1993 Annual Report

# of the

National Computer System Security

and

Privacy Advisory Board

March 1994

Executive Summary

This Annual Report documents the activities of the National Computer System Security and Privacy Advisory Board during 1993, its fifth 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 and privacy issues. Dr. Willis Ware, of RAND, has served as Chairman of the Board since July of 1989.

In 1992, the Board identified the need and called for a National Review of Cryptographic Policies and 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. However, in May of 1993, the President directed that the Administration conduct a review of issues related to public cryptography and advanced telecommunications systems to include: individual privacy, exportability, key escrow systems, industry requirements for information protection, to the government-developed "key escrow" chip, and related issues. Of particular interest was the impact upon industry of government cryptographic policies. As a result of the President's directive, Mr. Raymond Kammer, Deputy Director of NIST, requested the Board to devote its June meeting to collecting public comments from these outside communities for input to the Administration's deliberations. The cryptographic review was intended to track trends in telecommunication and encryption technologies, study export control issues, and examine the policy and implementation of the key escrow encryption initiative.

Subsequently, the Board devoted a special July meeting, and a limited amount of time at the September meeting, to the same subject to more completely respond to Mr. Kammer's request and to fulfill its statutory obligations under P.L. 100-235. The Board continues to monitor issues surrounding cryptography.

As a result of these meetings four resolutions (of cryptographic concern) were passed by the Board:

- The input collected reflected serious concerns regarding the key escrow initiative and that more time was needed to achieve a better understanding of the issues.

- The Board recognized that key escrowing encryption technology represented a dramatic change in the nation's information infrastructure. Therefore, the Board recommended that key escrowing encryption technology not be deployed beyond current implementations planned within the Executive Branch, until its significant public policy and technical issues are fully understood.

- Public input heightened the concerns of the Board to many issues, such as: 1) the kinds of problems that the key escrow encryption initiative attempts to solve, 2) the need to review export and import controls over cryptographic products, and 3) the key escrow encryption initiative and DoD Capstone technology proposals not addressing the needs of the software industry, and several others.

- The Board endorsed the process pursued by the Administration in the form of an interagency review but believed that the scope of that review needed to include adequate industry input. The Board believed that there were a number of issues that must be resolved before any new or additional cryptographic solutions are approved as U.S. government standards. Those issues were:

1) The protection of law enforcement and national security interests;

2) The protection of U.S. computer and telecommunication interests in the international marketplace; and

3) The protection of U.S. persons' interests both domestically and internationally.

In other discussions, the Board was briefed on the Clinton Administration's announcement of its intention to use the High Performance Computing and Communications as a foundation for developing a National Information Infrastructure (NII). The plan would be to draw upon a wide variety of private sector groups discussing issues associated with the NII.

In July, the Board endorsed the recertification of the Data Encryption Standard (DES) algorithm for an additional five year period, from 1993 through 1998. The Board recommended endorsement of DES for use in software versions that can be used to protect information covered by the Computer Security Act of 1987.

During the December meeting, the Board endorsed NIST's computer security plan for FY94 as a reasonable allocation of its limited resources for their computer security program.

The Board also established a work plan for 1994 which identified candidate topics for in-depth examination. These include:

- Cryptographic Issues;

    - Public Key Cryptography;
    - National Research Council Study
    - Telecommunications Security

- Council on National Information Infrastructure;

- Trusted System Criteria and Evaluation;

- Security Evaluation Process;
- Privacy;
- Implementation of the Computer Security Act; and
  - Risk and Threat Assessment
  - Electronic Commerce (EC) Security
- Monitoring Activities;
  - Changes in National Computer Security Policies
  - 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
  - Security and the Public Switched Network
  - Citizen Access to Government Electronic Records

These issues clearly demonstrate the extensive work which lies ahead for the Board in 1994 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) 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), 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. As of December 1993, the membership of the Board is as follows:

- <u>Chairman</u>
  Willis H. Ware, RAND

- <u>Federal Members</u>
  Patrick R. Gallagher, National Security Agency
  Henry H. Philcox, Department of the Treasury, Internal Revenue Service
  Cynthia C. Rand, Department of Transportation

- <u>Non-Federal, Non-Vendor</u>
  Cris R. Castro, ManTech, Inc.
  John A. Kuyers, Ernst and Young
  Sandra Lambert, Citibank

- <u>Non-Federal</u>
  Gaetano Gangemi, Wang Laboratories, Inc.
  Stephen T. Walker, Trusted Information Systems, Inc.
  Bill Whitehurst, International Business Machines Corp.

