

**1992 ANNUAL REPORT**  
**OF THE**  
**NATIONAL COMPUTER SYSTEM SECURITY**  
**AND**  
**PRIVACY ADVISORY BOARD**

**MARCH 1993**



## Executive Summary

This Annual Report documents the activities of the National Computer System Security and Privacy Advisory Board during 1992, its fourth year. The Board, which met four 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 identified the need and called for a National Cryptographic Review and has issued letters containing the Board's positions and recommendations to the appropriate Executive Branch officials. The letters identified issues surrounding cryptographic standards and the strength and availability of cryptographic products.

The Board's recommendations for the review stressed the need to involve participants from a variety of communities, including: manufacturers, users, government unclassified, the Intelligence Community, law enforcement and others. The Board worked hard to guarantee appropriate public participation in this review before final decisions were made in the federal government.

During the past two years the Board has continued to monitor the agency visit program by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA). This was a series of meetings between senior federal agency officials and OMB/NIST/NSA representatives to discuss agency computer security programs. In January 1992, the Board sent a letter to the Director of OMB supporting the visit program and recommending that a summary report be prepared. In its final report on these visits, OMB referenced the Board's support for this activity.

The federal criteria effort between NIST and NSA was also of continued interest to the Board this year. The Board asked for updates at each meeting to closely follow the effort's progress. While the Board took no universal position, some individual members expressed views somewhat skeptical of the overall project's goals and objectives. Next year the Board will continue to monitor this endeavor.

NIST's cryptographic standards activities were closely followed by the Board this year. This included NIST's proposed digital signature standard and secure hash standard. In March 1992, the Board agreed not to take a formal position on the DSS until related cryptographic review issues were completed. Much of the September meeting was largely devoted to cryptographic issues including NIST's standards activities.

The Board also examined a number of other issues, including:

**Virus Incidents;**

**E-Mail Privacy;**

**NIST's Information Technology Security Handbook;**

**Information Technology Research Programs of the European Community; and**

**Security Issues Inherent in Citizens Access to Government Electronic Records.**

The Board did not take a formal position on these issues, judging that to do so would be premature. However, the Board did provide a useful public forum for discussions of computer security issues within the unclassified sectors of the government.

The Board also established a work plan for 1993 which identified candidate topics for in-depth examination. These include:

- **National Review of Cryptography;**
- **Data Encryption Standard Revalidation;**
- **Public Key Cryptography;**
- **Telecommunications Security;**
- **Trusted System Criteria and Evaluation;**
- **Computer Security Guidelines and Standards;**
- **Security Evaluation Process;**
- **Privacy;**
- **Changes in National Computer Security Policies;**
- **Implementation of the Computer Security Act;**
- **Risk and Threat Assessment;**

- **Electronic Data Interchange (EDI) Security;**
- **The National Computer Security Conference;**
- **Monitoring Activities;**
- **Security and Open Systems;**
- **Effective Use of Security Products and Features;**
- **Status of Computer Emergency Response Capabilities in Civil Agencies;**
- **International Hacking;**
- **Local Area Network (LAN) Security;**
- **Information Security Foundation;**
- **Security and the Public Switched Network; and**
- **Citizen Access to Government Electronic Records.**

**The Board has expressed a desire to maintain a continuing interest in certain specific aspects of the NIST program or to receive periodic briefings on various critical issues, including:**

- **NIST's Cryptographic Standards;**
- **NIST/NSA Criteria Project; and**
- **The Revision of A-130, Appendix III.**

**These issues, coupled with an ever growing number of new security-related public policy issues, clearly demonstrated the extensive work which lies ahead for the Board in 1993 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 (NIST) 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 for a second time on March 27, 1992 by U.S. Department of Commerce Assistant Secretary for Administration Preston Moore. (See Appendix B for the text of the current charter.)

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 members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;
- four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and
- four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

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 1992, the full membership of the Board is as follows:

- Chairman  
Willis H. Ware, RAND
- Federal Members  
Bill D. Colvin, National Aeronautics and Space Administration  
Patrick R. Gallagher, National Security Agency  
Henry H. Philcox, Department of the Treasury, IRS  
Cynthia C. Rand, Department of Transportation
- Non-Federal, Non-Vendor  
Cris R. Castro, ManTech, Inc.  
John A. Kuyers, Ernst and Young  
Sandra Lambert, Citibank  
Eddie L. Zeitler, Fidelity Investments

- Non-Federal  
Gaetano Gangemi, Wang Laboratories, Inc.  
Steven B. Lipner, Digital Equipment Corporation,  
Subsequently of the MITRE Corporation  
Stephen T. Walker, Trusted Information Systems, Inc.  
Bill Whitehurst, International Business Machines Corp.

During 1992, Ms. Sandra Lambert was confirmed as a Board member filling the vacancy in the non-federal, non-vendor category. In addition, Mr. Bill Whitehurst of IBM Corp. replaced Mr. Lawrence Wills in the non-federal category, and Dr. Willis Ware was re-appointed Chairman.

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.

## II. Major Issues Discussed

The following section summarizes the discussions held by the Board in 1992. Additionally, the Board accomplishes much informal, non-decisional, background discussion and preparation for meetings by electronic 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, June, September, and December meetings are included as Appendices C to F, respectively. The required Federal Register announcement notices for the meetings are presented in Appendix G.

The substantive work of the Board during 1992 was devoted to various topics related to the security of federal unclassified automated information systems. Among the most important were:

- A National Review of the Use of Cryptography;
- Trusted Systems FIPS; and
- NIST's Digital Signature Standard.



## A National Review of the Use of Cryptography

During 1992, the Board identified the need for a national review of the public policy issues regarding the use of publicly available cryptography. The issue arose following the Board's examination of NIST's proposed DSS. The factors which led to the selection of this algorithm were indicative of larger issues, compounding the need for a national review. In March, Mr. Steve Walker proposed that the Board call for such a review. The Board explained that it saw the need for input from a wide variety of communities, including:

- The federal government for its own operational needs and in its role within the international community;
- The defense establishment, notably the communications security and various intelligence functions;
- Law enforcement for not only its own security needs but also for counter-intelligence actions against law-breaking organizations;
- Civil and other non-classified government to protect its unclassified yet sensitive data;
- Private sector corporations that function domestically and internationally and must protect sensitive data and communications;
- Society at large as users of telephony and other services that must assure confidentiality and privacy for communications;
- The individual as a user of personal computers and the data networks of the world with their extensive array of information services; and
- The academic community in pursuit of a legitimate discipline of study and research.

The Board agreed with Mr. Walker's proposal and sent a letter to cognizant governmental officials with their recommendation for the review. (See Exhibits III and V.) During the year, the Board also sought to assist NIST in identifying prominent organizations and individuals who should participate in the review. In fact, a special three-day meeting was called by the Board in September for just this purpose. Facing a change of administrations following the Presidential election, the Board agreed to send two letters. The first was sent to Bush Administration officials urging that they notify their transition teams of the

importance of the review. The second letter was sent to Clinton Administration officials urging them to support the review, (See Exhibits VII and IX.)

