1990 ANNUAL REPORT

OF THE NATIONAL COMPUTER

SYSTEM SECURITY

AND

PRIVACY

ADVISORY BOARD

MARCH 1991

Executive Summary

This Annual Report documents the activities of the National Computer System Security and Privacy Advisory Board during 1990, its second year. The Board, which met three times during the year, was established by Congress through the Computer Security Act of 1987 to identify emerging computer security issues. Dr. Willis Ware of RAND has served as Chairman of the Board since July of 1989.

The Board formally identified three areas of emerging concern and has issued letters containing the Board's positions and recommendations to appropriate executive and congressional officials. These were:

- NIST's Computer Security Program Budget;
- the Information Technology Security Evaluation Criteria; and
- the Need for Computer Security Guidelines.

The Board also established a work plan for 1991 which identified candidate topics for in-depth examination, including:

- Computer Security Guidelines
- NIST Plans and Activities;
- Privacy - EC Green Paper;
- Implementation of the Computer Security Act of 1987;
- Software Engineering and Reliability;
- Security and the Public Switched Network;
- Use of Security Products and Features;
- Rewrite of NSDD-145 and the NIST/NSA Memorandum of Understanding;
- Computer Emergency Response Team (CERT);
- Digital Signature; and
- International Hacking.

With such a list of important topics to examine, plus the ever growing relevant new issues and public policy questions, it is clear that much work lies ahead for the Board in 1991 and beyond.

I. Introduction

Board's Establishment and Mission

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 created 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, which includes specific provisions regarding the Board. The Act 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.

Board's Charter

The Board was first chartered on May 31, 1988 and was rechartered on May 30, 1990 by U.S. Department of Commerce Assistant Secretary for Administration Thomas Collamore. (See Appendix B for the text of the current charter.) It should be noted that because of the time necessary for the rechartering, the Board meeting scheduled for June could not be officially noticed in the Federal Register. Since a committee must have a current charter in order to notice a meeting, and since at least 15 days notice is required, the decision was made on May 8, 1990 to cancel the June meeting.

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 systems which process classified information or Department of Defense unclassified systems related to military or intelligence missions as covered by the Warner Amendment (10 U.S.C. 2315).

Membership

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 RAND, serves as Chairman of the Board. He was appointed in July 1989 following consultation with Congress which determined that it was inappropriate for a NIST official to chair the Board. As of December 1989, the full membership of the Board was as follows:

- Chairman
  Willis H. Ware, RAND
- Federal Members
  Bill D. Colvin, National Aeronautics and Space Administration
  Roger M. Cooper, Department of Agriculture
  Patrick Gallagher, National Security Agency (nominated)
  Rhoda R. Mancher, Department of Veterans Affairs
- Non-federal, Non-Vendor
  Robert H. Courtney, RCI Inc.
  John A. Kuyers, Ernst and Young (renominated)
  Eddie L. Zeitler, Fidelity Security Services, Inc.
  (vacancy)
- Non-federal
  Steven B. Lipner, Digital Equipment Corp.
  Lawrence L. Wills, International Business Machines Corp.
  Jack L. Hancock, Pacific Bell
  (vacancy)

NIST's Associate Director for Computer Security, Mr. Lynn McNulty, serves as the Board's Secretary and is the Designated Federal Official (DFO) under the Federal Advisory Committee Act. The DFO is responsible for ensuring that the Board operates in accordance with applicable statutes and agency regulations. Additionally, the DFO must approve each meeting and its agenda. Through the

Secretariat, NIST provides financial and logistical support to the Board as stipulated by the Computer Security Act of 1987.

During 1990, the terms of Mr. Walter Straub (Rainbow Technologies, Inc.) and Mr. Robert Morris (National Security Agency) expired. Additionally, Mr. Jack Simpson (Mead Data Central, Inc.) resigned on March 9, 1990. NSA chose Mr. Patrick Gallagher, Director of the National Computer Security Center, as their designated representative member on the Board. As of December, 1990, NIST's nominations to fill existing Board vacancies were still being processed.

