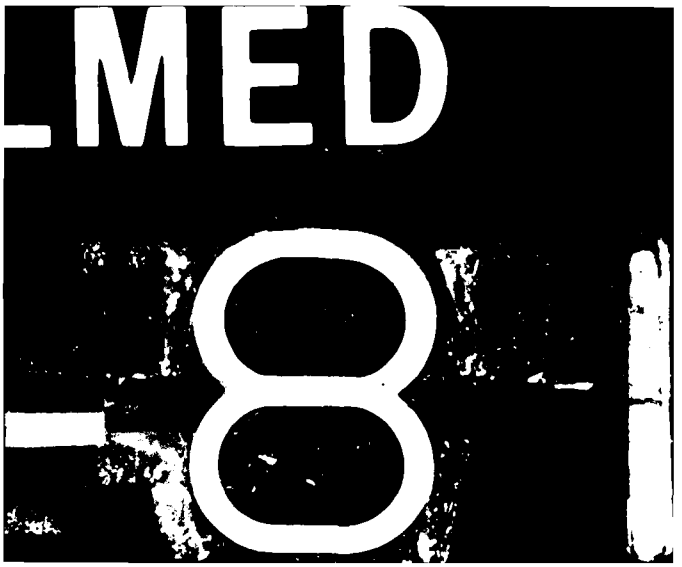
REFERENCES

1. Walker, S. T., *DoD Computer Security Initiative: A Status Report and R&D Plan*, Information Systems Directorate, Assistant Secretary of Defense, Communications, Command, Control, and Intelligence, Department of Defense, Washington, D.C., March 1981.
2. Walker, S. T., "The Advent of Trusted Operating Systems," *AFIPS Conference Proceedings*, Vol. 49, 1980 National Computer Conference, 1980, pp. 655-665.
3. *Proceedings of the Seminar on the DoD Computer Security Initiative Program*, National Bureau of Standards, Gaithersburg, Maryland, July 17-18, 1979.
4. *Proceedings of the Second Seminar on the DoD Computer Security Initiative Program*, National Bureau of Standards, Gaithersburg, Maryland, January 15-17, 1980.
5. *Proceedings of the Third Seminar on the DoD Computer Security Initiative Program*, National Bureau of Standards, Gaithersburg, Maryland, November 18-20, 1980.
6. Nibaldi, G. M., *Proposed Technical Evaluation Criteria for Trusted Computer Systems*, The Mitre Corporation, M79-225, October 25, 1979.
7. Schell, R. R., "Security Kernel Design Methodology," *Proceedings of the Seminar on the DoD Initiative Program*, National Bureau of Standards, Gaithersburg, Maryland, July 17-19, 1979, pp. E-1 - E-21.
8. Anderson, J. P., *Computer Security Technology Planning Study*, USAF Electronics System Division, ESD-TR-73-51, Hanscom AFB, Massachusetts, October 1972.
9. Ware, Willis H. (ed.), *Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security*, The Rand Corporation, R-609-1, reissued October 1979.
10. Trotter, E. T., and P. S. Tasker, *Industry Trusted Computer System Evaluation Process*, The Mitre Corporation, MTR-3931, May 1, 1980.
11. Nibaldi, G. H., *Specification of A Trusted Computer Base (TCB)*, The Mitre Corporation, M79-28, November 30, 1979.
12. *Security Requirements for Automatic Data Processing (ADP) Systems*, Department of Defense Directive 5200.28, December 18, 1972, as amended (change 2, April 29, 1978).