In September of 1993, Messrs. Colvin, Zeitler, and Lipner's terms expired, leaving three vacancies in the following categories: federal, non-federal, non-vendor, and computer or telecommunications industry.

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 1993. Additionally, the Board accomplishes much informal, non-decisional, background discussion and preparation for meetings by electronic mail between meetings. The Board's activities complement those of the individual Board members. (Note that the minutes and agenda from the June, July, 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.)

Much of the substantive work of the Board during 1993 was devoted to collecting public comments on the subject of the Administration's key escrow encryption technology. The Board collected input from a wide range of individuals and groups representing industry, academia, privacy rights advocates, and private citizens.

Key Escrow and Public Use of Cryptography

The focus of the June meeting was on the "key escrow" encryption chip, and more broadly, the public use of cryptography and government cryptographic policies and regulations. On April 16, 1993 the President announced the development of a state-of-the-art microcircuit called the key escrow encryption chip (commonly referred to as the "Clipper" chip.) (The use of the term "Clipper" has been discontinued to avoid any potential conflict with similarly named products.) This initiative is intended to bring the federal government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement. The chip scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today. A "key-escrow" system will be established to ensure that the key escrow encryption chip is used to protect the privacy of law-abiding Americans while preserving the ability of approved agencies to gain access to the keys when legally authorized.

In June, Mr. Ray Kammer, Deputy Director of NIST,2 briefed the Board on the status of the panel of cryptographers who had been invited to evaluate the SKIPJACK algorithm used in the key escrow encryption chip. Mr. Kammer informed the Board that the President had directed the National Security Council to lead the study group considering the key escrow and cryptography issues.

Mr. Clint Brooks, Advisor to the director of NSA, discussed their role in the development of the key escrow encryption chip, NSA had two goals in mind: 1) to provide high quality cryptographic protection to U.S. federal government agencies and those organizations and individuals in the private sector that voluntarily wish to take advantage of it and 2) to provide a mechanism for lawful access to the encrypted information when lawfully authorized (e.g., if this powerful technology is misused to hide criminal activity).

Many issues were derived from the development of the key escrow initiative. Private citizens expressed their views concerning the inadequate time that had been allotted to understanding the issues involved and that the Constitutional issues had not been adequately examined. They were concerned that the relationship of the escrow agents to the government was unclear and questioned how independent the escrow agents would be. Some of the following concerns, with regard to cryptography, and key escrowing/technology, were expressed by a number of panelists:

- export controls on cryptography;
- no legal or policy basis for the key escrow encryption initiative;
- the key escrow encryption initiative effectiveness is unclear with regard to law enforcement;
- the key escrow encryption initiative threatens existing, individual rights to privacy;
- the government banning of non-escrowed encryption;
- possible misuse or compromise of escrowed key components through abuse of political power or bribery;
- the algorithm not being implemented in software; and
- probable rejection of the key escrow encryption initiative by foreign markets. (because it is classified)

The issue of privacy was also discussed. Some of the concerns were the presence of "information brokers" who sell information from government databases to the private sector, the disclosure of secret files on individuals, and the abuse of social security numbers. International issues regarding wiretapping involving eavesdropping of politicians was also a concern. One private sector organization concluded that the key escrow system will not work unless it is mandatory and believes the government will seek to legislate its use. (The government has repeatedly stated however, that it has no intention of seeking such legislation.)

Export Control

Export issues were also examined from a business perspective. Several panel members expressed that current U.S. export laws do not make sense given the claimed widespread foreign availability of cryptographic products. They related that software companies have suffered economic losses, and difficulties with joint ventures as a result.

