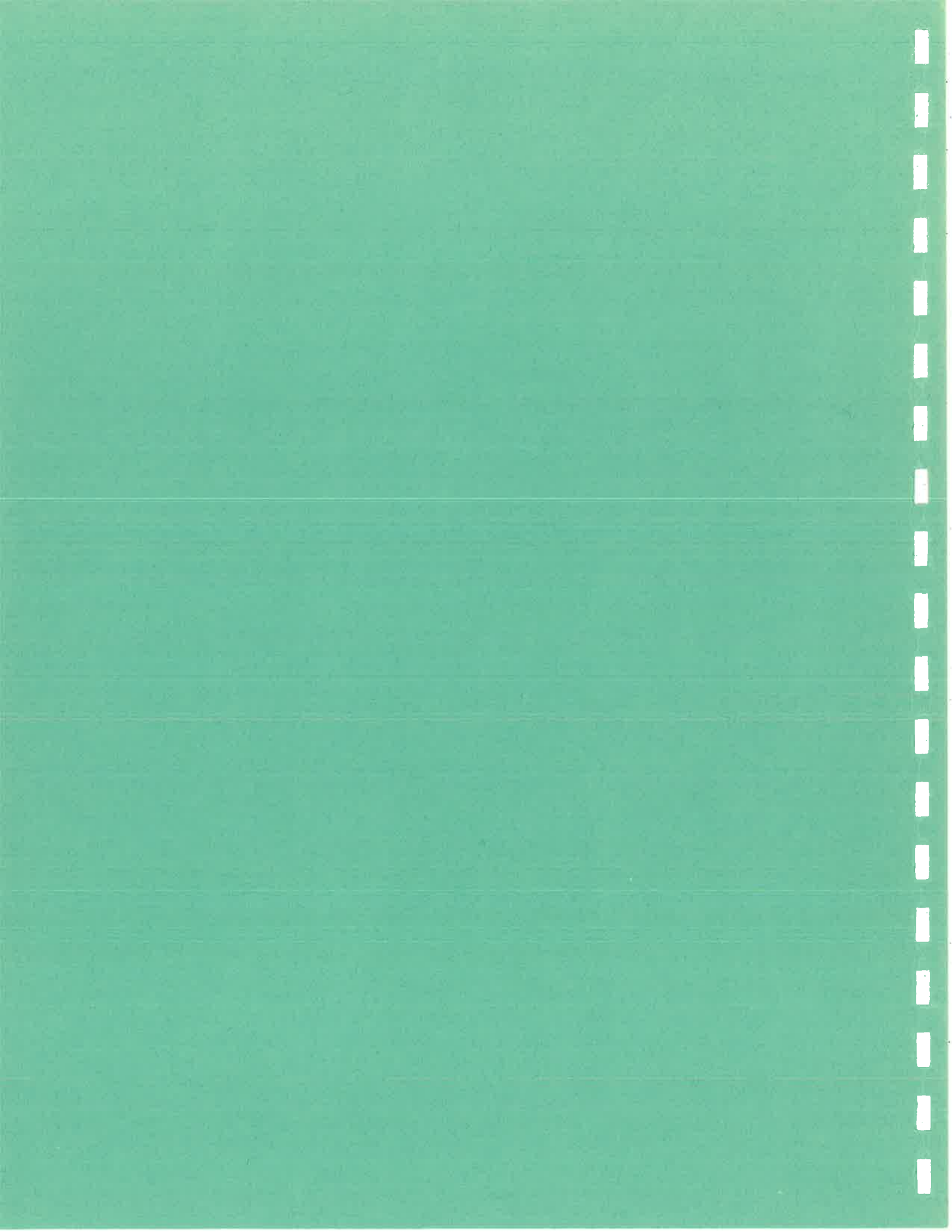


1991 ANNUAL REPORT
OF THE
NATIONAL COMPUTER SYSTEM SECURITY
AND
PRIVACY ADVISORY BOARD

MARCH 1992



Executive Summary

This Annual Report documents the activities of the National Computer System Security and Privacy Advisory Board during 1991, its third 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 formally identified four areas of emerging concern this year and has issued letters containing the Board's positions and recommendations to appropriate Executive Branch officials. These issues were:

- agency lack of compliance with the computer security requirements of OMB Circulars A-130 and A-123;
- the need for users of federal electronic mail systems to be informed of the level of privacy to be accorded their messages;
- specific program recommendations for improving NIST's Information Security Program; and
- the lack of formalized computer emergency response capabilities at federal agencies.

The Board also established a work plan for 1992 which identified candidate topics for in-depth examination. These include:

- Data Encryption Standard (DES) Revalidation;
- Public Key Cryptography;
- Citizen Access to Government Electronic Records;
- Local Area Network (LAN) Security;
- Electronic Data Interchange (EDI) Security;
- Security and Open Systems;
- Threat and Vulnerability Assessment;
- Effective Use of Security Products and Features;

- Status of Computer Emergency Response Capabilities in Civil Agencies; and
- International Hacking.

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:

- Computer Security Guidelines and Standards;
- Security Evaluation Process;
- Privacy;
- Changes in National Computer Security Policies;
- Information Security Foundation;
- Implementation of the Computer Security Act; and
- Security and the Public Switched Network.

With such a list of important topics to examine and reexamine, plus the ever growing number of relevant new issues and public policy questions, it is clear that much work lies ahead for the Board in 1992 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 on May 30, 1990 by then U.S. Department of Commerce Assistant Secretary for Administration Thomas Collamore. (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 experts from outside the federal government, one of whom is a representative of a small- or medium- size firm;
- four non-government employees who are not employed by or a representative of a producer of computer or telecommunications equipment; and
- four members from the federal government, including one from the National Security Agency of the Department of Defense.

Currently, Dr. Willis H. Ware, a senior researcher of the Corporate Research Staff of RAND, serves as Chairman of the Board. He was appointed in July 1989 following consultation with Congress which determined that it was inappropriate for a NIST official to chair the Board. As of December 1991, the full membership of the Board was as follows:

- Chairman
Willis H. Ware, RAND
- Federal Members
Bill D. Colvin, National Aeronautics and Space Administration
Patrick Gallagher, National Security Agency
Henry H. Philcox, Department of the Treasury, Internal Revenue Service
Cynthia C. Rand, Department of Transportation
- Non-federal, Non-Vendor
Chris R. Castro, SRI, Inc.
John A. Kuyers, Ernst and Young
Eddie L. Zeitler, Fidelity Security Services, Inc.
(vacancy)
- Non-federal
Gaetano Gangemi, Wang Laboratories, Inc.
Steven B. Lipner, Digital Equipment Corp.
Stephen T. Walker, Trusted Information Systems, Inc.
Lawrence L. Wills, International Business Machines Corp.