Related to this effort, the Board also monitored the development of an agreement between the Software Publishers Association and the National Security Council to allow the expedited export of products containing specified cryptographic algorithms. The Board was particularly interested in the strength of the algorithms and their potential to emerge as defacto standards.

### Trusted Systems FIPS

During 1992, the Board continued to monitor the joint NIST and NSA project to develop a replacement for the Department of Defense "Orange Book," the Trusted Computer Security Evaluation Criteria. The Board heard updates from Stu Katzke and Gene Troy of NIST's Computer Security Division and Lt. Col. Ron Ross of NSA on both the criteria effort and the Trusted Technology Assessment Program, under which evaluations against the criteria will be conducted. A first draft of the FIPS was expected to be released in January, 1993. The Board plans to continue to monitor this effort.

### NIST's Digital Signature Standard

Since 1991, the Board has been actively interested in NIST's progress toward developing a DSS FIPS, which was proposed by NIST in mid-1991 for public review and comment. In February 1992 the public comment period for NIST's proposed DSS closed. The Board was briefed on the comments received by NIST and how NIST planned to respond. A number of issues remain outstanding before NIST recommends the adoption of the standard to the Secretary of Commerce for approval. The Board will continue to pursue its interest in this issue.

Comments from the private sector were generally negative while those from federal agencies were neutral to favorable. Many also called for a federal key management standard using public key cryptography, which NIST is studying.

In December 1991, the Board authorized and directed the Chairman to meet with Dr. John W. Lyons, Director of NIST, to express their concerns with respect to the DSS.

In early 1992, Dr. Ware met with Dr. Lyons regarding the private sector opposition to DSS. Dr. Lyons said the private sector would have to clearly explain the negative economic impacts of the DSS if a change is desired. Dr. Lyons does not see a case from the DSS comments that the adoption of the DSS would cause significant financial hardship or dislocation for the private sector.

### III. Advisory Board Correspondence

During 1992, the Board issued letters reporting its findings on cryptographic technology and the call for a national review of the issue.

#### Cryptographic Technology, Including Encryption

The Board issued a letter to the Secretary of Health and Human Services expressing its concerns for the need to protect the confidentiality of patient information.

Also, on April 1, 1992, the Board issued letters to the Secretary of Commerce, the Department of Defense, the Attorney General of the Department of Justice, the Director of the Office of Management & Budget, The Director of the National Institute of Standards and Technology, and the Director of the National Security Agency, soliciting their support of a call for a national review of the use of cryptography. A resolution calling for a national review and two related resolutions pertaining to the endorsement of the DSS were included as enclosures to the letters.

#### Exhibits

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

- Exhibit I      Letter dated, March 31, 1992, from Chairman Ware to the Honorable Louis Sullivan of HHS on protecting the confidentiality of patient data and patient records.
- Exhibit II      Answer from Jeff Sanders, Director, Office of Legislation & Policy.
- Exhibit III     Letter dated, April 1, 1992, from Chairman Ware to the following on the issue of a national cryptographic review:
- Honorable Barbara Hackman Franklin  
Secretary of Commerce
- Mr. Duane P. Andrews  
Department of Defense
- Honorable Richard G. Darman  
Office of Management & Budget

**Dr. John W. Lyons  
Director, National Institute of Standards  
and Technology**

**Vice Admiral W.O. Studeman  
Director, National Security Agency**

**Exhibit IV      Answer from Under Secretary of Commerce for Technology (Dr. White) to Chairman Ware agreeing with a national cryptographic review**

**Exhibit V      Follow-up letter from Chairman Ware to the following on the issue of a national cryptographic review:**

**Honorable Richard G. Darman  
Office of Management & Budget**

**Honorable William P. Barr  
Attorney General**

**Mr. Duane P. Andrews  
Department of Defense**

**Vice Admiral John M. McConnell, USN  
Director, National Security Agency**

**Exhibit VI      Answer from the following to Chairman Ware regarding a national cryptographic review:**

**Mr. James B. MacRae, Jr.  
Office of Management & Budget**

**Mr. Duane P. Andrews  
Department of Defense**

**Vice Admiral John M. McConnell, USN  
Director, National Security Agency**

**Exhibit VII      Letter dated, December 16, 1992, from Chairman Ware to the following requesting that appropriate action be taken on and the new administration be made aware of the issue of a national cryptographic review:**

**Honorable Barbara Franklin  
Department of Commerce**

**Honorable William P. Barr  
Attorney General**

**Honorable Nicholas F. Brady  
Department of the Treasury**

**Honorable Richard B. Cheney  
Department of Defense**

**Honorable Richard G. Darman  
Office of Management & Budget**

**Honorable Lawrence S. Eagleburger  
Secretary of State**

**Honorable Robert M. Gates  
Director of Central Intelligence**

**Honorable Brent Scowcroft  
Assistant to the President  
for National Security Affairs**

**Exhibit VIII     Answer from Mr. Theodore J. Clark, Central Intelligence Agency,  
to Chairman Ware in support of a national  
cryptographic review**

**Exhibit IX       Letter dated, January 22, 1993, from Chairman Ware to the  
following requesting support of a national cryptographic  
review:**

**Honorable Ronald H. Brown  
Secretary of Commerce**

**Honorable Les Aspin  
Department of Defense**

**Honorable Warren Christopher  
Department of State**

**Honorable Lloyd Bentsen  
Department of Treasury**

**Mr. William S. Sessions  
Director, Federal Bureau of Investigation**

**Honorable Anthony Lake  
National Security Council**

**Honorable Robert Rubin  
Director, National Economic Council**

**Honorable Leon Panetta  
Director, Office of Management and Budget**

**Exhibit X      Answers from the following to Chairman Ware regarding a  
national cryptographic review:**

**Honorable Ronald H. Brown  
Secretary of Commerce**

**Mr. William D. Clarke  
Department of State**

**Mr. William S. Sessions  
Director, FBI**

**Honorable Robert E. Rubin  
Director, National Economic Council**

THE NATIONAL  
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987*

March 31, 1992

Honorable Louis Sullivan  
Department of Health and Human Services  
200 Independence Avenue, S.W.  
Washington, DC 20201

Dear Mr. Secretary:

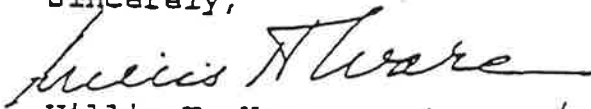
I am writing to you as the chairman of the Computer System Security and Privacy Board which was created by the Computer Security Act of 1987 and is charged with identifying latent policy issues and potential problems related to government utilization of computer and communication technology. While we have concentrated for three years on matters related to security, it is our intent this year to emphasize the Privacy aspect of our name and responsibility.