The July meeting was a continuation of the June meeting devoted to collecting public comment on the key escrow encryption initiative. The Board had two tasks in this regard: 1) to provide a record of the public comments it received and 2) to deliver its own input, if desired.

SKIPJACK Algorithm

In order to allow those in the private sector to ascertain for themselves the strength of the SKIPJACK algorithm, the government made the algorithm available to a group of independent cryptographers (under appropriate security conditions). Dr. Dorothy Denning, Georgetown University, was one of the reviewers of the SKIPJACK algorithm. Dr. Denning provided the Board with a status report and the following conclusions: 1) There is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years. 2) There is no significant risk that SKIPJACK can be broken through a shortcut method of attack. 3) While the internal structure of SKIPJACK must be classified in order to protect law enforcement and national security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm. Dr. Denning said that the reviewers plan to evaluate the entire key escrow system once final details become available.

Key Escrow Agents

The Department of Justice reported on the outline of the criteria the Attorney General will use when naming escrow agents. The escrow agents would be U.S. government agencies that posses the following attributes: 1) credibility with the public, 2) the ability to handle sensitive information, and 3) the ability to respond rapidly in an emergency situation. Key generation will be done at a secure facility and, for extra security, the key components will be encrypted prior to providing them to the escrow agents.

Law Enforcement Requirements

A panel of representatives of law enforcement presented their requirements for wire surveillance to the Board. They outlined the limited circumstances where a wiretap is used and the procedures involved in authorizing one. They endorsed the key escrow initiative because it provides the public with strong encryption to protect information, but allows law enforcement access when legally authorized.

User Community

Some members of the user community expressed their support for key escrow technology provided that the following issues be resolved:

Vendors must be able to implement key escrow mechanisms;

Export controls must be addressed;

The government should take the lead in establishing interoperability standards;

Key escrow data must remain under the control of the U.S. government;

The integration of key escrow in foreign markets; and

Administrative costs need to addressed.

Escrow Encryption Standard/Escrow Procedures

There was continued discussion of cryptographic issues during the September meeting. The Federal Information Processing Standard for an Escrowed Encryption Standard (EES) was discussed. The proposed standard specifies use of a symmetric-key encryption/decryption algorithm and a key escrowing method which are to be implemented in electronic devices and used for protecting certain unclassified government communications when such protection is required.

The Department of Justice reported that the key escrow procedures are being developed and, when completed, will be publicly announced and put in the public domain. As of December 1993, The Department had not announced the selection of the key escrow agents.

Federal Criteria and Evaluation Program

The Board received a status report from Ms. Janet Cugini, Computer Security Division, NIST, on the Federal Criteria and Evaluation Program. NIST held a two-day workshop and Ms. Cugini related that there was a clear agreement among the participants that the document was severely deficient by not addressing distributed systems, networks, encryption, and PC security. The draft Federal Criteria document will become input to the new Common Criteria along with the Canadian Criteria and the ITSEC.

Information Brokering

The Social Security Administration (SSA) provided the Board with a video, developed in-house, documenting actual information brokering in SSA. The video presents actual SSA personnel going through the procedures for access control which led them to the brokering of SSA information by an SSA employee to an outside entity.

National Information Infrastructure

The Board was presented a view of the emerging National Information Infrastructure (NII) in the context of the ongoing Federal High Performance Computing and Communications (HPCC) program. The Administration announced its intention to use the HPCC as a foundation for developing a National Information Infrastructure drawing upon the wide variety of private sector groups discussing issues associated with the NII. The Board will study this activity.

Cryptographic Wrap-Up

The December meeting was intended as a wrap-up of cryptographic issues. The Board was presented the initial plans for a study by the National Research Council of the National Academy of Sciences, as mandated by Congress, on cryptographic technologies and national cryptography policy. The purpose of the study is to assess the effect of cryptographic technologies on:

- national security and law enforcement interests of the U.S. government;
- commercial interests of U.S. industry; and
- interests of U.S. industry of export controls on cryptographic technologies.