During 1991, the terms of Mr. Roger Cooper (Department of Justice), and Mr. Robert Courtney, Jr. (RCI, Inc.), expired. One vacancy remains to be filled in the Non-federal, Non-Vendor category.

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 1991. Additionally, the Board accomplishes a lot of 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 1991 was devoted to various topics related to the security of federal unclassified automated information systems. Among the most important were:

- NIST's Computer Security Program;
- OMB/NIST/NSA Computer Security Agency Visits;
- NIST's Digital Signature Standard;
- Electronic Mail Privacy; and
- Computer Emergency Response Capabilities.

NIST's Computer Security Program

During 1991, one item of continuing interest to the Board was NIST's computer security program. In March, the Board was briefed by NIST as to its plans for 1991 and beyond. The Board at that time informally noted its concerns with the scope and adequacy of the program

to meet NIST's responsibilities under the Computer Security Act. General discussion indicated that the Board believed that too much of the program is driven by externally funded taskings, drawing attention and resources away from other more important projects. The Board also noted that many projects are understaffed and, as a result, many tasks remain uncompleted and are carried over from year to year.

During the year, the Board issued a recommended program plan to NIST. The plan consolidated the NIST plan into nine items and included the Board's view of the threat environment which should drive NIST's program. (These recommendations, issued in two parts, are included in Section III.) At the December meeting, the Director of NIST's Computer Systems Laboratory, Mr. James Burrows, examined each of the Board's recommendations one at a time, and explained why they could or could not be implemented.

OMB/NIST/NSA Computer Security Agency Visits

As a followup to the computer security plan review process mandated by the Computer Security Act, officials from OMB, NIST, and NSA have been visiting senior officials at federal departments and agencies. The purpose of these visits is to discuss major agency automation efforts, the risks to the agency's mission associated with those automation plans, and the protection that the agency has acquired or is planning to by the implementation of security measures.

Senior managers are asked to report on three of the agency's most sensitive systems, including the kind of data processed by the systems, the potential threats to the systems and what measures are being taken to reduce the risks to the systems.

At the March meeting, two panels were convened to discuss these visits. The first panel consisted of representatives from OMB, NIST, and NSA who have been active participants in the visits to federal agencies to review their computer security programs in fulfilling the intent of the Computer Security Act. The panel members reported that agencies have been candid in discussing their problems and that the visits have reinforced the need for additional agency guidance, particularly in the area of networking and laptops. The visits also served to let NIST and NSA know what they could do better to help agencies meet their security requirements. The second panel of three federal agency computer security program managers agreed that the visits were a success. However, all three managers expressed their opinion that feedback from OMB was desirable.

An update of the agency visit program was presented at the June meeting. Agencies have requested guidance on issues such as security of electronic data interchange applications; application of electronic signature technology; and network security. A report on the visit process is to be prepared and completed in the Spring of 1992.

In December the Board voted to send a letter to the Director of OMB noting that the agency visit process has been a success thusfar and recommended that a summary report be prepared of the visits. The Board also urged OMB to consider how the message of the visits could be effectively delivered to major federal centers outside the Washington area.

Digital Signature Standard

In August of 1991, NIST proposed a draft Digital Signature Standard (DSS) as a Federal Information Processing Standard. This issue has been of continuing interest to the CSSPAB. The Board was afforded briefings regarding the technical specification of the standard itself as well as a summary of the comments received by NIST (through December) on the standard.

In December the Board formally expressed its grave concerns with the draft DSS and directed the Chairman to discuss the Board's concerns with the Director of NIST.

Electronic Mail Privacy

The Board initially examined the issue of electronic mail privacy and security in 1990. During 1991, the Board again considered the issue and agreed to send a letter to the Director of NIST recommending that users of federal e-mail systems be advised of the level of privacy to be accorded their messages.

Computer Emergency Response Capabilities

The ability of federal agencies to respond to computer emergencies, including virus incidents, was raised as a concern among Board members in 1991. The Board convened a panel of experts to discuss the current response system and requested that NIST contact federal agencies to determine whether most agencies had formalized response capabilities in place. Upon hearing that most did not, the Board formally recommended to OMB that it advise federal agencies of the need to properly plan and organize for computer emergencies.

III. Advisory Board Correspondence

During 1991, the Board issued letters reporting its findings on three important issues:

- material internal control weaknesses;
- privacy of electronic mail systems; and
- NIST's information security program.

Also, the Chairman prepared correspondence to the Office of Management and Budget regarding computer emergency response capabilities and the need to properly plan and organize for computer emergencies. The Board recommended that during the forthcoming revision of the security appendix to OMB Circular A-130, existing contingency planning requirements should be enhanced to include the need to plan for such computer emergencies as viruses, malicious external attacks, and other similar events.

The Board also informed the Office of Management and Budget of its view of the progress of the Computer Security Act agency visit program described in OMB Bulletin 90-08 and the positive comments from all of those involved in the visits. The Board recommended that OMB build upon the successful formula that has produced the positive results. The Board believes that the emphasis on underscoring management involvement as a fundamental prerequisite for an effective computer security program is appropriate and should be maintained in a subsequent initiative. The Board also urged OMB to consider how this message can be effectively delivered to major federal centers and activities outside of the Washington area.

Material Internal Control Weaknesses

On May 17, 1991, the Board issued a letter to the Director of OMB advising him of its unanimous approval of a proposal to address agency lack of compliance with the computer security requirements of OMB Circulars A-130 and A-123. The Board recommended that OMB require that lack of compliance with certain of these requirements be defined as "material internal control weaknesses" which should then be required to be reported to the President and OMB under the Federal Managers Financial Integrity Act.

Privacy of Electronic Mail Systems

On June 19, 1991, the Board issued a letter to the Director of NIST advising him that users of federal electronic mail systems be informed of the level of privacy to be accorded their messages. The Board recommends that NIST work with OMB to identify a suitable means of implementation. Two approaches were suggested: 1) uniform government-wide guidance or 2) agency-specific guidance to be developed by each agency. Each approach has benefits and drawbacks. Uniform regulations, by definition, would be consistent across the government,

although their implementations could vary. On the other hand, individual agency policies may be more appropriate for each agency's operating environment and constituency. Whichever approach is taken, departments and agencies should be required to inform users of the level of privacy which they can expect.