II. Major Issues Discussed

The following section summarizes the discussions held by the Board in 1990. Additionally, the Board accomplishes a lot of informal, non-decisional, background discussion and preparation for meetings by e-mail between meetings. The Board's activities also complement the other activities of the Board's members, several of whom are quite active in many aspects of these topics. Note that the minutes and agenda from the March, September, and December meetings are included as Appendices C to E, respectively. The required Federal Register notices for the meetings are presented in Appendix F.

The substantive work of the Board during 1990 was devoted to various topics related to the security of federal unclassified automated information systems. Among the most important were:

- NIST's Computer Security Program Budget;
- Data Categorization;
- E-Mail Privacy and Security;
- Computer Security Evaluation Criteria; and
- Computer Security Guidelines.

NIST's Computer Security Budget

In 1989, the President had requested a substantial increase for NIST's computer security program. In late September 1989, the proposed increase for NIST's computer security program was cut by conference committee action. This led to discussions among Board members as to the inadequacy of the current budget, $2.5 million at the time. The Board decided at its December 1989 meeting to send a letter to Congress stressing the need for a higher funding level. The letters could not be formally approved until March 1990 since the letters had to be adopted by the Board in open session. The President's budget for FY-91 requested an increase for the computer security program, which ultimately resulted in an increased $1 million for the program.

Data Categorization

Since June of 1989, the Board has discussed the issue of data categorization of unclassified information. This topic continued to be one of interest in 1990, although members of the Board hold widely divergent opinions as to the desirability and feasibility of developing a standard governmentwide categorization scheme.

During the year, 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. 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.

In December 1990, during an extensive session on the topic, representatives from five government agencies were invited to share their positions on the topic with the Board. As with the Board itself, their positions varied; however, while most believed that such a scheme would be useful, they disagreed as to the feasibility of actually developing a scheme that would be useful across all agencies. A representative from the Canadian government also shared their experiences with a statutory based categorization scheme which is working very well.

The Board continues to examine this issue recognizing the importance of this issue and its far reaching implications. As of December, the Board asked two of its members to look further into the issue and report back in March 1991.

E-Mail Security and Privacy

At the suggestion of Mr. Cooper at the September meeting, the Board developed a session to e-mail privacy and security issues at the December meeting. The Board heard from representatives of the E-Mail Industry Association, American Bar Association, and a public interest group, the Computer Professionals for Social Responsibility.

Action by the Board on this matter was anticipated for 1991.

Computer Security Evaluation Criteria

Two distinct items are included in this category: 1) the European-developed draft Information Technology Security Evaluation Criteria (ITSEC) and the NIST response to that document and 2) the NIST and NSA effort to develop appropriate standards and guidelines for U.S. Government use.

At the September meeting, the Board examined the ITSEC and heard one vendor's reactions to it. The Board also was presented with NIST's official position on the document as relayed to the Europeans in a letter in August. In December, NIST provided the Board with an update on the ITSEC's progress and the European Community-sponsored conference held in Brussels in September on it. The Board

was also informed of efforts by NIST and NSA to arrive at a common response to the ITSEC. The Board, agreeing on the significance of the ITSEC effort and resulting possible implications for U.S. international trade, voted to send a letter to the Secretary of Commerce outlining their position on the U.S. government's role. (See next chapter for text of the letter and the response.)

Intertwined with the ITSEC topic was a discussion of what NIST should be doing, if anything, to develop a appropriate standards and guidelines for the federal government's use. Positions ranging from the need to modify the Orange Book to the non-usefulness of such a document were vigorously debated. In December, NIST and NSA announced their joint effort to develop a single federal criteria document, which would not begin with the Orange Book as an initial approach. NIST stressed that there was much that could be learned from users of trusted systems and that it would be holding a conference to gather the "lessons learned."

