1989 ANNUAL REPORT OF THE NATIONAL COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

MARCH 1990

Executive Summary

This Annual Report documents the activities of the National Computer System Security and Privacy Advisory Board during 1989, its first year. The Board was established by Congress through the Computer Security Act of 1987 to identify emerging computer security issues. Dr. Willis Ware of the Rand Corporation was appointed Chairman and assumed that role at the second meeting. The Board met four times during the first year.

In May, the Board asked the National Institute of Standards and Technology to prepare a computer security strategic plan for FY-90. At subsequent meetings, the Board reviewed this document with generally favorable results. During the year, the Board also reviewed the computer security plans for four Presidential Priority Systems being developed by the Internal Revenue Service, General Services Administration, Federal Aviation Administration, and the Department of Veterans Affairs. Major issues discussed during the year include:

(1) the sensitivity categorization of unclassified information;

(2) FY-90 implementation of security plan development requirements;

(3) review of the NIST strategic computer security program plan;

(4) the identification of several computer systems security and privacy emerging issues; and

(5) the general low state of readiness for computer security in the federal government.

The Board identified four areas of emerging concern and has issued (or is in the process of issuing) letters containing the Board's positions and recommendations to appropriate executive and congressional officials. These include:

(1) the addition of computer security to the President's Management-by-Objective program;

(2) a recommendation to discontinue annual security plan submissions;

(3) the unacceptable level of funding for NIST's computer security program; and

(4) a recommendation that the current export restrictions on cryptographic and certain security products be re-examined as they may be too restrictive.

During 1989, the Board also established a work plan for its activities during 1990 and identified candidate topics for in-depth examination. These topics included:

(1) Reviewing the Re-write of National Security Decision Directive 145;

(2) The Memorandum of Understanding between the National Security Agency and NIST;

(3) Computer Security Training;

(4) Development of International Computer Security Standards;

(5) Commercial Orange Book;

(6) Encryption;

(7) Privacy Issues;

(8) Utilizing Security Products/Functions;

(9) NIST Visibility;

(10) NIST Computer and Telecommunications Security (CTS) Council;

(11) Office of Management and Budget Circular A-130;

(12) Computer Security Criminal Activity; and

(13) Categorization System for Sensitive Data.

With such a list of important topics to examine, it is clear that much work lies ahead for the Board in the 1990s.

I. Introduction

The passage of the Computer Security Act of 1987 (P.L. 100-235, signed into law on January 8, 1988 by President Reagan) established the Computer System Security and Privacy Advisory Board. The Board was established by Congress as a federal public advisory committee in order to:

> identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

Appendix A includes the text of the Computer Security Act of 1987 and the enabling provisions relative to the Board. The Act also stipulates that the Board:

- advises the National Institute of Standards and Technology and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems; and

- reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget (OMB), the Director of the National Security Agency (NSA), and appropriate committees of Congress.

Consistent with the Computer Security Act of 1987, the Board's scope of authority extends only to those issues affecting the security and privacy of unclassified information in federal computer systems or those operated by contractors or state or local governments on behalf of the federal government. The Board's authority does not extend to private sector systems (except those operated to process information for the federal government) or Department of Defense systems which process classified information or intelligence or military information covered by the Warner Amendment. The formal charter of the Board was approved on May 31, 1988 by Department of Commerce Assistant Secretary for Administration Katherine M. Bulow. (See Appendix B for the text of the charter.)

The Board is composed of twelve computer security experts in addition to the Chairperson. The twelve members are, by statute, drawn from three separate communities:

- four experts from outside the federal government, one of whom is a representative of a small- or medium- size firm;

- four non-government employees who are not employed by or a representative of a producer of computer or telecommunications equipment; and

- four members from the federal government, including one from the National Security Agency of the Department of Defense.