NIST's Information Security Program

The Board also issued its findings on August 22 and October 22, 1991, regarding NIST's Information Security Program. In March, NIST presented its program consisting of twenty-four items. The Board recommended its program of nine elements as appropriate to the current and near-term threat environment, with the objective of improving the level of federal computer security by focusing the NIST security program on critical areas in which results are urgently needed.

Exhibits

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

- Exhibit I Letter from Chairman Ware to Director Darman of OMB on material internal control weaknesses
- Exhibit II Letter from Chairman Ware to Director Lyons of NIST on privacy of electronic mail systems
- Exhibit III Answer from Director Lyons of NIST to Chairman Ware
- Exhibit IV Letter from Chairman Ware to Director Lyons of NIST on NIST's Information Security Program
- Exhibit V Answer from Director Lyons of NIST to Chairman Ware
- Exhibit VI A second letter from Chairman Ware to Director Lyons of NIST on NIST's Information Security Program
- Exhibit VII Letter from Chairman Ware to Director Darman of OMB on computer emergency response capabilities
- Exhibit VIII Answer from Director Darman of OMB to Chairman Ware
- Exhibit IX Letter from Chairman Ware to Director Darman of OMB on the Computer Security Act agency visit program
(Reply anticipated in 1992.)

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

MAY 17 1991

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

Dear Mr. Darman:

The Computer System Security and Privacy Advisory Board was established within the Department of Commerce by the Computer Security Act of 1987, P.L. 100-235. The charter of the Board establishes a specific objective for the Board to advise the National Institute of Standards and Technology (NIST) on security and privacy issues pertaining to federal computer systems. The Board is also to inform the Office of Management and Budget (OMB), the National Security Agency, and appropriate Congressional committees of our findings.

The purpose of this letter is to advise you of the unanimous approval of the Advisory Board of our proposal (enclosed) to address agency lack of compliance with the computer security requirements of OMB Circulars A-130 and A-123.

We recommend that:

OMB require that lack of compliance with certain of these requirements be defined as "material internal control weaknesses" which would then be required to be reported to the President and OMB under the Federal Managers Financial Integrity Act.

We feel that this procedure will significantly raise the level of compliance with established computer security requirements. Implementing the recommendation will require coordination between

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

2

NIST and OMB; however, we have already coordinated our position with NIST and OMB personnel who attended the Board meeting in March.

Thank you for your consideration of our recommendation.

Sincerely,

Willis H. Ware

Willis H. Ware
Chairman

Enclosure

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

JUN 19 1991

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

Dear Dr. Lyons:

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

The purpose of this letter is to advise you of the unanimous view of the Advisory Board that users of federal electronic mail systems be informed of the level of privacy to be accorded their messages. To accomplish this, the Board recommends that NIST work with OMB to identify a suitable means of implementation.

In the discussions with OMB, we suggest that careful consideration be given whether such guidance should be uniform across the government or developed and issued by individual departments and agencies. Each approach has benefits and drawbacks. Uniform regulations, by definition, will be consistent across the government, although their implementations may vary. On the other hand, individual agency policies may be more appropriate for each agency's operating environment and constituency. Whichever approach is taken, departments and agencies should be required to inform users of the level of privacy which they can expect.

Since computer system administrators and system programmers commonly have access to all data in the machine, the Board believes that every agency or department should establish a policy prohibiting casual reading of electronic mail by such individuals. Access to mail records should be permitted only as required by emergency or system failure circumstances.

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

On the other hand, management personnel can also have access to the mail of others, and it is not clear what the appropriate policy should be. Each agency and department must examine this aspect with regard to its own management attitudes and philosophy, and establish an appropriate policy.

Without a full understanding of the legal and regulatory environment which may apply, (e.g., the Freedom of Information Act), the Board cannot take a position as to what level of privacy should or can be, only that it be developed and users fully informed. However, we observe that much e-mail traffic is in the nature of interoffice mail and as such is related to the business of the organization. In this case, the individual sending or receiving electronic messages should have no expectation of privacy unless the organization has taken specific steps to assure it.

In addition to our concern for the privacy of electronic mail, we believe federal agencies should also address its security aspects. In particular, the positive authentication of message originators and the confidentiality of electronic messages while in transit and in computer systems are major concerns. Security technology is already available which agencies should be encouraged to utilize now. An important new capability will be the digital signature standard which NIST intends to propose shortly and which will address the user authentication matter.

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

Sincerely,

Willis H. Ware

Willis H. Ware
Chairman



NIST

Exhibit III
UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

JUN 26 1991

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

Dear Willis,

Thank you for your letter from the Advisory Board on the subject of the security of electronic mail. I, as a user, am keenly aware of the problem and am grateful to you for pointing out that we should do something about this.

Please be assured we shall address this matter.

Sincerely,
ORIGINAL SIGNED BY
JOHN W. LYONS

John W. Lyons
Director

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

AUG 22 1991

Established by the Computer Security Act of 1987

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

Dear Dr. Lyons:

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

The purpose of this letter is to provide you with the Advisory Board's recommendations (enclosed) for improving NIST's Information Security Program. Our proposal begins with a discussion of the current and near-term threat environment, thereby providing the context for the plan which follows. In contrast to the twenty-four items in NIST's program (as presented to us in March), our recommended program has nine elements. The Board believes that these nine items can contribute in a very significant way toward improving the level of federal computer security by focusing the NIST security program on critical areas in which results are urgently needed.

You should be aware that we have already discussed our recommendations with Mr. James Burrows at our meeting in June. He indicated that NIST would be prepared to respond to our proposals at the September Advisory Board meeting.

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

Sincerely,

Willis H. Ware

Willis H. Ware
Chairman

Enclosure

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

A PROPOSED NIST INFORMATION SECURITY PROGRAM

INTRODUCTION

The following material is a plan devised by the Advisory Board for presentation to NIST as the Board's suggestions for improving the NIST information security program.

This plan does not have the highly detailed structure which NIST brought to the March CSSPAB meeting, nor is that necessary for the immediate purpose of presenting a wholly different plan. The current NIST program has twenty-four line items. The one proposed here has nine. These nine items are not consolidations of the twenty-four. They are nine discrete items which can contribute in a very meaningful way to the safety of our rapidly increasing dependence on computer-based systems.