NIST's Security Program Plan

The Board examined NIST's Security Program Plan. Some of the major areas of the program include:

- cryptography and authentication;
- network security;
- security management;
- criteria and evaluation; and
- electronic commerce.

Threats to Telecommunications Security

The Board received a report on threats to telecommunications security from Mr. Rick Kuhn of NIST's Computer Systems Laboratory. Mr. Kuhn reported that typically, traditional and non-traditional threats cause significant government and industry concerns. Today's telecommunications environment of open network architecture means much grater access to the Public Switched Network (PSN); therefore, the PSN must be secure from accidental or malicious cause.

III. Advisory Board Correspondence

During 1993, the Board issued three letters: 1) to the Director, National Economic Council with regards to the economic aspects of federal cryptographic policies and standards upon American competitiveness, 2) the Acting Chief Counsel for Technology, NIST on the NIST-proposed patent agreement with Public Key Partners, and 3) the Deputy Director, NIST regarding his request to collect public comments on key escrow encryption.

Exhibits

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

Exhibit I — Answer from Jane L. Sullivan, Acting Deputy Assistant Secretary for Information Systems, Department of Treasury for Secretary Bentsen, concerning efforts to develop national policies for using public key cryptography.

Exhibit II — Letter dated, March 12, 1993, from Chairman Ware to the Honorable Robert E. Rubin, regarding the economic aspects of federal cryptographic policies and standards upon American competitiveness.

Exhibit III — Answer from Robert E. Rubin, thanking the Board for sending articles about the economic aspects of federal cryptographic policies and standards.

Exhibit IV — Letter dated, August 4, 1993, from Chairman Ware to Mr. Michael R. Rubin, regarding the terms of the NIST-proposed patent agreement with Public Key Partners.

Exhibit V — Letter dated, August 24, 1993, from Chairman Ware to Mr. Raymond G. Kammer, regarding the Board's June meeting being devoted to collecting public comments on the subject of the Administration's key escrow encryption technology.

EXHIBIT I

DEPARTMENT OF THE TREASURY
WASHINGTON

February 9, 1993

Mr. Willis H. Ware
Chairman, National Computer System Security and
  Privacy Advisory Board (NCSSPAB)
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

Dear Mr. Ware:

I am responding to your letter dated, January 22, 1993, to Secretary Bentsen concerning efforts to develop national policies for using public key cryptography.

The Treasury Department supports the need for a national examination of the issues raised in your letter.

The technologies associated with public cryptography and digital signatures will enable the evolution of many strategic telecommunications programs in the government and the private sector. Many applications being planned for electronic commerce, electronic tax filing, and law enforcement will be supported by the Treasury Communications System (TCS) and will rely on cryptography for privacy and authentication.

As you are aware, the Chief Information Officer, Internal Revenue Service, is a member of the NCSSPAB and has worked closely with Treasury Officials from my office and the Office of Security over the past few years on these issues.

If you need additional information or have questions regarding Treasury policy regarding cryptography please contact Richard P. Riley, Director of Security. If you need additional information on Treasury's plans to implement public key cryptography to support telecommunication requirements please contact Jim Flyzik, Director Office of Telecommunications Management.

Sincerely,

Jane L. Sullivan

Jane L. Sullivan
Acting Deputy Assistant Secretary
  for Information Systems

EXHIBIT II

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

March 12, 1993

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

Dear Mr. Rubin:

Thank you for your recent letter. As you requested, please find enclosed recent articles regarding the economic aspects of federal cryptographic policies and standards upon American competitiveness. These articles provide a broad perspective of the private sector views on federal cryptographic standards activities. Among other multi-national businesses, the U.S. software industry, with sales of $100 billion per year, has stated that federal cryptographic policies are restraining their ability to ship products to the export market which represents approximately half their customer base.

Currently, little quantitative data exists to document the economic impacts upon American industry of federal cryptographic activities. Despite the lack of hard figures, there are significant economic and societal consequences of this issue. You may wish to request the Department of Commerce to gather such information.