Currently, Dr. Willis H. Ware, a senior researcher of the Corporate Research Staff of the Rand Corporation, serves as Board Chairman. He was appointed following consultation with Congress which determined that it was inappropriate

for a NIST official to chair the Board. Following his appointment as Chairman, a vacancy was created which was filled by the appointment of Mr. Jack L. Hancock of Pacific Bell to the Board. As of December 1989, the full membership of the Board was as follows:

- Chairman
  Willis H. Ware, Rand Corporation

- Federal Members
  Bill D. Colvin, National Aeronautics and Space Administration
  Roger M. Cooper, Department of Agriculture
  Robert Morris, National Security Agency
  Rhoda R. Mancher, Department of Veterans Affairs

- Non-federal, Non-Vendor
  Robert H. Courtney, RCI Inc.
  Jack L. Hancock, Pacific Bell
  John A. Kuyers, Ernst and Young
  Eddie L. Zeitler, Bank of America

- Non-federal
  Steven B. Lipner, Digital Equipment Corp.
  Jack W. Simpson, Mead Data Central
  Walter W. Straub, Rainbow Technologies, Inc.
  Lawrence L. Wills, International Business Machines Corp.

NIST's Associate Director for Computer Security, Lynn McNulty, serves as the Board's Secretary and is the Designated Federal Official (DFO) under the Federal Advisory Committee Act. (See Appendix C.) The DFO is responsible for ensuring that the Board operates in accordance with applicable statutes and agency regulations. Through the Secretariat, NIST provides financial and logistical support to the Board as stipulated by the Computer Security Act of 1987.

II. Overview of Meetings

March 1 - 2, 1989
Maryland Maritime Institute of Technology, Linthicum, Maryland

The first meeting of the Board was primarily used as an introductory gathering for the members to get acquainted with other members and begin to familiarize themselves with the role and duties of the Board. Mr. James H. Burrows, Director of the National Computer Systems Laboratory, chaired the meeting. As at all meetings, the members were brought up to date with recent activities of interest to the federal computer security community. The Board was briefed on the nature of open meetings and the limited statutory avenues available to close meetings. The entire first meeting was open to the press. Members were also counseled on relations between the Board and the Congress.

Mr. Frank Reeder provided the Board with an overview of the computer security policy structures within the government, as seen by the Office of Management and Budget. The new allocation of responsibilities resulting from the passage of the Computer Security Act of 1987 was also discussed. In particular, Mr. Reeder saw a role for the Board in:

- providing advice about significant security issues, potential problems, and new technologies that the federal government must address; and

- providing assistance to the government in identifying system security products, awareness strategies and techniques for measuring compliance with the law, and future computer security standards.

Mr. James Cox spoke to the Board representing the Office of the Inspector General, Department of Health and Human Services. He reviewed a report, "Review of General Controls in Federal Computer Systems," recently issued by the President's Council on Integrity and Efficiency.

Mr. John Lane of the Computer Sciences Corporation briefed the Board on an information security study prepared by the Armed Forces Communications and Electronics Association for the National Security Agency. Mr. Lane served as study director.

During a discussion session, the Board agreed that it needed to identify critical issues for the Board to examine. Mr. Courtney agreed to develop a prioritized list of computer security problems to serve as a basis for discussion at a future meeting. The resulting list is included in this report as Appendix D. Also, the Board agreed to ask NIST to develop a computer security strategic plan for the Board to examine.

Mr. Richard Weingarten from the Office of Technology Assessment spoke to the Board about recent developments in the field and recommended, among other things, that the Board consider:

- how security can be designed into large complex new systems. Examples cited included the Federal Aviation Administration's air

traffic control system and Internal Revenue Service systems; and

- whether the Computer Security Act of 1987 is useful and if new bills are needed.

Mr. Anthony Taylor and Dr. Harold Podell, staff members of the House Science, Space, and Technology Subcommittee, provided additional Congressional branch input to the Board. They discussed the legislative history of the Act and provided advice about what the duties of the Board should be; specifically, the Board should:

- serve as an independent forum for debate and discussion of information security issues;

- exercise oversight of the standards development process; and

- critique the NIST strategic plan.

Additionally, they recommended that the Board testify at a Congressional hearing scheduled for March 21, 1989. The Board agreed that it was premature to send a representative.

Finally, Mr. Al Bayse of the Federal Bureau of Investigation (FBI) reviewed for the Board various computer-related cases that have occurred over the past few years. He also discussed the privacy and security issues confronting the National Criminal Information Center (NCIC) system. He noted that the FBI was conducting research on the access authentication, user identification, and audit trail analysis. He urged the Board to address the requirement for assuring that computer threat data is collected, processed, and disseminated to the designers and operators of unclassified computer systems.