On November 6 of last year, the Washington Post reported your activity in regard to a uniform nationwide health insurance billing system. You correctly and quite properly noted that there will be a major problem in protecting the confidentiality of patient data and patient records. This aspect -- data protection -- is very much related to both computer system security and privacy and hence, falls within our interests.

I would imagine that the HHS has identified a particular program office to oversee this huge development and to assure that both system security and patient confidentiality are properly attended. It may prove that our Board can be of support to the Department as it moves forward; but probably, the initial move would be to put us in contact with the appropriate person or officer. We can take it from there and arrange for discussions and briefings as prove relevant and mutually productive.

Thank you for your attention in this matter.

Sincerely,



Willis H. Ware  
Chairman

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







APR 24 1992

Mr. Willis H. Ware  
Chairman  
Computer System Security & Privacy Advisory Board  
Technology Building, Room B154  
Gaithersburg, MD 20899

Dear Mr. Ware:

Thank you for contacting Secretary Sullivan on the issue of system security and patient privacy, regarding the Department's initiative toward an electronic health care system. He has asked me to respond to you directly.

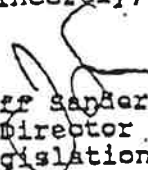
As the Secretary stated at the November 5 Forum on Administrative Costs, to which you refer in your letter, the Department of Health and Human Services views confidentiality of patient medical information as having paramount importance. Computerization of clinical information can only be achieved, nationwide, if patients are assured that their privacy will be protected.

Staff throughout the Department are working on this issue. Let me provide you with several points of contact. First, I am involved in implementation of the portions of the President's Comprehensive Health Reform Program that deal with the electronic health care system. I would be glad to speak with you about our plans; I can be reached at 202-426-3950.

You may also wish to contact the HHS Task Force on the Privacy of Private-Sector Health Records, which is chaired by Joan Turek-Brezina (phone: 202-245-6141) of the office of the Assistant Secretary for Planning and Evaluation. Another good contact would be J. Michael Fitzmaurice of the Agency for Health Care Policy and Research (phone 301-227-8483), which is the lead component within the Public Health Service on computerized clinical information matters.

Thank you for your interest in this important issue.

Sincerely,

  
Jeff Sanders  
Director  
Office of Legislation and Policy



THE NATIONAL  
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987*

April 1, 1992

Honorable Barbara Hackman Franklin  
Secretary of Commerce  
Washington, DC 20230

Dear Ms. Franklin:

The rapid progress of communications, computer, and electronic technology in the last 40 years has created a genuine civilian and non-defense demand for cryptographic techniques and devices to protect computer data, computer systems, and other communications against unauthorized access and eavesdropping.

Cryptographic technology, which includes encryption, historically has been in the custody of the defense and military establishment of the United States. A similar situation has prevailed throughout the world for centuries, but there have become many stakeholders all of whom now have a legitimate interest in cryptography, its technology, its operational deployment, and its oversight. Among them are the following.

- The Federal government for its own operational needs and in its role within the international community.
- The defense establishment, notably the communications security and various intelligence functions.
- Law enforcement for not only its own security needs but also for counter-intelligence actions against law-breaking organizations.
- Civil and other non-classified government to protect its unclassified yet sensitive data.
- Private sector corporations that function domestically and internationally and must protect sensitive data and communications.
- Society at large as users of telephony and other services that must assure confidentiality and privacy for communications.

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

- The individual as a user of personal computers and the data networks of the world with their extensive array of information services.
- The academic community in pursuit of a legitimate discipline of study and research.

The interests of all such parties overlap and are often in conflict which makes the matter an urgent concern of national policy. In view of this, the Computer System Security and Privacy Advisory Board (CSSPAB), created by the Computer Security Act of 1987 and charged under the Act to identify latent issues of national policy significance, resolved during its March 17-18 meeting to call for a national public review of the issue.

The resolution and two related ones are enclosed to this letter. The Board commends them to your attention and solicits your support of this important action.

Sincerely,



Willis H. Ware  
Chairman

Enclosure

**Identical letters sent to:**

Mr. Duane P. Andrews  
Department of Defense  
The Pentagon  
Washington, DC 20301

Attorney General William P. Barr  
Department of Justice  
10th Street & Constitution Ave., NW  
Washington, DC 20530

Honorable Richard G. Darman  
Office of Management & Budget  
Old Executive Office Building  
17th Street & Pennsylvania Avenue, NW  
Washington, DC 20515

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

Vice Admiral W.O. Studeman  
Director, National Security Agency  
9800 Savage Road  
Fort George G. Meade, MD 20755-6000

## COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

## RESOLUTION #1

March 18, 1992

The Board has examined the present status of the proposed Digital Signature Standard (DSS) being undertaken by the National Institute of Standards and Technology (NIST). In view of:

- (1) the significant public policy issues raised during the review of the proposed standard;
- (2) the increasingly pervasive use of digital technologies;
- (3) the potential impacts upon the security of the unclassified/sensitive government community;
- (4) the relationship of the DSS to the existing NIST cryptographic security program; and
- (5) the posture of the U.S. in international commerce.

## THE BOARD FINDS THAT:

- (1) a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required. This national level review must involve the national security, law enforcement, government unclassified/sensitive, and commercial communities. Representatives from the private sector should include both vendors and users. In the next several months, NIST/NSA should sponsor a workshop on the widespread use of cryptography. This national review should be concluded by June 1993 and should result in a national policy concerning the use of cryptography in unclassified/sensitive government and the private sector.
- (2) NIST has made significant progress in resolving the technical issues related to the proposed DSS. The Board recommends that NIST continue to seek resolution of the patent, infrastructure, and other remaining issues raised during the public comment process. The Board recognizes that much of the work, and in particular the infrastructure, is algorithmic independent and must be continued by NIST to assure timely implementation of digital signature technology within the government.

FOR: Colvin, Gallagher, Gangemi, Kuyers, Lipner, Philcox,  
Rand, Walker, Wills, and Zeitler  
AGAINST: None ABSTAIN: None

Motion Unanimously Approved.

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION #2

March 18, 1992

The Board resolves that:

The approval of the Digital Signature Standard (DSS) by the Secretary of Commerce should be considered only upon conclusion of the national review.

The Board agrees to continue to monitor the activities involving the DSS and the proposed national review at future meetings.

FOR: Colvin, Kuyers, Lipner, Philcox, Rand, Walker, Wills, and Zeitler

AGAINST: Gallagher, Gangemi

ABSTAIN: None

Motion Approved.

Background: In August, 1991, the National Institute of Standards and Technology issued a draft Digital Signature Standard as a Federal Information Processing Standard. This resolution #2 should be read in context of Resolution #1, calling for a national public review of the use of cryptography.