Computer Security Guidelines (Handbook)

In mid-1990, Mr. Courtney suggested to Board members that they endorse a recommendation to NIST to develop a set of computer security guidelines to aid federal agencies in the selection of cost-effective security measures. He also prepared a draft outline for NIST's use. After discussion of the outline at the September meeting, and minor modifications, the Board recommended to the Director of NIST that he give the development of such a document high priority. The Director responded that NIST would be examining ways to meet the need addressed by the Board.

III. Advisory Board Correspondence

During FY-89, the Board issued letters reporting the Board's findings on the three important issues:

- the level of funding of NIST's computer security program budget;
- the draft European Information Technology Security Evaluation Criteria; and
- the development of computer security guidelines.

Also, the Chairman conducted correspondence with the Department of Commerce's General Counsel regarding the legal constraints on the Board. Finally, the Secretary of Commerce forwarded the Board's 1989 Annual Report to the Congress and Administration officials.

NIST's Computer Security Budget

On April 20, 1990, the Board issued a letter to Congressional officials on the state of NIST's computer security program budget and recommended that it be increased, as the President requested in his FY-91 budget request. The Board's letter was forwarded to the Congress by the Secretary of Commerce. The increase was ultimately approved and in FY-91 the program budget was increased by $1 million to $3.5 million.

Development of Computer Security Guidelines

On October 10, 1990, following action at its September meeting, the Board issued a letter to the Director of NIST recommending that NIST develop and issue a comprehensive set of computer security guidelines. The Board also provided NIST with a proposed outline of the envisioned publication. On October 26, 1990, Dr. Lyons responded that he was reviewing alternatives to meet the need developed by the Board. NIST now plans to use the outline as the basis for a Computer Security Handbook, to be developed under contract to NIST.

Information Technology Security Evaluation Criteria

The Board also issued its findings on October 20, 1990, regarding the draft European-developed Information Technology Security Evaluation Criteria document. The Board recommended that this important trade issue be coordinated among all concerned federal agencies. Also, the Board sought active protection of U.S. interests via the International Standards Organization process. Secretary of Commerce Mosbacher replied on December 18, 1990 that the Department would be following this important issue.

Exhibits

The Board's correspondence and replies (when received) are included in the following exhibits:

Exhibit I	Budget letter from Chairman Ware (No replies were received.)
Exhibit II	Transmittal of 1989 Annual Report by Secretary Mosbacher (No replies were received.)
Exhibit III	Letter from Chairman to U.S. Department of Commerce General Counsel on legal issues
Exhibit IV	Answer from General Counsel to Chairman Ware
Exhibit V	Chairman's letter to NIST Director Lyons regarding computer security guidelines (Handbook)
Exhibit VI	Oct 26, 1990 answer to the Board from NIST Director Lyons
Exhibit VII	Oct 20, 1990 Board letter to Secretary Mosbacher regarding the Information Technology Security Evaluation Criteria
Exhibit VIII	Dec. 18, 1990 answer from Secretary Mosbacher to the Board

EXHIBIT I

THE NATIONAL COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

APR 2 0 1990

Honorable Robert C. Byrd
Chairman, Committee on Appropriations
United States Senate
Washington, D.C. 20510-6025

Dear Mr. Chairman:

The Computer System Security and Privacy Board, established under Section 21 of the Computer Security Act of 1987 [P.L. 100-235], herewith conveys its finding, as stipulated under Section 21(b)(3) of the Act, on the issue of budget support for the National Institute of Standards and Technology (NIST), and its National Computer Systems Laboratory (NCSL).

Through the Act, Congress assigned to the NIST/NCSL responsibility in Section 20(a) "to [develop] standards, guidelines, ...methods and techniques for cost-effective security...[in Federal computer systems]." At our recent meetings, the Board discussed the funding level of NIST/NCSL for the computer security program to meet the Congressionally mandated goal.