The agenda and full minutes for this meeting are included as Appendix E and F, respectively.

May 31 - June 1, 1989
Maryland Maritime Institute of Technology, Linthicum, Maryland

At the second meeting, Mr. Burrows turned over the Chairmanship to Dr. Willis H. Ware. Dr. Ware subsequently received a formal appointment letter from the Director of NIST (Appendix G). The meeting focused on two principal topics:

- the NIST Computer Security Strategic Plan; and

- long-term directions for the Board.

A closed session was held in accordance with the Federal Advisory Committee Act to discuss the NIST Computer Security Strategic Plan. The Department of Commerce approved closing the meeting as the disclosure of future budget information in the plan would be likely to significantly frustrate implementation of proposed agency actions. The Board provided a number of useful comments to NIST personnel, including the need for:

- additional computer security threat information,

- prioritizing tasks, and

- "selling" NIST's efforts.

During a general discussion session which followed the closed session, Mr. Burrows clarified the status of the applicability of NIST-issued documents. The Board identified the need for NIST to issue a document on the development of agency computer security policy statements. The Board agreed that Phase 1A of the plan was sufficient to proceed with the development of Phase 1B.

A discussion of the priorities of the Board followed. The basis for the discussion was Mr. Courtney's prioritized list of computer security problems referenced earlier in this report.

In a discussion of the merits of data categorization, Ms. Mancher and Messrs. Cooper and Colvin agreed to form a working group to prepare a white paper on the topic for the Board to review.

The agenda and full minutes for this meeting are included as Appendix H and I, respectively.

September 13 - 14, 1989
Sheraton Reston International Hotel and Conference Center, Reston, Virginia

The first half of the third Board meeting focused on selected Presidential Priority Systems and the security controls which were being integrated into each system. The purpose was to familiarize the Board with four large federal systems under development and the magnitude of the security concerns with each system. (The agenda for the meeting follows as Appendix J.)

The four systems examined were:

- the Internal Revenue Service's **Tax Modernization System**;

- the General Services Administration's **Federal Telephone System 2000**;

- the Federal Aviation Administration's **Advanced Automation System**; and

- the Department of Veterans Affairs' **Decentralized Hospital Computer Program**.

Speakers from each of these agencies provided an overview of the system and their security plans. A summary of each presentation is contained in the minutes of the meeting (Appendix K).

Following these presentations, the Board discussed the integration of computer security into the Presidential Management-By-Objective (MBO) program. During the discussion, the government representatives indicated that this was an appropriate time to establish such priorities. It was suggested that the Board solicit the Secretary of Commerce's support in recommending to the President

that computer security be identified as a governmentwide priority and be included in the MBO program. Including computer security as an MBO would require each agency to report on the computer security program to the agency head, and be subject to audit by the Inspector General, thus giving the program the high visibility needed to make this program work. (See Chapter IV for the text of the letter which was subsequently sent to Secretary of Commerce Mosbacher.)

The Board also reviewed the second phase of the NIST Computer Security Strategic Plan. Due to the amount of information contained in the plan, the Board agreed to appoint a subcommittee to review the plan and report their findings to the Board at the December 1989 meeting.

Next, the Board discussed the security planning efforts undertaken in accordance with the Computer Security Act of 1987. Dr. Stuart Katzke presented an overview of the efforts of NIST's Computer Security Division to process the plans and some of the common themes identified during the process. It was noted by the Board that the annual submission of plans to NIST/NSA does not constitute a judicious, valuable, or cost-effective procedure. It may be better to develop a specific format for the submission of such plans to the heads to the respective agencies rather than to NIST. The Board agreed that the Chairman would prepare a letter to OMB with regard to the future submission of security plans to NIST.

The Board then heard the draft position paper of the subcommittee on data categorization. The main thrust of the report was that more rigorous oversight and levels of sensitivity of data are needed for all non-national security information. The Board agreed to transmit this recommendation to the NIST Computer and Telecommunications Security Council.

In general discussions, the Board agreed that it required a work plan for the Board. A subcommittee was formed to develop the plan and report to the Board at the December meeting.