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION #3

March 18, 1992

The Board resolves that:

The Board defers making a recommendation on approval of the Digital Signature Standard (DSS) pending progress on the national review.

The Board agrees to continue to monitor the activities involving the DSS and the proposed national review at future meetings.

FOR: Colvin, Gallagher, Gangemi, Kuyers, Lipner, Philcox, Rand,  
Walker, Wills, and Zeitler

AGAINST: None

ABSTAIN: None

Motion Unanimously Approved.

Background: In August, 1991, the National Institute of Standards and Technology issued a draft Digital Signature Standard as a Federal Information Processing Standard. This resolution #3 should be read in context of Resolution #1, calling for a national public review of the use of cryptography.







UNITED STATES DEPARTMENT OF COMMERCE  
The Under Secretary for Technology

Washington, D.C. 20230  
DIRECTOR'S OFFICE

NIS

'92 MAY -1 P5:08

APR 28 1992

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

Dear Dr. Ware:

On behalf of the Secretary of Commerce, I would like to thank you for the recent recommendation of the Computer System Security and Privacy Advisory Board regarding the need for a national public review of the use of cryptography. We agree with the Board's call to hold such a public discussion on these important issues.

The Director of the National Institute of Standards and Technology has initiated the activities necessary to accomplish this review. We anticipate this will lead to a set of position statements which will address the issues raised by the Board.

I appreciate the Board's continued dedication to the identification of emerging computer security issues and look forward to hearing from you in the future.

Sincerely,

Robert M. White, Ph.D.



THE NATIONAL  
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987*

July 2, 1992

Honorable Richard G. Darman  
Office of Management & Budget  
Old Executive Office Building  
17th Street & Pennsylvania Avenue, NW  
Washington, DC 20515

Dear Mr. Darman:

This is a follow-up letter from the Computer System Security and Privacy Advisory Board to our earlier letter to your office of April 1, 1992. (See Enclosure #1.) In it, pursuant to our responsibilities under the Computer Security Act of 1987, we identified cryptography for general civilian use and its export control as a latent issue of high significance and called for a national public review and dialogue.

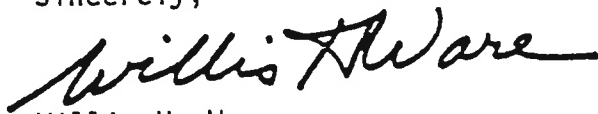
Dr. Robert M. White, Under Secretary of Commerce for Technology, advised in his response of April 28, 1992 that the National Institute of Standards and Technology (NIST) has initiated activities to accomplish this review and indicated his agreement with the importance of this matter. (See Enclosure #2.)

In our effort to further support NIST's preparation for the national review, the Board plans to hold its next meeting devoted to the subject of cryptography. (See Enclosure #3.)

The Board wishes to advise your office of its intent and to solicit the participation of your representative to help set the agenda for the national review.

Thank you for your support.

Sincerely,



Willis H. Ware  
Chairman

Enclosures

Identical letters sent to:

Honorable William P. Barr  
The Attorney General  
Washington, DC 20530

Mr. Duane P. Andrews  
Department of Defense  
The Pentagon  
Washington, DC 20301

Vice Admiral John M. McConnell, USN  
Director, National Security Agency  
9800 Savage Road  
Fort George G. Meade, MD 20755-6000

A

H  
O  
O  
l  
W

D

T  
t  
a  
t  
c

(  
l  
c  
-:

THE NATIONAL  
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987*

April 1, 1992

Honorable Richard G. Darman  
Office of Management & Budget  
Old Executive Office Building  
17th Street & Pennsylvania Avenue, NW  
Washington, DC 20515

Dear Mr. Darman:

The rapid progress of communications, computer, and electronic technology in the last 40 years has created a genuine civilian and non-defense demand for cryptographic techniques and devices to protect computer data, computer systems, and other communications against unauthorized access and eavesdropping.

Cryptographic technology, which includes encryption, historically has been in the custody of the defense and military establishment of the United States. A similar situation has prevailed throughout the world for centuries, but there have become many stakeholders all of whom now have a legitimate interest in cryptography, its technology, its operational deployment, and its oversight. Among them are the following.

- The Federal government for its own operational needs and in its role within the international community.
- The defense establishment, notably the communications security and various intelligence functions.
- Law enforcement for not only its own security needs but also for counter-intelligence actions against law-breaking organizations.
- Civil and other non-classified government to protect its unclassified yet sensitive data.
- Private sector corporations that function domestically and internationally and must protect sensitive data and communications.
- Society at large as users of telephony and other services that must assure confidentiality and privacy for communications.

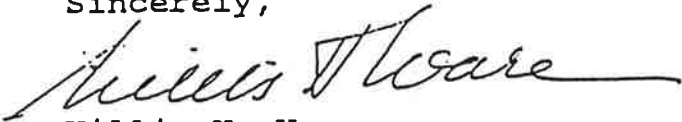
Executive Secretariat: Computer Systems Laboratory  
National Institute of Standards and Technology  
Technology Building, Room 8154, Gaithersburg, MD 20899  
Telephone (301) 975-3240

- The individual as a user of personal computers and the data networks of the world with their extensive array of information services.
- The academic community in pursuit of a legitimate discipline of study and research.

The interests of all such parties overlap and are often in conflict which makes the matter an urgent concern of national policy. In view of this, the Computer System Security and Privacy Advisory Board (CSSPAB), created by the Computer Security Act of 1987 and charged under the Act to identify latent issues of national policy significance, resolved during its March 17-18 meeting to call for a national public review of the issue.

The resolution and two related ones are enclosed to this letter. The Board commends them to your attention and solicits your support of this important action.

Sincerely,



Willis H. Ware  
Chairman

Enclosure

NOTE: Enclosures are not reproduced here as they are included in Exhibit III.

APP  
r.  
na:  
an  
and  
70  
an  
ea:  
n  
or  
ri  
ev  
sal  
the  
ec  
hi  
sta  
a  
de  
for



ENCLOSURE #2  
UNITED STATES DEPARTMENT OF COMMERCE  
The Under Secretary for Technology  
Washington, D.C. 20230

APR 28 1992

Dr. Willis H. Ware  
Chairman, Computer System Security  
and Privacy Advisory Board  
and Corporation  
700 Main Street  
Santa Monica, CA 90406-2138

Dear Dr. Ware:

On behalf of the Secretary of Commerce, I would like to thank you for the recent recommendation of the Computer System Security and Privacy Advisory Board regarding the need for a national public review of the use of cryptography. We agree with the Board's call to hold such a public discussion on these important issues.

The Director of the National Institute of Standards and Technology has initiated the activities necessary to accomplish this review. We anticipate this will lead to a set of position statements which will address the issues raised by the Board.

We appreciate the Board's continued dedication to the identification of emerging computer security issues and look forward to hearing from you in the future.