Congress did not provide FY-90 funding commensurate with the relevant technical and managerial issues that must be addressed. The Board believes that the current funding level of $2.5 million for the NIST/NCSL computer security program is inadequate, a view consistent with the White House support of a $6.0 million funding level in FY-90. With limited funding, Congress must appreciate that issues which led to the passage of legislation will not be promptly addressed, and that adequate solutions will be delayed.

With the integration of computer systems into all aspects of our daily lives and the national economy, the failure to address system protection and security controls could have potentially serious consequences for the nation. Moreover, money spent on improving the security posture of government computer systems will be more than recouped from savings that result from more effective and safer system operation with more reliable and accurate data.

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

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

MAY 24 1990

Honorable John Conyers, Jr.
Chairman, Committee on
Government Operations
House of Representatives
Washington, D.C. 20515-6143

Dear Mr. Chairman:

I am pleased to submit the Annual Report of the Computer System Security and Privacy Advisory Board, U.S. Department of Commerce, for calendar year 1989, in compliance with the Computer Security Act of 1987.

Sincerely,

Robert A. Mosbacher

Honorable Robert C. Byrd
Chairman, Committee on Appropriations
United States Senate
Washington, D.C. 20510-6025

Dear Mr. Chairman:

Honorable Ernest F. Hollings
Chairman, Committee on Commerce, Science,
and Transportation
United States Senate
Washington, D.C. 20510-6125

Dear Mr. Chairman:

Honorable Jamie L. Whitten
Chairman, Committee on Appropriations
House of Representatives
Washington, D.C. 20515-6015

Dear Mr. Chairman:

Honorable Robert A. Roe
Chairman, Committee on Science, Space,
and Technology
House of Representatives
Washington, D.C. 20515-6301

Dear Mr. Chairman:

Honorable John Conyers, Jr.
Chairman, Committee on Government Operations
House of Representatives
Washington, D.C. 20515-6143

EXHIBIT III

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

APR 09 1990

Wendell L. Willkie II, Esquire
General Counsel
U.S. Department of Commerce
Washington, DC 20230

Dear Mr. Willkie:

During a recent meeting of the Computer System Security and Privacy Advisory Board (CSSPAB) established under Section 3 of the Computer Security Act of 1987 (Public Law 100-235), several items of CSSPAB functioning were discussed at length in public session with Mr. Michael Rubin of your office. Admittedly, some of these things are interpretive in nature or even uncertain in view of the words of the law and its legislative history. Accordingly, on behalf of the Board, I am formally soliciting an official departmental written legal opinion on the following questions. Your guidance will greatly assist the effective functioning of the CSSPAB and will hopefully resolve confusion which has arisen as to its proper role, relationship to the Department of Commerce, and obligations under various laws.

1. What is the relationship between the CSSPAB and the Federal Advisory Committee Act? Is it necessary that the CSSPAB be established pursuant to the procedures of the Federal Advisory Committee Act, or does the Computer Security Act in and of itself provide a sufficient basis for the CSSPAB to function?

2. In view of the wording of PL 100-235, what is the relationship between the CSSPAB and the Department of Commerce? Although the CSSPAB resides within the Department, does it follow that the Department must establish the CSSPAB's charter and set its agenda? To what degree does the Board have any independence from the Department? Do the members of the Board have the power to amend the CSSPAB's charter? To what extent are the DOC administrative review and approval procedures for correspondence relevant to CSSPAB?

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

interest of obtaining advice or recommendations for any Federal agency. 5 U.S.C. App. 2 § 3(2). The requirements of the FACA are applicable to every advisory committee "except to the extent that any Act of Congress establishing such advisory committee specifically provides otherwise." 5 U.S.C. App. 2 § 4.