December 12 - 13, 1989
National Institute of Standards and Technology, Gaithersburg, Maryland

The Board began its fourth meeting with a discussion of the NIST budget situation. (See Appendix L for the meeting agenda.) NIST's computer security budget had not received a planned increase of $3.5 million for FY-90. The Board discussed the reasons for the denial of this increase and the resulting impact upon the computer security program. The Board heard from Ray Kammer, NIST Acting Director, James Burrows, NCSL Director, and Frank Reeder, Director of Information Policy, OMB. The Chairman had prepared a list of questions for each speaker; details are contained in the minutes of the meeting (Appendix M). The Board agreed that the cuts were unacceptable and would send a letter to Congress on the matter.

Next, the Board briefly reviewed NIST computer security strategic plan and agreed that a subcommittee should review the plan in greater detail and report back to the Board.

The Board then turned its attention to the issue of current export restrictions on security products. The Board identified this as an emerging issue and agreed to send a letter to Congress discussing the issue. Two types of products are currently under export restrictions:

- products which contain B3 security functions as defined by the Orange Book; and

- cryptologic devices.

A draft issue paper on the subject will be developed by the Chairman for consideration by the Board.

The Board then considered a draft work plan for its activities for 1990 which was developed by the Work Plan Subcommittee. (See Chapter V.) The Subcommittee on Information Categorization also reported. Messrs. Courtney and Ware agreed to develop an issue paper on information sensitivity.

The Board's Secretary provided the members with an update of the rewrite of National Security Decision Directive 145 (NSDD-145). The National Telecommunications and Information Systems Security Committee (one of the inter-agency committees established by NSDD-145) reviewed a draft during its early December meeting and had sent it back to NSA for revision. The new document appeared to limit NSA's involvement to classified and Warner Amendment systems.

All Federal Register notices which have been issued regarding the Board's activities through the end of 1989 are contained in Appendix N.

III. Major Issues Discussed

The substantive work of the Board during 1989 was devoted to addressing five major topics related to the security of federal unclassified automated information systems. These were:

- Sensitivity Categorization of Unclassified Data;
- FY-90 Implementation of the Security Plan Requirements of the Computer Security Act;
- Review of the NIST Computer Security Strategic Plan;
- Development of Board's Work Plan for 1990; and
- Identification of Emerging Issues for Computer Security and Privacy.

The Board discussions and major conclusions concerned these five topics are summarized below.

Sensitivity Categorization of Unclassified Information

At the June meeting, the Board discussed whether or not a requirement existed for the development of a governmentwide policy on the sensitivity categorization of unclassified information. Several Board members spoke in favor of such a policy stating that unless some sort of sensitivity categorization were introduced into the management of information, protection afforded to truly sensitive information would be at the lowest common denominator. The information classification practices of large industrial corporations were cited as a example of the need to develop a policy for the government in order for security resources to be allocated on some sort of rational basis. The underlying concern was to develop a policy that would supplement the requirement expressed in the Computer Security Act of 1987 to protect "sensitive" information.

Several Board members argued against the desirability of defining or categorizing sensitive information. The essence of their position was that all information held by government agencies has some degree of sensitivity, as defined in terms of its unauthorized disclosure, loss of integrity, or inadvertent or intentional destruction. It was stated that in most instances the development of sensitivity policies have focused entirely upon the confidentiality aspects of the problem to the exclusion of integrity and availability requirements. Any Board recommendation would serve to continue this pattern of confusing the fundamental security issues affecting the protection of unclassified information.

Given these divergent views, the Chairman requested three of the government agency representatives to form a study group and present their conclusions and recommendations on this issue at the September meeting. At this meeting, subcommittee members Mancher, Cooper, and Colvin presented a draft paper on data categorization. Their report concluded that a policy was needed within the federal government to identify information which required additional

protection over and above that afforded all unclassified sensitive information. An extensive discussion followed. The Chairman determined that in view of the deeply divided opinions on this matter, the work being done by the CTS Council should form the basis of any future Board discussions. To that end, the Board will review the Council work at the March 1990 meeting.

FY-90 Implementation of Security Plan Development Requirements

At its September meeting the Board reviewed the activities related to the review of computer security plans for sensitive systems submitted by federal agencies in compliance with the Computer Security Act of 1987. The Board was briefed on the results of the plan review process and the general conclusions that could be drawn from the approximately 1700 civil agency plans. The Board was also informed that NIST and NSA would be reviewing, from mid-August to mid-December, an estimated 29,000 plans submitted by Defense Department elements.