In addition to loss of international market share, there is also a need to consider the economic impacts of federal cryptographic policies and standards on American competitiveness. Federal policies will affect the ability of American industry to remain on the cutting edge of technology in order to compete effectively in world markets.

Also, U.S. business is increasingly reliant upon cryptography to protect itself against industrial espionage, much of which is sponsored by the intelligence services of friendly governments.

For example, many of the corporations comprising the State Department's Overseas Security Advisory Committee have lost sensitive information to active foreign intelligence efforts. While the interests of the law enforcement and intelligence communities have been adequately expressed and are even almost automatically understood, American business must also be allowed to present their legitimate concerns to the Administration.

Please let me know if I may be of further assistance.

Sincerely,

Willis H. Ware

Willis H. Ware, PhD
Chairman

Enclosures

EXHIBIT III

THE WHITE HOUSE

WASHINGTON

March 23, 1993

Willis H. Ware, Ph.D.
Chairman
The National Computer System Security
and Privacy Advisory Board
Technology Building
Room B154
Gaithersburg, MD 20899

Dear Dr. Ware:

Many thanks for sending me the articles about the economic aspects of federal cryptographic policies and standards.

I appreciate the follow-up.

Sincerely,

Robert E. Rubin
Assistant to the President
for Economic Policy

EXHIBIT IV

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

August 4, 1993

Mr. Michael R. Rubin
Acting Chief Counsel for Technology
National Institute of Standards and Technology
Gaithersburg, MD   20899

Dear Mr. Rubin:

As provided under the Computer Security Act of 1987 [PL 100-235], the Computer System Security and Privacy Board finds that the terms of the NIST-proposed patent agreement with Public Key Partners [PKP], as announced in the Federal Register, may have latent consequences that would be negative for the country and the general public. The Board conveys the attached resolution to you as a formal response to the request for comment as provided in the announcement.

The basis of our resolution is that we have been told that no economic analysis of the proposed exclusive license to PKP has been performed. Hence, the financial impact of the proposed license may have possible and major negative effects on the country and the widespread use of a public-key digital signature standard. The resolution, which was adopted by a 9-1 vote, reflects our concern that the proposed settlement may not be in the joint best interests of the government and the public.

Sincerely,

Willis H. Ware

Willis H. Ware, PhD
Chairman

Attachment

cc: Ray Kammer

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION #93-4

JULY 30, 1993

The Board is concerned that:

1. The original goal that the Digital Signature Standard would be available to the public on a royalty free basis has been lost; and

2. The economic consequences for the country have not been addressed in arriving at the Digital Signature Algorithm exclusive licensing arrangement with Public Key Partners, Inc.

FOR:	Castro, Colvin, Kuyers, Lambert, Lipner, Philcox, Walker, Whitehurst, Zeitler
AGAINST:	Gallagher
ABSTAIN:	none
ABSENT:	Gangemi, Rand

EXHIBIT V

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

August 24, 1993

Mr. Raymond G. Kammer
Deputy Director
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dear Mr. Kammer:

At your request, the Computer System Security and Privacy Board devoted its June meeting to collecting public comments on the subject of the Administration's key escrow encryption technology as well as broader issues of cryptographic policy. In all, we heard two days of public statements and received 58 written submissions from a wide range of individuals and groups representing industry, academia, privacy rights advocates, and private citizens. The statements, along with a document summarizing the major issues, are enclosed in this package.

I hope this satisfies your objective in seeking the Board's assistance. If we can be of any further assistance in the cryptographic policy review, please do not hesitate to contact us.