13. *ADP Security Manual: Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource-Sharing ADP Systems*, Department of Defense Manual DoD 5200.28-M, January 1973, as amended (change 1, June 25, 1979).
14. Epperly, E., "Trends in DoD Directives: Survey of Federal Computer Security Policies," *Selected Papers and Presentations from the U.S. Army Third Automation Security Workshop, Williamsburg, Virginia, 8-10 December 1980*, International Business Services, Inc., Washington, D.C., 1981.
15. Parker, D. B., *Crime by Computer*, Scribner, New York, 1976.
16. Russell, S. H., T. S. Eason, and J. M. Fitzgerald, *System Auditability and Control Study: Data Processing Control Practices Report*, SRI International for the Institute of Internal Auditors, Altamonte Springs, Florida, 1977.
17. Ruder, B., T. S. Eason, M. E. See, and S. H. Russell, *Systems Auditability and Control Study: Data Processing Audit Practices Report*, SRI International for the Institute of Internal Auditors, Altamonte Springs, Florida, 1977.
18. *The Dimensions of Privacy*, Sentry Insurance Company, Stevens Point, Wisconsin, 1978.
19. *Summary of Federal ADP Activities in the United States Government, Fiscal Year 1980*, General Services Administration, Washington, D.C., 1981.
20. *Fifth Annual Report of the President on the Implementation of the Privacy Act of 1974, Calendar Year 1979*, Washington, D.C., August 1, 1980.
21. *Fraud and Abuse in Government Benefit Programs*, Department of Justice, Washington, D.C., November 1979.
22. "Privacy Act Guidelines, Supplement to OMB Circular A-108," *Federal Register*, Vol. 40, No. 132, July 9, 1975, pp. 28954ff.
23. *Guidelines for Implementing the Privacy Act of 1974*, National Bureau of Standards, FIPS PUB 71, May 30, 1975.
24. Vorlander, C. W., *State Information Systems, Book of the States, 1980-1981*, The Council of State Governments, Lexington, Kentucky, 1980.
25. *Information Systems Technology in State Governments, 1978-1979*, National Association for State Information Systems, Lexington, Kentucky, 1979.
26. Smith, R. E., *Compilation of State and Federal Privacy Laws*, Privacy Journal Publishers, Washington, D.C., 1978.
27. *Privacy and Security of Criminal History Information: Compilation of State Legislation*, National Criminal Justice Informa-

tion and Statistics Service, Department of Justice, Washington, D.C., January 1978.

28. *Privacy and Security of Criminal Justice Information: Compilation of State Laws*, 1979 Supplement, National Criminal Justice Information Service, Department of Justice, Washington, D.C., 1979.
29. Dantziger, J. N., W. H. Dutton, R. Kling, and K. L. Kraemer, *Computers and Politics*, Columbia University Press, New York, 1981.
30. Jacks, E. L., "Computer Security Interest in the Private Sector," *Proceedings of the Second Seminar on the DoD Computer Security Initiative Program*, National Bureau of Standards, Gaithersburg, Maryland, January 15-17, 1980, pp. E-1 - E-10.
31. Taber, J. K., "On Computer Crime (Senate Bill S.240)," *Computer/Law Journal*, Vol. 1, No. 3, Winter 1979, pp. 517-543.
32. Westin, A. F., *Computers, Health Records, and Citizen Rights*, National Bureau of Standards, NBS Monograph 157, December 1976.
33. Westin, A. F., *Computers, Personnel Administration, and Citizen Rights*, National Bureau of Standards, NBS Special Publication 500-50, July 1979.
34. *Personal Privacy in an Information Society*, Report of the Privacy Protection Study Commission, Washington, D.C., July 1977.
35. Securities and Exchange Commission, "Statement of Management on Internal Accounting Controls," *Federal Register*, Vol. 45, No. 116, June 13, 1980, p. 40134ff.
36. Turn, R. (ed.), *Transborder Data Flows: Concerns in Privacy Protection and Free Flow of Information*, AFIPS, Arlington, Virginia, 1979.
37. *Convention on Protection of Individuals with Regard to Automatic Processing of Personal Data*, Council of Europe, Strasbourg, France, January 28, 1981.
38. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organization for Economic Cooperation and Development, Paris, 1980.
39. Campbell, R. P., and G. Sands, "A Modular Approach to Computer Security Risk Assessment," *AFIPS Conference Proceedings*, Vol. 48, 1979 National Computer Conference, 1979, pp. 293-304.
40. *Guidelines for Automated Data Processing Risk Analysis*, National Bureau of Standards, FIPS PUB 65, August 1, 1979.


LMED
8