Following this briefing the Board discussed the costs versus benefits of the entire plan submission process. The consensus was that this had not been a cost-effective activity and that the annual submission of such plans for NSA/NIST review did not seem to be a judicious, valuable or cost-effective procedure. The Board authorized the Chairman to send a letter to the Director of the Office of Management and Budget expressing the Board's concern and recommending that FY-90 OMB guidance to the civil agencies place emphasis on the status and effectiveness of agency computer security programs. The exchange correspondence is contained in Chapter IV.

Review of the NIST Strategic Computer Security Plan

At the initial meeting, the Board received a briefing on existing computer security activities at the National Computer Systems Laboratory. The Board asked many detailed questions about future plans and programs. At the conclusion of this discussion, the Board requested the Director of NCSL to prepare a strategic plan that would reflect NCSL computer security activities for FY-89 and projected activities for FY-90.

This project was undertaken jointly by NIST's Associate Director for Computer Security and the Chief of the Computer Security Division. An initial draft plan was presented to the Board at its June meeting. The Board found to plan to be generally satisfactory, and recommended that NSCL continue to refine this document and prepare a detailed plan for FY-90. This document was prepared and presented to the Board at its September meeting. Once again there was general approval of the management assumptions and technical premises underlying the program. Much of the discussion of this document was based on the assumption that NIST would receive the additional $3.5 million contained in the FY-90 appropriation. Unfortunately these funds were deleted at the last moment, and the FY-90 strategic plan will have to be revised accordingly. This final version of the document was reviewed at the Board's December meeting. Throughout the various discussions on the NIST computer security plan, the Board provided NIST with expert views and opinions and avoided any appearance of attempting to manage NIST's ongoing activities. The NIST computer security program benefited greatly from preparing the planning documents and presenting them to a group of interested, knowledgeable experts.

Development of Board's Work Plan for 1990

At its third meeting, the Board formed a subcommittee to develop a proposed work plan for 1990 for the Board. The subcommittee reported to the Board at the fourth meeting at which time the plan was slightly revised. A summary of the Board's plans for 1990 follows in Chapter V.

Identification of Emerging Issues for Computer Security and Privacy

During the course of FY-89, the Board identified a number of emerging computer system security and privacy issues:

- the need for increased management attention to computer security and a proposal to add a computer security Management-by-Objective (MBO) to the President's overall management plan;

- the current export restrictions on security products which result in the decreased availability and increased cost of those few products which are developed and marketed; and

- the unacceptable state of funding for the NIST computer security program.

As discussed in the next chapter, the Board has issued a letter on the MBO issue and, at the time of this writing, letters on the other two issues were being drafted and coordinated.

IV. Reports Issued

During FY-89, the Board issued letters reporting the Board's findings on two important issues: the need for increased management attention to computer security issues and the computer security planning activities being carried out in accordance with the Computer Security Act.

Letter to the Secretary of Commerce on MBO

The first letter was sent to Secretary of Commerce Robert Mosbacher on September 22, 1989, recommending that he seek the support of the President to establish a computer security Management-By-Objective in the President's governmentwide program. (See Exhibit I.) Mr. James Burrows, Director of NIST's National Computer Systems Laboratory, has provided an interim response to the Board on behalf of Secretary Mosbacher. (See Exhibit II.)

Letter to the Director of OMB Recommending that the Submission of Annual Plans be Discontinued

The second letter was sent on October 19, 1989 to Director Darman of OMB. This letter detailed the Board's position on the computer security planning effort and whether plans should be submitted to NIST and NSA for review on an annual basis. (See Exhibit III.) OMB's response is included as Exhibit IV.

Exhibit I

THE NATIONAL COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

SEP 2 2 1989

Honorable Robert A. Mosbacher
Secretary of Commerce
Washington, DC 20230

Dear Mr. Secretary:

As required by the Computer Security Act of 1987, I am pleased to submit the following recommendation for your action from the Computer System Security and Privacy Advisory Board.