Throughout this document, the word security, without modifiers, should be read to mean information security.

THE CURRENT AND NEAR-TERM THREAT ENVIRONMENT

In support of the recommendation of a specific NIST information security program, it is necessary to describe the security environment on which recommendations are based. The quite diverse array of experience encompassed by the members of the CSSPAB permits the board to describe a threat environment on which NIST can safely base its security program provided only that it maintain an awareness of any emerging and unanticipated problems.

The CSSPAB believes the following statements to accurately describe the the general threat environment and related considerations on which NIST should base its security program.

1. The Absence of Significant Discontinuities in the Threat Environment.- Over the past twenty years and continuing until today, the distribution of loss to computer security incidents among several general categories has remained fairly constant. There have been no major and abrupt changes wholly out of keeping with long term, clearly discernible trends.

The most significant changes in the threat complement have been viruses, attacks on the public switched networks, and opportunities for harm presented by a worldwide Internet spanning multiple countries and organizations. None of these relatively new problems have generated losses exceeding 1% of the total cost of our security-related losses in the information systems environment. The inclusion of the security losses associated with LANs will still not top the 1% mark. (The source of the data supporting the 1% figure is described later in paragraph 3.)

It is doubtful that viruses would be a meaningful problem had the microcomputer not been introduced. The penetrations into the public switched networks are directly attributable to the broadly-based assimilation of computer-based switches into those networks. These two instances and the problems posed by the Internet are but the most recent of a long series of security problems that have been encountered because we failed to consider carefully the security implications of many advances in data processing technology before putting them to use without adequate safeguards.

In general, threats do not create vulnerabilities. The inverse is more commonly true. We build into our systems vulnerabilities to avarice, malice, carelessness, loyalties to other countries or organizations of persons with access to our systems, poorly trained and poorly motivated employees, technical show-offs, and irresponsibly directed curiosity. Those unfortunate characteristics of human nature, coupled with vulnerabilities to fires, floods, earthquakes, equipment failure and the many other similar and unfortunate things which can happen, are the origin of most security problems. Thus, more often than not, the vulnerabilities have the effect of encouraging specific threats. Our weaknesses are often the opportunities for others once they are aware of them.

It is generally true that it is very easy to design a system which, after it is built, is very difficult if not impossible to secure in an economically feasible way. It is also true, however, that it is usually not difficult to design a system providing the needed functionality but which is adequately secure if security is among the initial and basically coequal functional objectives. Thus, it is usually unnecessary, but nevertheless common, to invite threats through the incorporation of vulnerabilities into our designs.

Many of the systems which pose the more severe security challenges are those which evolved, Topsy-like, a component at a time, until it was belatedly recognized that the result was a complex difficult, if not sometimes impossible, to secure.

Concern for the ability to secure, after the fact, systems which were developed with little or no concern for security must be a major consideration in our design of security controls. However, the security needs of such systems must not be allowed to wholly dominate the programs to devise means for achieving security. Even though some of the more severe challenges are in existing systems, this should not be allowed to detract, by diversion of resources, from the drive to achieve adequate, economically feasible security.

2. The Relative Importance of Threats.- It is not a simple task to rank threats in accord with their relative importance. It is improper to assign relative importance to threats except in terms of both the consequences they produce and their probability of occurrence. Both the consequences and the probabilities of the realization of specific

threats are clearly system unique.

Threats cannot be weighed by just the severity of their consequences, because to do that is to ignore their probabilities of occurrence. Some of the most severe threats have probabilities of occurrence so low as to justify accepting the risks they present. If in the past we had ignored the probabilities of occurrence and weighed only the consequences, we would all now be wondering what to do with the few million bomb shelters in our back yards.

The relative severity of threats clearly varies as a function of the attractiveness of the target systems, their geographic locations, and other factors often including the perceived quality of the security provided them.

Threats should not be ranked by the number of security incidents attributable to a particular threat. If that is done, the incidents encountered or anticipated could then include huge numbers of relatively unimportant things while Illinois Bell's Hinsdale fire would be only one instance even though the cost to its customers exceeded \$500 million.

If threats are assessed in terms of the economic consequences, we have a workable basis for ranking them. No other basis has been shown to be workable in the information security environment. A major problem with ranking by economic consequences is the difficulties in costing social consequences, including loss of national security.

It is commonly argued that we cannot put a price tag on such matters as personal privacy or national security when, in reality, we do it quite routinely though haphazardly. Quite often we draw a line at what we are willing to spend, in dollars or inconvenience, to protect a facility or a system of records even though we know that there is residual vulnerability which can be eliminated by paying a higher price. In protecting against hard-to-quantify losses, the line is more often drawn at what we can afford, what is politically acceptable, or what we want to spend than it is related to the magnitude of the unfortunate consequences if the security is compromised.

3. Threat Rankings.- A survey of several hundred public and private sector organizations in the United States, Canada, and in seven western European countries reveals remarkable consistency in the relative importance or cost of the information security problems they encounter. Further, these rankings have remained quite stable over a period of thirteen years. Not only have their relative positions remained unchanged, so have the percentages of loss attributable to each problem category remained almost unchanged. For this reason, we should rely on these rankings until we have data indicating the need for change in them. These data indicate clearly that there is no basis for anticipation of an abrupt shift in the

problem environment unless a specific cause for that shift can be identified.

The categories into which the problems have been placed and the percentages of economic loss attributable to each are these:

- 65% errors and omissions
- 13% dishonest employees
- 6% disgruntled employees
- 8% loss of supporting infrastructure, including power, communications, water, sewer, transportation, fire, flood, civil unrest, strikes, etc.
- 5% water, not related to fires and floods
- <3% outsiders, including viruses, espionage, dissidents and malcontents of various kinds, and ex-employees who have been away for more than 6 weeks.

It might seem that minor variations in such a major category as errors and omissions would make the percentages attributable to the other categories highly unstable, but such has not been the case. For example, the factors which raise or lower losses to errors and omissions often have similar effects on losses to dishonest and disgruntled employees. For this reason, even though the size of the total losses may change, the apportionment among the categories has been fairly stable.

Again, these apportionments do not so much reflect the magnitude of the threats as they do the generality of the security weaknesses encountered in a large system population.