Since the CSSPAB is tasked with advising the National Institute of Standards and Technology (NIST) and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems, it is an advisory committee. The legislation establishing the CSSPAB provides that it is established within the Department of Commerce. 15 U.S.C. § 278g-4(a). The legislation also does not exempt the CSSPAB from any of the FACA's provisions. Consequently, the FACA's requirements are fully applicable to the CSSPAB. The CSSPAB is subject to all of the provisions of the FACA and the CSSPAB cannot meet or take any other action until the procedural and administrative requirements of the FACA have been satisfied.

Question 2

In view of the wording of PL-235, what is the relationship between the CSSPAB and the Department of Commerce (DOC)? Although the CSSPAB resides within the Department, does it follow that the Department must establish the CSSPAB's charter and set its agenda? To what degree does the Board have any independence from the Department. Do the members of the Board have the power to amend the Board's charter? To what extent are the DOC administrative review and approval procedures for correspondence relevant to CSSPAB?

Answer

As stated above, the CSSPAB is an advisory committee within the Department of Commerce. The FACA requires each agency to "exercise control and supervision over the establishment, procedures, and accomplishments of advisory committees established by that agency." 5 U.S.C. App. 2 § 8(b). Agencies are also required to file a charter for each advisory committee. Id. § 9(c). Charters for advisory committees over which the Department has jurisdiction are required to be prepared and filed in accordance with the procedures set forth in Part 2, Chapter 2, Section B of the Department's Committee Management Handbook. The CSSPAB's charter must be prepared and filed in accordance with these procedures.

The FACA also provides that a designated Federal official or employee must attend each meeting of an advisory committee and that no advisory committee shall conduct any meeting in the absence of that officer or employee. Advisory committees are prohibited from holding meetings except with the advance approval of the designated Federal official. Further, the agenda of every advisory committee meeting must be approved by this official.

5 U.S.C. App. 2 § 10 (e), (f). Accordingly, the CSSPAB is prohibited from operating independently of the Department of Commerce. The meetings and agenda of CSSPAB must be approved by the appropriate Department official. The CSSPAB's charter also cannot be amended by the members. Any charter amendment must be effected in accordance with the procedures set forth in Part Two, Chapter Two, Section D of the Department's Committee Management Handbook, which requires the approval of amendments by the Assistant Secretary for Administration. Likewise, since the CSSPAB reports through the Director of NIST, the administrative review and approval procedures applicable to the correspondence of advisory committees within the jurisdiction of the Department are fully applicable to the CSSPAB.

Question 3

The duties of the CSSPAB include the statutory responsibility to "report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of Congress." The question has arisen whether these reporting requirements are sequential or concurrent. Can the CSSPAB, for example, report its findings directly to Congress or must it report its findings to Congress through the Secretary? Is it legally significant that Congress did not use the preposition "through" but stated "to ...the Congress" when it described the Board's reporting requirements?

Answer

The Computer Security Act does require the CSSPAB to report to several entities in addition to the Secretary of Commerce. However, nothing in the legislation or in the legislative history indicates that the reporting to the various entities is to be concurrent. Although the statute establishing the CSSPAB does not explicitly require that all reports shall be made through the Department, the reporting requirements must be viewed in light of the placement of the CSSPAB within the Department of Commerce.

The CSSPAB is required to submit its reports in accordance with the CSSPAB charter. The charter provides that the Board report "through the Director of [NIST]." This requirement is consistent with the position of the CSSPAB as an advisory committee within the Department. Thus, the CSSPAE cannot report directly to Congress but must report through the Director of NIST as required by the CSSPAB charter. We view the requirement that the CSSPAB report to entities other than the Secretary as an expression of congressional intent that the other entities be kept informed, not as a mandate for the CSSPAB to operate independently of the Department in which it has been established.

- He was barred from seeking or receiving, directly or indirectly, any money, gratuity, or other thing of value from any competing contractor or its agents.

In addition, any member of the Board who was given authorized or unauthorized access to proprietary or source selection information regarding any agency procurement was barred from knowingly disclosing such information, directly or indirectly, to any person other than a person authorized by the head of such agency or the contracting officer to receive such information. This prohibition applied without regard to one's status as a procurement official.