At its third meeting, the Advisory Board agreed that the Office of Management and Budget should include the strengthening of computer security programs as a major goal in the Management-By-Objective (MBO) program for next fiscal year. Full compliance with the requirements stated in Appendix III of OMB Circular A-130, "Management of Federal Information Resources," is a sound foundation for implementing this proposed MBO goal. Accordingly,

> **the Board recommends that you seek the cooperation of the President and urge that he include a computer security MBO in his overall program.**

The Board recognizes the government's ever-increasing dependence on the use of computer technology for the proper functioning of government. The initiation of a computer security MBO will help ensure that agencies act promptly to institute a cost-effective computer security program to provide appropriate protection for the confidentiality, integrity, and availability of sensitive data in federal computer systems.

This recommendation will address many deficiencies raised to the Board by Federal agencies. It is consistent with reports we have reviewed, including those from the President's Council on Integrity and Efficiency, the General Accounting Office, and individual agencies.

I would be happy to discuss this matter further at your convenience. I look forward to hearing of your reaction to the Board's recommendation.

Sincerely,

Willis H. Ware
Chairman

Executive Secretariat: National Computer Systems Laboratory
National Institute of Standards and Technology
Technology Building, Room B154, Gaithersburg, MD 20899
Telephone (301) 975-3240

cc: Honorable Robert A. Roe
Honorable John Conyers, Jr.
Honorable Ernest F. Hollings
Richard Darman, Director, OMB
Raymond G. Kammer, Acting Director, NIST
Vice Admiral W. O. Studeman, Director, NSA

OCT 17 1989

Dr. Willis H. Ware
Chairman, Computer System Security
and Privacy Advisory Board
c/o The Rand Corporation
1700 Main Street
P.O. Box 2138
Santa Monica, CA 90406-2138

Dear Dr. Ware:

I would like to extend Secretary Mosbacher's appreciation for your recent recommendation from the Computer System Security and Privacy Advisory Board.

We are examining the recommendation and approaches for its implementation. I have asked Lynn McNulty to keep you informed of its status.

I appreciate the continued effort by the Board to improve the level of computer security in the Federal government and look forward to receiving further reports from the Board.

Sincerely,

ORIGINAL SIGNED BY:
James H. Burrows
James H. Burrows
Director
National Computer Systems Laboratory

cc: Honorable Robert Roe
Honorable John Conyers, Jr.
Honorable Ernest Hollings
Honorable Richard Darman, Director, OMB
Raymond G. Kammer, Acting Director, NIST
Vice Admiral W.O. Studeman, Director, NSA

Exhibit III

THE NATIONAL COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

October 19, 1989

Honorable Richard Darman
Director, Office of Management and Budget
Old Executive Office Building
Washington, DC 20503

Dear Mr. Darman:

As required by the Computer Security Act of 1987, I am pleased to submit the following report from the Computer System Security and Privacy Advisory Board for your consideration.

At its third meeting the Advisory Board examined the review of agency computer security plans being accomplished by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The Board noted that analysis has been completed on the 1700 plans received in January from the civilian agencies. Substantial progress is being made in reviewing the 25,000 to 40,000 plans received in mid-August from the Department of Defense.

The current review of plans has resulted in a significant expenditure of resources by both NSA and NIST. These scarce resources will be better utilized if the OMB guidance for FY-1990 directs plan development and review only for those systems whose submission was judged unacceptable or omitted by an agency. Additionally, the guidance should include preparation of plans for systems operated by contractors and state or local governments on behalf of the federal government.

For those agencies whose plans indicated a sufficient understanding of and commitment to improving the security level of computer systems, guidance should direct the development of an agency-wide management plan for implementation of their computer security plans. Additionally, all agencies should be required to describe in detail progress made over the past five years in implementing OMB Circular A-130 for establishment of comprehensive agency computer security programs.

Executive Secretariat: National Computer Systems Laboratory
National Institute of Standards and Technology
Technology Building, Room B154, Gaithersburg, MD 20899
Telephone (301) 975-3240

Finally, if your office wishes to establish an oversight mechanism to assure compliance with the planning requirements, each agency Inspector General should be tasked to accomplish a periodic examination of the agency's computer security plans.

I appreciate the opportunity to express the views of the Computer System Security and Privacy Advisory Board. I look forward to hearing of your reactions to the Board's comments regarding the security planning process. You can reach me through the Rand Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138.