The data supporting the apportionments were derived from a study of 1,347 incidents, exclusive of errors and omissions, over a period of three years ending February 1991. Similar data extending back over thirteen years are also available. The data on errors and omissions were obtained from 442 organizations over that same three-year period and from 2404 organizations over the thirteen year period.

Voluminous questionnaires were used in gathering the data, but they were completed by investigators during on-site visits. For example, the one for incidents of computer-related employee dishonesty has fifty-one pages.

One criticism which might be made of these data will come from the assertion that "those are just about the same numbers that we have seen for years". That is true and it is also the reason why they should be used. They clearly demonstrate the relative stability of the problem environment and provide justification for not anticipating seriously disruptive discontinuities in the threat environment until we have identified a credible cause for them.

4. New Threats.- The continued rapid expansion in our dependence on computer-based systems and the continued increase in the complexity

of such systems bring with them, as they have for the past two decades, the need for new security measures, both technological and procedural, to counter the threats which result from their introduction.

Twenty years ago the needed measures included such elemental things as write verification and protection against improper disk pack swapping. The then current security design deficiencies included such things as designs that required the operators at the consoles to enter the users' passwords. We continue to add measures and, now as then, only after problems have been encountered and we suffer losses. There was then and there is now a need to consider the security implications of technical advances when we reduce those advances to practice and not later after we have been hurt.

The greatest single change in the nature of data processing, with the exception of the microcomputer explosion, is the rapid increase in the communication of data among networked computers. Considerable unnecessary concern has been generated as a consequence of postulating dire threats resulting from this still increasing networking even though there are no signs of abrupt changes in the nature or magnitude of the associated threats.

There is a real possibility that the greatest threat to the continued evolution of economically feasible, highly useful networks will be over-reaction to relatively minor security incidents. Indeed, it is not unreasonable to suggest that the real damage done by the Internet worm will be to the ease of use of that complex by those who would secure it. The overselling of security threats can itself be a problem often as threatening as the postulated problems.

There is still a widespread fear in the public and private sectors that cryptographic techniques impose unacceptable complexity on a system and greatly increase the serviceability problems. Because of this, many organizations have not bothered to find that cryptography is not nearly so complex and not nearly so expensive as they believe it to be and, because it is not expensive, is an economically feasible way for protecting the integrity and confidentiality of communications.

The rapidly evolving networking of systems clearly requires the continued rapid development of cryptographic systems which can accommodate the security needs of these complex systems. It is anticipated that this requirement will be reflected in the product-level standards and guidelines which are recommended below.

Certainly a significant threat to the confidentiality of proprietary data held by multinational corporations and ranking immediately after that of departing employees, is communications intercept on satellite links. In spite of that, typically there is a lack of familiarity with and a fear of using commercial cryptography, and together they remain a real barrier to countering the threat.

SUMMARY ON THREATS

There is no basis for a forecast of impending major discontinuities in the threat environment. Neither the nature nor the rate of change in data processing technology or in the application of new developments are such as to threaten major, broadly based and abrupt changes in the fundamental nature of the security problems.

The pace of business has accelerated greatly in recent years as a consequence of the introduction of computers into virtually every aspect of our organizations and has served to increase dependence on the availability of data and the means of producing information from them. As a consequence of that increased dependence, there is a steadily increasing and very healthy concern for information security growing in both public and private sectors.

An over concern has been given to highly sophisticated but improbable threats to data and data centers while the leaking roof over the main frame has been neglected and no means are provided for continuity of essential data processing services following a disruption of normal services. There is clear need for greater responsiveness of the NIST security activities to the actual problem environment experienced and reasonably anticipatable by the NIST constituency. Solid, fact-based education in the nature and relative importance of security problems is needed by both the civil agencies and the private sector.

The NIST security program should reflect concern for the ability of system implementers to develop a well-defined, properly prioritized security problem description for their specific environments. In the absence of better data than those provided above and additional data which are available, and which data have been validated repeatedly in the operational experience of many organizations, NIST should use these data until there is justification for change to data known to be better. The proposed NIST program provides for a critical evaluation of these data in association with other problem identification activities.

A RECOMMENDED SECURITY PROGRAM FOR NIST

A. SPECIFIC SECURITY PROGRAM COMPONENTS

The sequencing of the tasks will be constrained more by the availability of appropriate skills, talents, and experience and by the availability of valid requirements data than by the relative importance of getting them finished.

1. International Cooperation on Information Security Standards.- It is essential that NIST work aggressively to establish a cooperative relationship with the European standards proponents to the end that U.S. vendors are not harmed. NIST should represent the U.S.

interests in this area with the European Community as strong advocates of positions favorable to the interest of both the U.S. and the European Community.

It is important that we devise programs which dovetail with theirs to the end that the respective programs are mutually acceptable. It is too late to propose a radical departure from present proposals. It seems not at all late to propose an adaptation which is more attractive to all vendors than are any of their current ones.

2. Requirements Determination.- For NIST to establish and maintain a security program aligned with the needs of its constituency it must have a sufficiently comprehensive knowledge of the near-term future trends in data processing within that constituency and the security implications of those trends.

There are today some requirements for assistance which can be satisfied fairly quickly, that is, within a calendar year. Guidance in the conduct of a comprehensive information security program is an example. In general, however, most of the needs are not so obvious and many of the most important ones and the ones most likely to benefit from NIST participation are not today's needs but tomorrow's. In fact, attempts by NIST to respond to today's needs for security measures would, in general, not be helpful because of the multi-year lead times needed to accomplish most meaningfully progressive steps in the security area.

Attempts to satisfy many of today's needs would result only in the provision of obsolete problem solutions. For these reasons, the CSSPAB believes a specific process is essential for the determination of current and future requirements for NIST assistance in making information systems adequately secure.

The experience of vendors, professional societies conducting surveys, major accounting firms, and others has been that neither questionnaires nor interviews are adequate to the provision of enough information about current and future security needs to support other than quite superficial plans based on the information derived in that manner. Examination of the shortcomings of each of those approaches, however, leads to the conclusion that a combination of the two, carefully implemented, will yield the information sought.

For example, major deficiencies in the interview process include:

- a. access to the proper people,
- b. limitations in the breadth of knowledge of those interviewed,
- c. limitations in the familiarity of the interviewers with all aspects of data processing and security,

d. unwillingness of many of those interviewed to admit to any shortcomings in their security program,

e. difficulties in correlating the information acquired through conversations with people in many different organizations.