Sincerely,

A handwritten signature in black ink, appearing to read "R. White".

Robert M. White, Ph.D.

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD  
RESOLUTION  
June 11, 1992

At its March meeting the Computer System Security and Privacy Advisory Board recommended that the federal government conduct a public review of the issues surrounding the civil and public use of cryptography. In order to make itself more aware of the issues and to assist the National Institute of Standards & Technology (NIST) in framing the recommended public review, the Board requests the Executive Secretary to schedule a special Board meeting, as soon, in advance of the date scheduled for the September meeting, as feasible to address issues relevant to the public review and develop an agenda for the review. At this special meeting the Board proposes to consider the following issues and positions:

- (1) The dimensions and parameters of cryptographic technology;
- (2) U.S. and International Market needs for cryptographic technology including industry input on actual market size and sensitivity;
- (3) U.S. export controls on cryptographic products including: policy, procedures, and industry experience with implementation of the controls;
- (4) Non-U.S. export and use controls on cryptographic products including: U.S. industry experience with foreign governments' application of controls and foreign availability of cryptographic products;
- (5) The present status of the reported negotiations, between U.S. government and industry, that may result in the relaxation of U.S. export controls on encryption embedded in mass market software; and
- (6) The interests of the defense, intelligence, and law enforcement communities as to the availability and export of cryptographic products.

The Board requests that the Executive Secretary work with Board members, NIST personnel, and others as appropriate to begin preparations for the special meeting. The Board expects that topics for discussion will involve the presentation of proprietary or private information, and that they will also involve the presentation of classified information. Consequently the Board requests the Executive Secretary to take such actions as necessary to conduct those portions of the special meeting where such proprietary and classified information will be discussed as closed sessions, in accordance with the criteria enumerated in the Department of Commerce Committee Handbook.

The Board authorizes the Chairman to identify a subcommittee for members to assist the Executive Secretary with planning for this meeting, and to review for suitability to the Board's purpose classified briefing material proposed for presentation to the entire Board.

FOR: Castro, Colvin, Gallagher, Gangemi, Kuyers, Lipner, Rand, Walker, Wills, and Zeitler

AGAINST: None ABSTAIN: None

Motion Unanimously Approved





EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

EXHIBIT VI

AUG 26 1992

Dr. Willis H. Ware  
Chairman  
The National Computer Security  
and Privacy Advisory Board  
1700 Main Street  
Santa Monica, CA 90406-2138

Dear Dr. Ware:

This is in response to your letter of July 2, 1992 to Director Darman concerning the Board's recommendation calling for a public review and dialogue about use of cryptography and its export control.

In our view, public discussion of this important issue has been and should be ongoing. We note, for example, recent hearings held by the Committee on the Judiciary of the U.S. House of Representatives on this subject. The effect of the Board's recommendation -- to further heighten visibility of and participation in the discussion -- can only be helpful.

I believe it is critical that the discussion be based upon factual information and analysis if it is to result in productive policy. In this regard, the technical expertise of the Board will prove to be an important resource. To the extent that the Board's action contributes to development of data and analysis of the impact of existing and potential policies it will provide a great service. Some facets of the issue could hamper or undermine existing capabilities for law enforcement or affect our national defense. I trust the Board will use its discretion in public discussion in these circumstances, carefully weighing the advantages of discussion versus possible harm.

We look forward to working with the Board in helping to set the agenda for this important and continuing public discussion.

Sincerely,  
Original Signed by  
James B. MacRae, Jr

James B. MacRae, Jr.  
Acting Administrator  
and Deputy Administrator  
Office of Information  
and Regulatory Affairs



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

21 August 1992

COMMAND, CONTROL,  
COMMUNICATIONS  
AND  
INTELLIGENCE

Dr. Willis H. Ware  
Chairman  
National Computer System Security  
and Privacy Advisory Board  
National Institute of Standards and Technology  
Room B154  
Gaithersburg, Maryland 20899

Dear Dr. Ware:

The importance of maintaining the confidentiality, integrity, and availability of information are of vital interest to the Department of Defense. General civilian use of cryptography and its export control are of material relevance to these concerns. In fulfilling the responsibility of the National Computer System Security and Privacy Advisory Board to identify such issues and advise the Secretary of Commerce, the Administration, and Congress, the Board will address matters currently being considered and acted upon by the Department of Defense. I believe both the Department and the Board may profit from an exchange of information and viewpoints.

I have directed Mr. Dan Ryan, Director of Information Systems Security, to contact you regarding support for your review of these issues.

Sincerely,

A handwritten signature in cursive script, appearing to read "Duane P. Andrews", is written in black ink.

Duane P. Andrews

NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

23 July 1992



Dr. Willis H. Ware  
Chairman, National Computer System  
Security and Privacy Advisory Board  
and Corporation  
700 Main Street  
P.O. Box 2138  
Santa Monica, CA 90407-2138

Dear Dr. Ware:

We have read with interest your letters of 2 July 1992 and April 1992 and your Board's resolution calling for a national public review on the use of cryptography.

The National Security Agency has serious reservations about a public debate on cryptography. We do, however, support the need to ensure that government decision makers are made aware of the oft-conflicting interests of the various stakeholders who seek to influence cryptographic policy. To the extent that we can be assured that national security interests will not be jeopardized in a public debate, we are willing to pursue with NIST actions that address the concerns raised by the Board.

J.M. McCONNELL  
Vice Admiral, U.S. Navy  
Director, NSA

Copy Furnished:  
Attorney General  
Secretary of Commerce  
Director, OMB  
ASDC<sup>3</sup>I  
Director, NIST



THE NATIONAL  
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987*

December 16, 1992

Honorable Barbara Franklin  
Department of Commerce  
14th & Constitution Avenue, NW  
Washington, DC 20230

Dear Madam Secretary:

The Computer System Security and Privacy Advisory Board is directed under the Computer Security Act of 1987 to identify emerging public policy issues related to information, computers and communications technology; and to bring them to the attention of national decision makers for consideration.

The Board has before it an issue that has not been resolved at the national level, but has become of such importance and urgency that it must have high priority for the next administration. We request that you take the appropriate actions needed to identify public cryptography as a critical policy issue to the new administration through key senior career officials and the transition team members. We send this letter to you as a Federal official whose organization will be affected by resolution of this issue.

The rapid progress of communications, computer, and electronic technology in the last 40 years has created a genuine civilian and non-defense demand for cryptographic techniques and devices to protect computer data, computer systems, and other communications against unauthorized access and eavesdropping. These advances impact such diverse national concerns as international competitiveness and its consequences for trade balance and state of the economy, pivotal societal privacy issues such as those of medical patient records, national security in a rapidly changing world, efficient conduct of electronic business, and the capability of law enforcement.