Should the suspended Act take effect again on November 30, 1990, questions might arise about its continuing application to activities that occurred between July 16, 1989 and November 30, 1989. In this event, you might wish to consult us for additional advice.

As a final matter, let me assure you that it is entirely appropriate for the CSSPAB to seek advice from this office. Since the CSSPAB is an advisory committee within the Department of Commerce, advice on its status and operation must be based upon an interpretation of Departmental requirements as well as the establishing legislation. Please feel free to contact this office again if you have additional questions on this matter.

Sincerely,

Dan Haendel
Deputy General Counsel

Exhibit V

THE NATIONAL COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

OCT 10 1990

Dr. John W. Lyons
Director
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dear Dr. Lyons:

The Computer System Security and Privacy Advisory Board was established within the Department of Commerce by the Computer Security Act of 1987, P.L. 100-235. The charter of the Board establishes a specific objective for the Board to advise the National Institute of Standards and Technology (NIST) and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems.

The purpose of this letter is to advise you of the unanimous concern of the Advisory Board that information security guidelines be written and published by NIST. We feel that these guidelines are a basic building block of the government's information infrastructure program and will provide the necessary detailed guidance to Federal agencies to ensure proper safeguards for unclassified systems.

There are numerous laws and regulations requiring attention to computer security and privacy, but the missing link is the proposed NIST guidelines.

1. Privacy Act of 1974 (P.L. 93-579) -- Provides for the protection and accuracy of information about individuals.

2. Federal Managers Financial Integrity Act (P.L. 97-225) -- Requires the use of internal controls to reduce fraud, waste and abuse.

3. OMB Circular A-123 -- Requires the establishment and periodic review of internal controls.

4. OMB Circular A-130 -- Assigns governmentwide security responsibilities and describes minimum agency security program components.

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

5. OMB Circular 90-08 -- Provides guidance to Federal agencies on computer security planning.

6. Computer Security Act of 1987 (P.L. 100-235) -- Assigns NIST primary responsibility for providing guidance and assistance for unclassified computer security.

7. President's FY-91 Budget, Managing for Integrity and Efficiency Section -- Describes the need for data integrity and accuracy.

Clearly the concerns of the Congress and the Office of Management and Budget regarding the need for improved computer security of the Government's unclassified systems have been repeatedly addressed. The Board shares these concerns, and has identified the lack of a comprehensive computer security guideline as adversely affecting the Government's ability to effectively and efficiently implement these laws and regulations. Such guidelines would have immediate governmentwide benefits in the strengthening of controls, resulting in improved computer security.

Recognizing the technical and fiscal resource constraints of NIST, and other competing priorities, the Advisory Board has independently produced an outline of these guidelines (enclosed). We are now requesting that you recognize this need, and consider whatever managerial alternatives are at your disposal to expedite the writing and issuance of these guidelines.

Thank you for your time and consideration of our recommendation. I am available to discuss this with you at your convenience.

Sincerely,

Willis H. Ware

Willis H. Ware
Chairman

Enclosure

A SYSTEMATIC APPROACH TO INFORMATION SECURITY

1. Purpose

It is intended that this document be used as a handbook to guide the selection anc implementation of security measures in data processing and data communications environments. It does not provide exhaustive treatment of every aspect of computer and telecommunications security. It does provide references to other material which can be used to augment that presented here.

A major difference between this material and other, similar efforts is that it offers guidance to specific references in its bibliography as a function of the particular problem being addressed. For example, if the problem is control of access to data at the record and field level, the reader will not be directed to the many papers on generalized access control at the file or data set levels, but rather to references to papers on only that aspect of access control.

It has been our experience that it can be irritating and very time consuming to be given broadly-based references which force the reader to acquire and read many papers to find which, if any of them, contain the desired, specific information.