The major problems presented by the use of questionnaires include:

a. inability to assess the competence or position of the person/s completing the questionnaires,

b. the inability to ask follow-on questions when the answers are interesting or seemingly important,

c. problems accommodating unexpected deficiencies in the questions asked on the questionnaire.

For NIST to acquire the information it needs for the proper conduct of its security program, it should initiate a requirements determination program employing both the interview and questionnaire processes. Each of these two approaches should be designed to complement the other so as to minimize the shortcomings of each.

A questionnaire should be devised which asks specific questions about the current data processing environment and any recognized security deficiencies and the reasons for them, such as funding or the availability of adequate technical measures. The questionnaire should also ask about the direction of future growth in information systems and the security problems which will be introduced by this growth.

The handbook outline which the CSSPAB provided earlier should, with only a few modifications, provide an acceptable format for examining both the current and future security environments. The data requested should include copies of significant documentation, including policy statements, procedures manuals, physical security instructions, and a copy of the contingency plans.

The responses to the questionnaire should include the names and telephone numbers of the persons who can be contacted for further information about each response category, such as physical security, ID and authentication, contingency plans, logical access control.

Examination of the responses to the questionnaires will reveal needs for additional information or clarification, need for verification of some responses, and needs for further discussion of seemingly important issues raised by the responses. Much of this additional information can be obtained by telephone from the persons identified in the responses. Some of the responses will open major new areas of concern; some will identify new applications which introduce previously unanticipated problems; and some will provide new and seemingly important insights. Many of these will justify follow-up

5. Product Level Security Standards and Guidelines.- There is a clear need to address with appropriate balance the whole set of security needs of information systems. We cannot afford to consider confidentiality in isolation from integrity and availability. Measures which provide protection for all of these often can be recognized and selected if all three are given properly balanced and concurrent consideration. They must not be considered separately. When they are considered separately, it is not unusual to see the protection of one compromised by the protection afforded the other and, even when that pitfall is avoided, the measures selected will rarely be most economically feasible set because they will not complement each other properly.

The data processing market reflects quite clearly the need and desire of those implementing data processing systems, at other than the single microcomputer level, for an ability to select the hardware and software components they need and want as opposed to having the vendor supply complete, integrated systems. Identical requirements are so rare as to make it generally infeasible to package and thus impose fixed hardware and software configurations on the customers.

There is as much justification for flexibility in the composition of security attributes as there is for flexibility in the selection of other functional and performance characteristics. The diversity of security concerns seen routinely in the private sector can also appear in the civil agencies of the federal government. They must be containable at reasonable cost through the availability of appropriate measures selected to provide a set customized to the particular needs of each different situation.

What is sorely needed now is enough uniformity in describing the functional characteristics of the individual security measures at the device level to permit the establishment of a market for the appropriate measures. Those procuring data processing products, whether they are main frames or data base management systems, must be forced into the position of having to prepare detailed specification of the security characteristics each needs. If they do that, no two sets of functional objectives will be alike and the cost for each will then be prohibitively high. Examine now how we might fix that situation.

We propose that NIST, with the advice and consultation of the federal and private sector user communities and the vendors, immediately and aggressively undertake the preparation of guidelines describing, for each major product category, a set of the principal security attributes which should be considered by vendors for inclusion in products in that category. The product categories would be things such as mainframes, minicomputers, data base management systems, disk drives and their associated controllers, communications controllers, point-of-sale terminals (which are used in federal systems), microcomputers, and others.

visits with the individual persons who can address those specific areas of interest.

(Experience with this approach shows that about half to one-third of the responses need follow-up by telephone and one in seven are worth a visit, but these ratios are highly sensitive to the composition of the questionnaire and the nature of the organizations to which they are sent.)

3. Issuance of a Security Handbook.- NIST already has plans for the preparation of a handbook for guiding the implementation of information security programs. It is anticipated that this handbook will not be a text on information security but a means for providing education in the general topic and references to more detailed treatment of specific topics.

Plans should be made now to maintain the handbook perhaps in loose-leaf form. A major portion of the maintenance activity should be the provisions of new references for specific areas of the handbook.

Every reasonable effort should be made to make this handbook a major contribution to the well-being of the NIST constituency and to NIST's profile in the information security area. Its quality must not be compromised in a rush to publication.

4. Guidelines and Standards on Network Security.- The need for network security standards is now evolving quite rapidly. Their generation should have high priority on any list of NIST security activities.

Computer networks often present challenging security problems. Homogeneous networks joining heterogeneous organizations present significant and sometimes challenging security problems, particularly in access control and accountability. But heterogeneous networks joining heterogeneous organizations provide a major challenge to those who must secure them. In spite of the size of the challenge, adequate, practicable, and economically feasible security is needed and the need for it will continue to grow well into the foreseeable future.

There is no reason to expect the many vendors of network components to arrive at a mutually compatible set of security measures except as those measures are provided in response to formal standards.

In the generation of network security standards, NIST must resist the temptation to overly complex, too heavily layered solutions with resulting negative economic effects, which will be difficult to maintain, and which lack adaptability to differing and changing security environments. Care must be taken to avoid an overly complex solution in the image of the "Swiss Army Knife", that is, a solution which attempts to address with one basically non-modular package a quite diverse problem environment, addresses each problem partially, and collectively can be a noticeable burden.

To illustrate, the vendors would not be required to implement all or even any of the attributes described. They would be required, if they want federal business, to list on the equivalent of a sticker in the left rear automobile window, the following:

- a. the whole set of security attributes in the NIST list for that product type,
- b. the ones which are in the base product and are not options,
- c. the ones which are available only as factory-installed options,
- d. the ones which are available as field installable options,
- e. those security measures which are not on the NIST list but which have been included by the vendor and, if they are substitutes for any on the NIST list, identification of those for which they are substitutes.

It is anticipated that these guidelines would become standards as promptly as they can be evaluated, corrected where needed, and the process of issuing them, one at a time, completed.

The proposal made here for product-level standards makes adequate security at reasonable cost an achievable goal. It has been conceived with the notion of satisfying the needs of both the users and the vendors. We need to start now; time is of the essence.

It is assumed that work in the cryptography area will be a subset of the activities leading to the generation of standards and guidelines in products. If those cryptographic activities do not lead to description of appropriate implementations in products, then their utility to the NIST constituency should be reconsidered.

It is also assumed that work in support of public key systems will be a major subset of this product-level security guidelines and standards work.