Cryptographic technology, which includes encryption, historically has been the purview of the defense and military establishment of the United States. A similar situation has prevailed throughout the world for centuries but there are now many stakeholders, each of whom has a legitimate interest in having access to cryptography and its technology and products, in using it operationally, and including it as a discipline for academic study and research. Among the stakeholders are:

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

- The Federal government, for its own operational needs and to function in the international community.
- The defense establishment, notably for communications security and various intelligence functions.
- Law enforcement, not only for its own security needs but also for counter-intelligence actions against law-breaking organizations.
- Civil and other non-classified government, to protect its unclassified but nonetheless sensitive data.
- The international competitive position of the U.S. computer and telecommunications industry.
- Private sector corporations, to function domestically and internationally and to protect sensitive data and communications.
- Society at large, as users of telephony and other services that must assure confidentiality and privacy for communications.
- The individual citizen, as a user of personal computers and the data networks of the world with their extensive array of information services.
- The academic community, as a legitimate discipline of study and research.

Not surprisingly, the interests of all such parties overlap and are often in conflict which makes the matter an urgent concern of national policy. In view of this, the CSSPAB resolved at its March 17-18, 1992 meeting to call for a national public review of the issue. The principal resolution from our March meeting and two related ones adopted at the same time are attached to this letter.

The Board commends them to your attention and solicits your support in calling this very important national and societal issue to the transition team.

Sincerely,



Willis H. Ware  
Chairman

Attachments

NOTE: Attachments are not reproduced here as they are included in Exhibit III.

Identical letters requesting that appropriate actions be taken to identify public cryptography as a critical policy issue to the new administration through key senior career officials and the transition team members were sent to the following:

Honorable William P. Barr  
Attorney General  
10th Street & Constitution Avenue, NW  
Washington, DC 20530

Honorable Nicholas F. Brady  
Department of the Treasury  
1500 Pennsylvania Avenue, NW  
Washington, DC 20220

Honorable Richard B. Cheney  
Department of Defense  
The Pentagon  
Washington, DC 20301

Honorable Richard G. Darman  
Office of Management & Budget  
Old Executive Office Building  
17th Street & Pennsylvania Avenue, NW  
Washington, DC 20515

Honorable Lawrence S. Eagleburger  
Secretary of State  
2201 C Street, NW  
Washington, DC 20520

Honorable Robert M. Gates  
Director of Central Intelligence  
Washington, DC 20505

Honorable Brent Scowcroft  
Assistant to the President  
for National Security Affairs  
White House  
Washington, DC 20500

bcc: Dr. John W. Lyons  
Director, NIST

Vice Admiral John M. McConnell, USN  
Director, National Security Agency

Mr. James H. Burrows  
NIST  
Director, Computer Systems Laboratory





Washington, D.C. 20505

14 January 1993

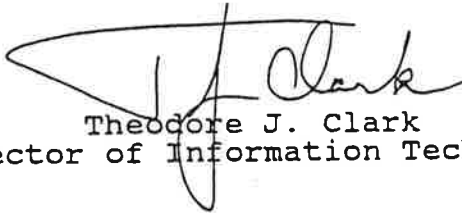
Dr. Willis H. Ware  
Chairman, The National Computer System  
Security and Privacy Advisory Board  
National Institute of Standards and Technology  
Gaithersburg, Maryland 20899

Dear Dr. Ware:

I am responding to your letter of 16 December 1992 to Mr. Gates in which you expressed concern about the issue of public cryptography. As you state, this is a complex area where the interests of various parties legitimately conflict. Should a national review be conducted on this issue, appropriate representatives from the Intelligence Community will certainly be involved.

I will give the transition team your letter as you requested. Thank you again for raising this issue to the Director and for your evident concern for the protection of the United States' interests in this area.

Sincerely,



Theodore J. Clark  
Director of Information Technology



THE NATIONAL  
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987*

January 22, 1993

Honorable Ronald H. Brown  
Secretary of Commerce  
Washington, DC 20230

Dear Mr. Secretary:

The Computer System Security and Privacy Advisory Board is directed under the Computer Security Act of 1987 to identify emerging technology and public policy issues related to information, computers and communications technology; and to bring them to the attention of national decision makers for consideration.

The Board has before it the issue of public cryptography, which has not been resolved at the national level, but has such importance and urgency that it must have high priority for the administration.

The rapid progress of communications, computer, and electronic technology in the last 40 years has created a genuine civilian and non-defense demand for cryptographic techniques and devices to protect computer data, computer systems, and other communications against unauthorized access and eavesdropping. These advances impact such diverse national concerns as international competitiveness and its consequences for trade balance and state of the economy, pivotal societal privacy issues such as those of medical patient records, national security in a rapidly changing world, efficient conduct of electronic business, and the capability of law enforcement.

Cryptographic technology, which includes encryption, historically has been the purview of the defense and military establishment of the United States. A similar situation has prevailed throughout the world for centuries but there are now many stakeholders, each of whom has a legitimate interest in having access to cryptography and its technology and products, in using it operationally, and including it as a discipline for academic study and research. Among the stakeholders are:

- The Federal government, for its own operational needs and to function in the international community.
- The defense establishment, notably for communications security and various intelligence functions.

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

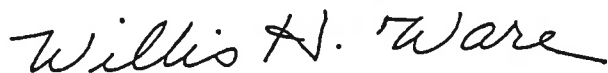
- Law enforcement, not only for its own security needs but also for counter-intelligence actions against law-breaking organizations.
- Civil and other non-classified government, to protect its unclassified but nonetheless sensitive data.
- Private sector corporations, to function domestically and internationally and to protect sensitive data and communications.
- Society at large, as users of telephony and other services that must assure confidentiality and privacy for communications.
- The individual citizen, as a user of personal computers and the data networks of the world with their extensive array of information services.
- The academic community, as a legitimate discipline of study and research.

Not surprisingly, the interests of all such parties overlap and are often in conflict which makes the matter an urgent concern of national policy. In view of this, the C SSPAB resolved at its March 17-18, 1992 meeting to call for a national public review of the issue.

Your office and possibly you, as an individual, will likely be involved with the national review that we have called for and with the establishment of a national policy on cryptography. The Board commends this crucial national and societal issue to your attention, and solicits your support in moving the matter forward.

The principal resolution from our March meeting and two related ones adopted at the same time are attached to this letter.

Sincerely,



Willis H. Ware  
Chairman

Attachments [3]

NOTE: Attachments are not reproduced here as they are included in Exhibit III.