2. Scope

It is intended that this handbook provide material and references which will assist in identifying, implementing, and assessing the relative cost and adequacy of security controls in data processing and telecommunications environments.

3. Definitions of Key Terms

There is no broad agreement on what is meant by many of the most commonly used computer security-related terms, such as integrity, quality, value, accountability, auditability, access control, and even data and computer security. An understanding of such terms constitutes a virtual sine qua non for the usefulness of the following material.

4. Computer Security Policy Statements

Treat here the need for policy statements, guidance in the preparation and issuance, and sample policies which have proven effective. Include here comments on enforcement.

16.2.2 Application code

16.2.2.1 Purchased

16.2.2.2 In-House Generated

16.3 Physical Security

16.4 Contingency Planning

16.4.1 Emergency Response Measures

16.4.2 Back-Up Plans

16.4.3 Recovery Plans

16.5 Security Procedures and Practices

16.6 Protection against Electromagnetic or Acoustic Eavesdropping

16.7 Protection against Communications Intercept
This section should include enough guidance in cryptography to understand those aspects essential to the selection and implementation of appropriate means. In addition, it should provide enough information to relieve fear that cryptography is too complex, costly or burdensome for most conventional systems. References to more detailed treatments of cryptography are important.

17. Message Authentication and Digital Signatures

18. Microcomputer Security

Physical and logical. Include comments on legal/ethical issues involving software.

19. Security in Local Area Networks

20. Viruses, Worms, Trojan Horses, etc.

21. The importance of Federal, National and International Standards in the Selection and Implementation of Security Measures to Assure Quality and Availability

22. Monitoring Security Measures and Controls

Describe here the very important role of the internal audit function in seeing that all appropriate security controls have been selected and implemented.

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

OCT 26 1990

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

Dear Dr. Ware:

Thank you for your recent recommendation from the Computer System Security and Privacy Advisory Board on the need for the National Institute of Standards and Technology (NIST) to issue computer security guidelines. We at NIST share the Board's interest in seeing that timely computer security standards and guidelines are developed and promulgated. The outline developed by the Board appears to provide a useful framework for those seeking to utilize appropriate computer security measures.

I will be meeting with James Burrows, Director of the National Computer Systems Laboratory, to discuss alternatives for the development of a document to meet the needs identified by the Board. I have asked him to keep the Board apprised of our progress on this matter.

Let me take this opportunity to emphasize my appreciation for the continued efforts of the Board to improve the level of computer security in the federal government. I look forward to receiving further reports from the Board.

Sincerely,

ORIGINAL SIGNED BY
RAYMOND G. KAMMER

John W. Lyons
Director

THE NATIONAL COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

OCT 2 0 1990

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

Dear Mr. Secretary:

Pursuant to its responsibility under the Computer Security Act of 1987, the Computer System Security and Advisory Board wishes to call the following issue to your attention.

The European Community has developed and circulated for comment a draft Information Technology Security Evaluation Criteria document. This proposed standard is similar to but different in important ways from the U.S. Trusted Computer System Evaluation Criteria. Both are intended as guidance to computer vendors in developing secure computer systems and products.

Since much of U.S. industry is multi-national, the possibility of a European standard significantly different from a U.S. posture is an important issue.

Such divergence could:

a) Impact the ability of the U.S. computer industry to market in Europe; and

b) Impact multi-national users who operate computer systems in various countries which may be required to use local standardization.

The situation is properly being monitored by the National Institute of Standards and Technology (NIST) and the National Computer Security Center of the National Security Agency (NSA).

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

However, we believe this is an important emerging issue and therefore we strongly recommend that you:

a) Actively coordinate this issue within the government including such departments as the U.S. Department of State, International Trade Administration and Office of the U.S. Trade Representative; and

b) Actively protect the interests of U.S. industry via our international representation in the International Standards Organization arena.

It is of the utmost national importance that the efforts of NIST and NSA be sustained, encouraged, and supported.