Sincerely,

Willis H. Ware

Willis H. Ware, PhD
Chairman

Enclosures

cc: Director, OMB
Director, NSA
George Tenet, NSC

IV. 1994 Advisory Board Workplan

I. INTRODUCTION

This section sets forth the proposed 1994 work plan for the Computer System Security and Privacy Advisory Board (CSSPAB). This document, to be approved by the Advisory Board, is intended to be used as a planning guide for the Board's 1994 activities. The Board recognizes that other subjects not previously identified in this planning document may arise during 1994. 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 1994 WORK ITEMS FOR CSSPAB

A.Action Items. The Board will examine the following topics during its 1994 program year:

A.1.Cryptographic Issues. In March 1992, the Board recommended a national level review of the use of cryptography for protecting unclassified information. During 1993 the Board devoted a large part of its efforts collecting public comment on the Administration's key escrow encryption initiative. The Board will continue to follow developments surrounding this important issue in 1994 with emphasis on the impact of cryptography on the National Information Infrastructure, the evolution of key escrow concepts and procedures and the Digital Signature Standard (DSS). In conjunction with this item, the Board will pursue these related topics:

A.1.a.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.b.National Research Council has been charged in the 1994 Department of Defense Public Law 103-160 to conduct a Comprehensive Independent Study of National Cryptography Policy." The Board will track developments in this study and assist as it can in this realization of its March 1992 recommendation.

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.Council on National Information Infrastructure. The Board will work with the Advisory Council on the National Information Infrastructure (ACNII) in the area of Information Security aspects of the National Information Infrastructure. The CSSPAB will monitor the actions of the ACNII and the privacy and information security issues inherent in its development.

A.3.Trusted System Criteria and Evaluation. The Board has been following the development of Federal Computer Security Evaluation Criteria. This criteria has now been advanced as part of the U.S. input into a new Common Criteria, involving U.S., Canadian, and European interests. The Common Criteria is expected to play a major role in the evolution of trusted system technology in the U.S. and internationally. The Board will closely follow developments with the Common 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.4.Security Evaluation Process. The Draft NIST/NSA Work Plan on Trusted System Technology identifies the possibility of the NSA focusing on the higher levels of trust (B2 and above) and the NIST focusing on the lower levels of trust (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 split of responsibilities. 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.5.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.6.Implementation of the Computer Security Act. Subsumed under this heading are the various related issues the Board would like to address in 1994 including any proposed changes to the Computer Security Act of 1987, the role of the Inspectors General in

:nputer security, and computer security training and its effectiveness. The Board will ·iew the current status of OMB/NIST/NSA agency security planning visits and plans for low-up activities.

5.a.Risk and Threat Assessment. The Board will review the state of risk management ıctices in the Federal Government, and make recommendations on the process by which :ncies evaluate their threat, vulnerability, and risk posture in the process of devising t-effective programs of security measures. The Board will review the status of FIPS ɔlication 65, Guideline for ADP Risk Analysis, and of agencies' application of this deline. The Board will review the product of the DCI Threat IV study, and consider extent of its relevance and availability to civil agencies. The Board will develop ommendations on the availability of threat data to civil agencies and on their use of eat and vulnerability data to perform risk analysis and develop security programs.

5.b.Electronic Commerce (EC) Security. Many Federal agencies are about to launch bitious automation programs that will make extensive use of EC technology. There are ıificant security policy and technical issues that must be addressed to assure that the of EC complies with the spirit and intent of the Computer Security Act and other :ting computer security Government directives. The Board will address this issue both n a policy and technology perspective.

Ionitoring Activities. The Board has expressed a desire to maintain a continuing :rest in various critical issues. The Board may choose to exercise its statutory reporting ɔonsibilities if it believes that a specific issue has become sufficiently important to rant such action.

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

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

Effective Use of Security Products and Features. A study conducted by the President's ncil on Integrity and Efficiency indicated that many security functions and features : 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.4.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.5.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.6.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.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 1993, the Computer System Security and Privacy Advisory Board held meetings devoted to the "key escrow" encryption chip and the public use of cryptography and government cryptographic policies and regulations. In a response to a request from Mr. Ray Kammer, Deputy Director of NIST, the Board collected public input for the presidentially-directed review of national cryptographic policies. The Board also issued several resolutions on this issue.

The Board also developed its work plan and priorities for 1993. With regard to cryptographic issues, the Board will continue to follow developments surrounding this important issue in 1994 with emphasis on the impact of cryptography on the National Information Infrastructure. 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.