Identical letters were sent to the following:

Honorable Les Aspin  
Department of Defense  
The Pentagon  
Washington, DC 20301

Honorable Warren Christopher  
Department of State  
2201 C Street, NW  
Washington, DC 20520

Honorable Lloyd Bentsen  
Department of Treasury  
1500 Pennsylvania Avenue, NW  
Washington, DC 20220

Mr. William S. Sessions  
Director, Federal Bureau of Investigation  
J. Edgar Hoover, FBI Building  
10th & Pennsylvania Avenue, NW  
Washington, DC 20535

Honorable Anthony Lake  
National Security Council  
White House  
Washington, DC 20500

Honorable Robert Rubin  
Director, National Economic Council  
White House  
Washington, DC 20500

Honorable Leon Panetta  
Director, Office of Management and Budget  
Old Executive Office Building  
17th Street & Pennsylvania Avenue, NW  
Washington, DC 20515

bcc: Vice Admiral John M. McConnell, USN  
Director, National Security Agency

Dr. John W. Lyons  
Director, Nist

Mr. James H. Burrows  
NIST  
Director, Computer Systems Laboratory

21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100



EX-101-1  
THE SECRETARY OF COMMERCE  
Washington, D.C. 20230

March 1, 1993

Dr. Willis H. Ware  
Chairman, Computer System Security  
and Privacy Advisory Board  
National Institute of Standards and Technology  
Gaithersburg, MD 20899

Dear Dr. Ware:

Thank you for your recent letter regarding the subject of public cryptography. As the Board notes, this matter involves the interests of many communities, including various organizations within the federal government.

The National Institute of Standards and Technology (NIST) is conducting several studies on the policy and regulatory issues which have a direct bearing on public cryptography. NIST is also examining current cryptographic product market trends as well as the current uses of cryptographic techniques to protect unclassified information within the government. When completed, this information is expected to be useful in addressing important policy decisions.

As the Department of Commerce addresses matters in this area, we will draw upon the expertise and advice of knowledgeable experts, such as those who comprise the Board. Please convey my appreciation to all the members of the Board for their continued service. I look forward to receiving additional reports from you in the future.

Sincerely,

A handwritten signature in black ink, appearing to read "Ron Brown", written over a large, stylized flourish that extends to the left and loops back under the signature.

Ronald H. Brown



United States Department of State

Washington, D.C. 20520

February 25, 1993

Mr. Willis Ware, Chairman  
The National Computer System Security and Privacy Board  
National Institute of Standards and Technology  
Technology Building, Room B154  
Gaithersburg, Maryland

Dear Mr. Chairman:

The Department of State is in receipt of your letter, dated January 22, 1993, regarding the upcoming review of the implications of public and secret key cryptography. Mr. Frederick C. Brandt, Director, Office of Information Systems Security, will be the point of contact for the Department of State on these issues. He can be reached at (202) 663-0557. If the National Computer System Security and Privacy Board requires more information, please contact Mr. Brandt.

Sincerely,

A handwritten signature in cursive script that reads "William D. Clarke".

William D. Clarke  
Deputy Assistant Secretary  
Countermeasures and  
Counterintelligence





U.S. Department of Justice  
Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

February 26, 1993

Dr. Willis H. Ware  
Chairman  
The National Computer System Security  
and Privacy Advisory Board  
National Institute of Standards and Technology  
Room B154  
Technology Building  
Gaithersburg, MD 20899

Dear Dr. Ware:

In response to your letter of January 22, 1993, the issue of public cryptography is one in which I am deeply and personally involved. I enthusiastically support public access to effective cryptographic products for protection of legitimate interests, which include both sensitive public and private corporate information and a citizen's right to privacy. I likewise believe that promotion of international competitiveness of U.S. business is of critical importance. However, as a law enforcement official I have a compelling concern that the technical capability to protect one's voice, data, and image communications through encryption not be used to thwart the laws which Congress and state legislatures have established for the protection of the public and our Nation's security. I am confident that all concerns can be accommodated in a manner which gains stakeholder support.

The most feasible forum for productively collecting input from stakeholders holding diverse views, examining and analyzing the issues, and developing candidate alternatives is a matter on which I expect to obtain guidance from the new Administration. The proactive posture of your Board is appreciated.

Sincerely yours,

William S. Sessions  
Director

THE WHITE HOUSE  
WASHINGTON

February 10, 1993

Mr. Willis H. Ware  
Chairman  
The National Computer System Security  
and Privacy Advisory Board  
National Institute of Standards  
and Technology  
Technology Building, Room B154  
Gaithersburg, MD 20899

Dear Mr. Ware:

Thank you for sending me the resolutions from your March 17-18, 1992 meeting.

I appreciate your sharing this with me, and please feel free to send me any additional background material.

Sincerely,



Robert E. Rubin

## IV. 1993 Advisory Board Workplan

### **I. INTRODUCTION**

This section sets forth the proposed 1993 work plan for the Computer System Security and Privacy Advisory Board (CSSPAB). This document, approved by the Advisory Board, is intended to be used as a planning guide for the Board's 1993 activities. The Board recognizes that other subjects not previously identified in this planning document may arise during 1993. The Board reserves the right to address any matter that pertains to its fundamental missions and may modify its program plan to meet evolving situations and changing priorities.

### **II. APPROVED 1993 WORK ITEMS FOR CSSPAB**

A. Action Items. The Board will examine the following topics during its 1993 program year:

A.1. National Review of Cryptography. In March 1992, the Board recommended a national level review of the use of cryptography for protecting unclassified information. In its June and September meetings, the Board heard commentary on issues surrounding the national review. The Board will continue to follow this important issue in 1993 with emphasis on the impact that the Data Encryption Standard (DES) revalidation decision, the recent Software Publishers' Association/U.S. Government agreement, and the Digital Signature Standard (DSS) will have on this review. In conjunction with this item, the Board will pursue these related topics:

A.1.a. Data Encryption Standard Revalidation. The DES will come up for revalidation in early 1993. The Board may be the only public forum, outside of the Congress, where this matter can be discussed in a dispassionate manner by knowledgeable individuals from the public and private sectors. The Board will review developments in this subject area.

A.1.b. Public Key Cryptography. The Board will continue to review the progress in developing a Digital Signature Standard for use by the unclassified segment of the Federal Government. Of equal importance will be an examination of the infrastructure issues related to the use of public key cryptography by Federal agencies. Regardless of the algorithm to be selected as the basis for the standard, it is important that critical policy and technical alternatives be identified for managing the issuance and distribution of certificates. Which organizational entities of the Government should have operational responsibilities for the infrastructure?

**A.1.c. Telecommunications Security.** Law enforcement and national security interests have advocated legislation that might place limits on the security of the communications facilities available to the public. The Board will review the implications of current proposals for the security and privacy of computer and communications systems available to civil Government and the private sector.

**A.2. Trusted System Criteria and Evaluation.** The Board has followed the development of Federal Computer Security Evaluation Criteria during 1992. This criteria, expected to become available in early 1993, will play a critical role in the evolution of trusted system technology in the U. S. and internationally. The Board will closely follow developments with the Federal Criteria, their relationship with the DoD Trusted Computer System Evaluation Criteria (TCSEC), and the mechanisms being evolved for the conduct of evaluations in the U.S. The following specific topic areas will be covered:

**A.2.a. Computer Security Guidelines and Standards.** The Board will monitor the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) plans and programs for the international harmonization of computer security requirements as well as their experiences and plans for guidelines, standards, and interpretations. The Board will pay particular attention to the execution of the NIST/NSA Work Plan on Trusted System Technology.