Sincerely,

Willis H. Ware

Willis H. Ware
Chairman

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

December 18, 1990

Dr. Willis 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:

Thank you for your letter regarding the recommendations of the Computer System Security and Privacy Advisory Board concerning the draft Information Technology Security Evaluation Criteria developed by the European Community. I have asked the Office of the Under Secretary for Technology to examine the important issues raised in your letter. Also, the National Institute of Standards and Technology is working with the Europeans to address United States' concerns with their draft criteria.

I would like to take this opportunity to express my appreciation for the continued efforts of the Board to improve the level of computer security in the federal government. I look forward to receiving further reports from you.

Sincerely,

Robert A. Mosbacher

IV. Future Advisory Board Activities

At its December meeting, the Board discussed a number of agenda topics for its 1991 meetings. Among the more important topics and questions of possible interest are:

Computer Security Guidelines and Standards

The Board would like to continue to receive updates of NIST plans and programs for an international solution/harmonization of computer security requirements and continue to monitor European developments. Also to be included are updates from NSA on Orange Book experiences and plans for any additional guidance and standards.

NIST Plans and Activities

Includes regular updates of status of completing guidelines document suggested by the Board and updates on current NIST projects and workplans, including priorities, schedule for rewrite of outdated guides, and work deferred due to lack of resources.

Privacy - EC Green Paper

This topic includes a briefing of EC Green paper vis-a-vis U.S. position which should include status report from Congress. Also, included are briefings on current privacy issues by organizations, individuals with competing views, and possibly Congressional staff.

Implementation of the Computer Security Act of 1987

Subsumed under this heading are various related issues the Board would like to address in 1991. These include an examination of Office of Management and Budget policies, including the anticipated rewrite of OMB Circular A-130. Also of interest is the role of the Inspector General in computer security. Computer security training and its effectiveness are also to be studied. Lastly, the Board would look into the status of OMB/NIST/NSA security planning agency visits.

Software Engineering and Reliability

Much attention is focussed on security environments, products and data bases. Less has been said about the quality and reliability of application software. An April, 1990 Congressional report (Bugs in the Program) questions whether the federal government is capable of developing software as reliable as it needs. The Board would like to be briefed on the state-of-the-art in software reliability.

Security and the Public Switched Network

A number of studies have highlighted the vulnerabilities of the public switched network. At the moment, much activity is taking

place behind closed doors on this issue, particularly in the National Security Emergency Preparedness arena. At some point this issue needs to be surfaced and examined by the Board.

Use of Security Products and Features

A study conducted by the President's Council on Integrity and Efficiency indicated that many security functions and features were either unused or misused by system administrators and users. The experience of emergency response teams further bears this out. The Board would like to examine what must be done to change this and whether better guidelines are needed on how to use basic security tools such as passwords.

Rewrite of NSDD-145 and the NIST/NSA Memorandum of Understanding

The Board would like to continue to receive written updates or briefings by NSA/NIST on the status of the NIST/NSA Memorandum of Understanding and the recent Presidential directive on computer and telecommunications security.

Computer Emergency Response Team (CERT)

The Board believes that it would be useful to hear from NIST, other participants in the CERT program as well as victims of malicious software attacks. Periodic briefings on the CERT system and what lessons can be learned to improve security would be useful. Since most incidents occur because accepted routine security practices are not followed, should this not be well publicized, as an awareness or training tool?

Digital Signature

It is likely that during 1991 the Board will have the opportunity to examine the new digital signature algorithm.

International Hacking

Cases continue to be uncovered such as those that Cliff Stoll documented seems to be happening. Hackers continue to exploit the same old vulnerabilities that Stoll and many others have documented. Where is the accountability for taking care of known problems? Second, there appears to be continuing organizational confusion on the international hacking problem (i.e., who in the government, if anyone, is or should be responsible?)

V. Conclusions

During its second year, the Board continued to build the foundation toward 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.