Sincerely,

Willis H. Ware
Chairman

cc: Honorable Robert Roe
Honorable John Conyers, Jr.
Honorable Ernest Hollings
Raymond G. Kammer, Acting Director, NIST
Vice Admiral W. O. Studeman, Director, NSA

- Should representatives of the Office of Personnel Management and OMB be invited to discuss the training and follow-up programs with the Board?

- Should the Board take a position on these issues?

- How should that position be communicated and to whom?

Development of International Computer Security Standards

There has been a proliferation of "trusted systems" criteria among the defense/intelligence and commerce organization of the western world. Most of these criteria are the result of the work done by NSA as expressed in the "rainbow series" of publications. These criteria cover both classified and unclassified data, although the primary focus is on classified data.

Manufacturers of security hardware and software products are faced with the possibility of having to develop and support unique products for each individual set of criteria. This will result in multiple products, each with a smaller market and with a much higher price. The effect will be to raise the cost of security and therefore limit the market for security products.

Relevant questions the Board may wish to address include:

- Should the Board be briefed on these issues by individuals and organizations that are involved? If so, who?

- Should the Board take positions in these issues and if so, how and to whom?

Commercial Orange Book

The following issues regarding the development of a civilian orange book may be of interest to the Board:

- Is there a need for a private sector/unclassified data Orange Book?

- How would such a document relate to the NSA Orange Book? Would they be separate documents or should there be a single document?

- Who should be invited to discuss this issue with the Board?

- What organization should develop such a document? If it is NIST, how can the work be done within existing funding constraints?

- Could the NIST CTS Council assist in the development of this document?

Encryption

The primary way networks can be protected is through the use of encryption. By

the mid-1990s, there will be very little unencrypted, uncompacted data on networks. Government and the private sector operate in a worldwide market with worldwide networks. Of interest to the Board:

- How can the requirement for a commercial encryption algorithm for worldwide use be realized?
- How are export control regulations affecting the ability of the government to communicate with the private sector over encrypted networks?
- Is there a need for a public key standard in addition to the Data Encryption Standard?
- Is it realistic to expect the NSA to develop encryption algorithms that will be accepted outside the USA?
- How can the NIST CTS Council assist in this issue?
- Who should be invited to brief the Board on these issues?

Privacy Issues

The issue of privacy has been quiet for several years. However, recently the issue has been receiving renewed attention in the USA and the EC. The Board may be interested in exploring topics such as the following:

- What are the key issues in privacy?
- What is the status of existing laws and proposed legislation in the USA?
- What is the status of privacy in other areas of the world?
- Who should be invited to brief the Board on privacy issues?

Utilizing Security Products/Functions

A recent review of a number of existing computer installations in the federal government indicated that security functions in the systems were not being used or were being used improperly. Of interest:

- Should the Board pursue a strategy to provide guidelines to users on how to use the security functions in those systems?
- Should vendors of products be asked to assist in the development of such guidelines?
- Should the NIST CTS Council be asked to assist in the development of such guidelines?

NIST Visibility

The Board has concluded that NIST's computer security activities lack visibility. The present funding problems can exacerbated this problem. Specifically:

- How can the Board assist NIST to raise its visibility?

- Can the NIST CTS Council assist in this area?

NIST Computer and Telecommunications Security Council

The NIST CTS Council has been in existence for more than two years.

- Would there be value in having the Board briefed on the work of the Council?

- Should the Board meet with representatives of the Council or with the Council as a group?

- What work can the Council do to assist the work of the Board?

OMB Circular A-130

OMB Circular A-130 covering the security of federal automated systems was issued December 24, 1985. A number of issues may be relevant for the Board's consideration:

- Is that document current as it relates to the Computer Security Act of 1987?

- Does that document need revision as it relates to the current environment?

Criminal Activity

- Should the Board undertake work to identify exposures in federal systems to criminal activity?

VI. Conclusions

During its first year, the Board built the foundation toward better progress in the years ahead. It developed a work plan and established its priorities. The Board has begun to examine those issues which it should study further and has heard from a number of agencies and organizations as to its role and duties. While the Board has initiated an action plan to identify emerging computer security and privacy issues, much remains to be accomplished in successfully addressing the challenges of the 1990s.