**A.2.b. Security Evaluation Process.** The Draft NIST/NSA Work Plan on Trusted System Technology identifies the possibility of NSA focusing on the higher levels of trust with NIST participation (B2 and above) and NIST focusing on the lower levels of trust with NSA participation (C2 and B1), perhaps using the mechanisms of the National Voluntary Laboratory Accreditation Program (NVLAP). This suggestion may help increase the availability and timeliness of evaluated products at all levels by focusing attention and increasing resources available to specific areas. The Board will review the possibilities of this development through discussions and briefings from the NSA, the NIST, and civilian and defense organizations that would be affected by this new arrangement. One model for such an evaluation program might be the FIPS 140-1 cryptographic module product evaluation process. The Board will review this evolving process as part of its overall examination.

**A.3. Privacy.** There is a continued interest in privacy issues in the public press with mixed signals coming from the general public, showing concern for privacy but unwillingness to pay for protection or be inconvenienced. The Board should review the measures that are needed or being taken by the Government to protect privacy in Federal programs and issue recommendations on what NIST and others should be doing to encourage protection of individual privacy. Specific briefings from agencies involved in handling personal information

should be scheduled early in the year. The scope of this activity will also include monitoring developments in European privacy regulations to assess their potential impact upon U.S. entities.

**A.4. Changes in National Computer Security Policies.** The Board will continue to receive written updates and briefings from the Executive Secretary on any pending or proposed changes in national computer security policies. This area will include the revision to Appendix III, Office of Management and Budget (OMB) Circular A-130, which the Board recognizes as a critical component in the foundation of security policy foundation for the Government's unclassified systems.

**A.5. Implementation of the Computer Security Act.** Subsumed under this heading are the various related issues the Board would like to address in 1993 including the role of the Inspectors General in computer security, and computer security training and its effectiveness. The Board will review the current status of OMB/NIST/NSA agency security planning visits and plans for follow-up activities.

**A.5.1. Risk and Threat Assessment.** The Board will review the state of risk management practices in the Federal Government, and make recommendations on the process by which agencies evaluate their threat, vulnerability, and risk posture in the process of devising cost-effective programs of security measures. The Board will review the status of FIPS Publication 65, Guideline for ADP Risk Analysis, and of agencies' application of this guideline. The Board will review the product of the DCI Threat IV study, and consider the extent of its relevance and availability to civil agencies. The Board will develop recommendations on the availability of threat data to civil agencies and on their use of threat and vulnerability data to perform risk analysis and develop security programs.

**A.5.2. Electronic Data Interchange (EDI) Security.** Many Federal agencies are about to launch ambitious automation programs that will make extensive use of EDI technology. There are significant security policy and technical issues that must be addressed to assure that the use of EDI complies with the spirit and intent of the Computer Security Act and other existing computer security Government directives. The Board will address this issue both from a policy and technology perspective.

**A.6. The National Computer Security Conference.** NIST and NSA have for over ten years jointly sponsored this major conference that brings together users, suppliers, and evaluators of computer security. The Board will review the status of the conference and the extent to which it serves the needs of the unclassified community and the civil agencies of Government. The Board will make recommendations as appropriate.

**B. Monitoring Activities.** The Board has expressed a desire to maintain a continuing interest in various critical issues. The Board may choose to exercise its statutory reporting responsibilities if it believes that a specific issue has become sufficiently important to warrant such action.

**B.1. Security and Open Systems.** A major segment of the NIST Computer Systems Laboratory program is directed to achieving the concept of open systems. The Board will review the current status of security within the open systems context and seek to identify any critical areas where security issues may impede the full utilization of open systems. One frequently voiced problem area involves the lack of an adequate public key based cryptographic key distribution standard. Is this a valid concern and are there other security gaps that need to be addressed by NIST and other standards entities?

**B.2. Effective 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, training, etc., are needed on how to use basic security tools and features designed into existing products.

**B.3. Status of Computer Emergency Response Capabilities in Civil Agencies.** The Board has heard from several sectors of the U.S. Government that have organized highly effective emergency response teams and centers. How well prepared are other agencies such as HHS, HUD, etc., to handle computer emergencies? Is there a requirement for such agencies to establish such a capability? Periodic briefings on the use of a Computer Security Incident Response Capability (CSIRC) 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?

**B.4. International Hacking.** Cases of international hacking such as those that Cliff Stoll documented seem to keep occurring. 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? Also, 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?).

**B.5. Local Area Network (LAN) Security.** Federal agencies are experiencing significant security problems with the utilization of LAN technology. The pace of the installation of this technology, combined with the security exposures resulting from the use of LANs, has created a new level of risk for Federal information systems. Another aspect of this issue will be the potential explosive growth in the installation of wireless LAN technology over the next few years. The Board will examine the LAN issue to determine what can be accomplished to improve the security of installed LANs and what research, policy, and/or other initiatives must be undertaken to effect a long term improvement in LAN security.

**B.6. Information Security Foundation.** The Board will monitor developments in this area and offer appropriate comments/guidance as needed.

**B.7. 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.

**B.8. Citizen Access to Government Electronic Records.** There is considerable discussion underway concerning this issue. A legislative proposal, S. 1940, "Electronic Freedom of Information Improvement Act of 1991," was recently introduced for Congressional consideration. The Board will examine the information system security and related privacy issues inherent in this important public policy debate.

## **V. Conclusions**

During 1992, the Board focused on the important issues which will affect the state of computer security in the years ahead, in particular, the strength and availability of cryptographic products and standards as well as international harmonized trusted system standards.

The Board issued letters to appropriate Executive Branch officials and, to date, has received numerous responses supporting the national review effort. In September 1992, the Board called together a number of hardware/software vendors, cryptographic product vendors, public advocacy groups and stakeholders/users to identify and recommend issues which NIST should ensure are covered in the review and to recommend an approach to conducting the review.

**The federal criteria effort between NIST and NSA was also of continued interest to the Board this year. Some Board members noted the need for a broad cross section of users to participate in the development and review process of the federal trusted criteria document. While the Board took no universal position, some individual members expressed views somewhat skeptical of the overall project's goals and objectives.**

**The Board has continued to monitor the agency visit program by OMB/NIST/NSA and sent a letter to the Director of OMB noting particularly, the enthusiastic reactions of agency participants that visits to their agencies have resulted in greater awareness of computer security issues on the part of senior officials in their organizations.**

**The Board also developed its work plan and priorities for 1993. 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 their priorities on these important computer security issues. 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 computer security challenges of the 1990s.**