6. Risk Analysis.- It seems improbable that risk analysis, as an activity, should be wholly separated from the selection of security measures. For this reason, the philosophy underlying virtually all of the available software packages for risk analysis should be carefully examined.

Because almost all security measures have security benefits beyond containing just one problem, the assessment of risk and its reduction by appropriate, cost-justified measures must be an iterative process. Just as a truss bridge is not designed a member at a time nor should a member of it be modified, added, or deleted without assessing the effect on the overall structure, so must the need for protection and its provision be considered concurrently.

There is today no reasonably adequate, published guidance for the selection and implementation of cost-effective security measures. This situation should not be allowed to continue. Some real innovation will be required to make a meaningful contribution in this area.

It is imperative that risk analysis become an inherent part of designing, implementing and subsequently augmenting their capabilities as needs arise.

7. Digital Signature.- Work in this area should be carefully assessed for proper alignment with the requirements as determined through the Requirements Determination program recommended in Paragraph A.2, above. It should only be pursued if there is a real need for it and which need is sufficiently great to justify diversion of effort from the generation of the standards and guidelines described in A.5, above.
8. Guidelines on Contingency Planning.- There is a very real and broadly recognized need for innovation and instruction in contingency planning, that is, planning to respond to and, as necessary, cope with events which threaten to disrupt the means of collecting, entering, storing, selecting, and presenting data from which information is derived. This is no simple task. Currently available technology in this area, including studies of the economics of the available alternatives, is not adequate to the needs of many major data processing systems, although it would be useful to a number of smaller ones.

It is important that this activity not be called a "disaster recovery" activity. To do so misplaces the emphasis of the desired goal.

9. Support of the Joint NIST/NSA National Conference.- The joint conference is a major contribution to information security. Every reasonable effort should be made to enhance the quality and the value of the papers presented there. NIST must maintain and aggressively continue its support of the activity.

CONCLUSION

It is not easy for a technical group to resist attractive targets of opportunity with resulting neglect to more important, longer-term programs. The ability to resist is one important measure of the quality of its management. The strength to do that within the NIST computer security organization must be developed. If an activity does not lead clearly and directly to furtherance of the NIST security goals and if it does not wholly justify the diversion of resources, including time, it must not be considered.

Every effort must be made to attract technically strong, highly motivatable people who have genuine interest in working in information security. Particular emphasis should be given to the acquisition of people with the curiosity to acquire an in-depth understanding of the realities of the data processing environments to which their efforts will be applicable.

The civil agencies of the federal government, state and local governments, and the private sector all need the results of a well-conducted NIST information security program. Such a program should be pursued aggressively and as quickly as possible.



NIST

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

September 9, 1991

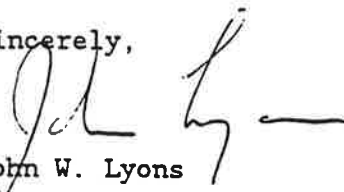
Dr. Willis H. Ware
Chairman
The National Computer System Security
and Privacy Advisory Board
Gaithersburg, MD 20899

Dear Willis:

Thank you for your letter of August 22 and the enclosed recommendations. I have gone through it and marked it up in several places and will be reviewing it with Jim and his team. With Ray Kammer's departure I have to rethink our working relations with other Federal agencies; your comments should help me with that too.

Thank you for the report.

Sincerely,



John W. Lyons
Director

cc: JHBurrows

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

OCT 22 1991

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

Dear Dr. Lyons:

Enclosed herewith is a second document which sets forth the Advisory Board's context for the conduct of the CSL research program. Actually this and our July letter are two parts of one document but have been sent you in reversed order. If you will please put the enclosed item on top of the prior one, the two together will become a coherent treatment of the Board's concerns about the program as previously presented to us.

The Board was particularly concerned and sensitive to the question of the boundary between the FIPS which NIST will publish for secure computer systems and the Criteria which NCSC has published and may revise. We feel it especially important that the vendor industry not have to market different products conforming to the requirements of your FIPS but separately to the NCSC Criteria.

Our best attempt to express our concerns is the fourth paragraph of section four on page two. We think it might well for your office to maintain some visibility over the NCSC/CSL interaction and the FIPS/Criteria interface to assure the best interests of the country are served.

We are available to discuss these two documents at your request.

Sincerely,



Willis H. Ware
Chairman

Enclosure

A CONTEXT FOR THE NIST SECURITY PROGRAM

I. POLICIES, POSITIONS AND RELATIONS.

1. NIST/CSL SECURITY Program Orientation - The principal thrust of the NIST/CSL security program should be to establish NIST/CSL as the preeminent authority to which the agencies of the federal government and, less directly, state and local agencies and the private sector look for leadership in information security. While NIST/CSL is often asked to perform consulting roles for agencies dealing with unclassified information, it should do so only to the extent that it does not limit the accomplishment of its principal thrust.

NIST/CSL must issue such standards and guidelines in information security as will benefit a broad segment of its constituency. As noted below, it should take an aggressive stance in advancing the interests of both the civil agencies and the U.S. vendor community by devising workable and potentially acceptable proposals for cooperating with European security initiatives.

2. Selling the NIST/CSL Program - NIST/CSL should aggressively sell the benefits to the federal government of its security activities. Too many members of Congress, congressional and OMB staffers, and many others in the government consider information security to be no more than protection of data against unauthorized disclosure (confidentiality).

The principal justification for funding the NIST/CSL security program should be the obvious benefits to the federal government, to state and local governments and to the private sector of having data which have, as appropriate, the characteristics of accuracy, timeliness, completeness, and confidentiality. The decision makers need to understand that money spent enhancing these characteristics of data is money returned several fold in increased effectiveness and reduced cost of government.

Unless the visibility of NIST/CSL's activities in computer and communications security is raised, there seems little reason to expect the major increases in funding needed to let NIST/CSL do what is really needed of it - and no one is able to raise its profile but NIST/CSL itself and, to a very limited extent, the Advisory Board.

3. NIST/CSL-NSA Relations - By both law and executive order, NIST/CSL and NSA perform significantly different functions in support of different though overlapping constituencies. The challenge for both agencies is to cooperate where necessary and appropriate without engaging in a burdensome and potentially endless process of coordination. Because the resources available to NIST/CSL are much smaller than those of NSA, the potential loss of productive effort is of much more concern to NIST/CSL.

There are, however, areas where NIST/CSL and NSA must either coordinate their efforts or clearly delineate the boundaries between their activities. In the area of cryptography, where certain responsibilities have been given to NSA by both law and presidential directive, there is a need for a high level of cooperative activity. While both agencies are active in the area of operating system ("trusted system") computer security, a delineation of responsibilities such as proposed in section 4 below is desirable.

Cooperative endeavors should not be rejected out of hand, but neither can cooperation be a forced goal for its own sake. It must be, rather, a basis for a mutually beneficial exchange of information.

As it is charged to do by P.L. 100-235, NIST/CSL must maintain awareness of pertinent technical developments within NSA which might benefit the constituency of the NIST/CSL security program and incorporate into the NIST/CSL program those developments appropriate to the program.

4. NIST/CSL and NSA Roles re Evaluation Criteria - It should be anticipated that most or all vendors will, in time, enhance the basic design of their operating systems and the supporting hardware to the end that C2 or B1 capabilities will be uniformly available and no longer optionable by the customer except to the extent that such things as access control or individual accountability may have no meaning in specific applications and are not then imposed.

NIST/CSL, with support from NSA, should take responsibility for the development and promulgation of criteria in the form of FIPS for what has until now been referred to as C2/B1 of the DoD Trusted Computer Security Evaluation Criteria. Testing and evaluation of systems which meet these criteria should be conducted under the auspices of the National Voluntary Laboratory Accreditation Program (NVLAP).

NSA, with support from NIST, should continue to develop and promulgate criteria for B2 and higher levels of trust and to conduct evaluations as appropriate for these levels.

There will likely be a tension between the desire for compatibility and continuity of the NIST/CSL criteria with those of NSA. NIST/CSL and NSA should each weigh carefully the needs of users, the security threats to be addressed, the needs of suppliers, and the desire for compatibility with other criteria (e.g., the European ITSEC) in determining what level of compatibility and continuity is appropriate. Draft criteria should be subject to trial use on systems of real-world scope and complexity, and the trial use experiences documented before the criteria are finalized. It is desirable that there be compatibility and continuity of the

NIST/CSL criteria with those of NSA.

5. Other Agency Activities - NIST/CSL should undertake outside funded activities when they are consistent with and contribute toward the accomplishment of NIST/CSL's principal thrust.

NIST/CSL should perform a careful review of its outside activities for FY92 and beyond and seek to terminate in an appropriate and timely manner those which do not directly support its basic goals and obligations.

6. Cryptography - NIST/CSL must continue its essential role in support of suitable cryptographic protection for the civil agencies and the private sector. Specific product-level activities, are a subset of paragraph II.5 of the document: "A Proposed NIST R&D Information Security Program."

There is need for continued pursuit of exportable algorithms. The current arrangement is seriously inadequate to the security needs of many organizations needing secure trans-border communications. Such security is essential to the national security even though the data are not those usually recognized as "national interest" data. The economic well-being of the U.S. business community is an extremely important national interest matter.

7. CERTS - NIST's activities in this aspect of the program should be limited to coordination and facilitation of federal agency activities. NIST should undertake no responsibilities that properly belong in operational agencies.

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

January 7, 1992

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

Dear Mr. Darman:

As provided by the Computer Security Act of 1987, I would like to take this opportunity to report to you that the Computer System Security and Privacy Advisory Board has reached consensus on an emerging issue effecting the security of federal computer systems.

The problem that we bring to your attention is the apparent lack of formalized computer emergency response capabilities on the part of most federal agencies which operate unclassified computer systems and networks. The need for formalized, structured emergency response capabilities was underscored at the time of the malicious software attack on the INTERNET in November 1988.

As a result of that event the Department of Defense established the Computer Emergency Response Team at Carnegie Mellon University. The value of the activity has been proven repeatedly over the past few years, and its success has led to the creation of eleven similar centers within the Department of Energy, the National Aeronautics and Space Administration and the military services.

During our September 1991 meeting, the Board requested that personnel from the National Institute of Standards and Technology informally survey the federal community for the purpose of identifying other organized computer emergency response structures. This informal survey identified no additional formally structured computer emergency response entity that could be activated in the event of a significant computer and/or telecommunications network emergency. Although we note that most agencies appear to be dealing effectively with localized incidents of computer viruses, this approach may not be adequate to enable them to respond to a highly sophisticated or large scale attack.

THE NATIONAL
COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

January 9, 1992

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

Dear Mr. Darman:

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

During the last three Advisory Board meetings we have reviewed the progress of the Computer Security Act agency visit program described in OMB Bulletin 90-08. In accomplishing this project we have heard from a wide variety of federal employees involved in various aspects of this effort. These individuals have included members of the OMB staff responsible for planning and executing the visit program; agency computer security officials and senior information management executives, and participants from the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

I am very pleased to state that we have heard nothing but positive comments from all of those involved in the agency visit program. We have been particularly impressed with the enthusiastic reactions of agency participants, who have advised the Board that visits to their agencies have resulted in greater awareness of computer security issues on the part of senior officials in their organizations. This, in turn, has resulted in enhanced management support for agency computer security programs.

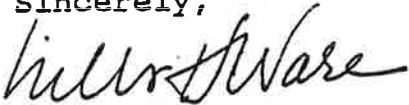
The Board notes that within the next few months OMB/NIST/NSA representatives will have completed visits to all of the agencies included in the initial Bulletin 90-08 program. We believe that it would be very beneficial if a summary report documenting the results of this activity were prepared and shared with concerned agency and Congressional officials, as well as interested private citizens. The pending conclusion of visits projected in Bulletin 90-08 will require OMB officials to plan for additional activities designed to sustain the spirit and intent of the Computer Security Act of 1987.

In planning these future activities, our Advisory Board recommends that OMB build upon the successful formula that has produced the positive results noted above. We believe that the emphasis on underscoring management involvement as a fundamental prerequisite for effective computer security program is appropriate and should be maintained in a subsequent initiative. The Board also urges OMB to consider how this message can be effectively delivered to major Federal centers and activities outside of the Washington area.

I appreciate the opportunity to express the views of the Computer Security and Privacy Advisory Board.

I look forward to your response. You can reach me through the RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138.

Sincerely,

A handwritten signature in cursive script that reads "Willis H. Ware".

Willis H. Ware
Chairman

IV. 1992 Advisory Board Workplan

I. INTRODUCTION

This section sets forth the proposed 1992 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 1992 activities. The Board recognizes that other subjects not previously identified in this planning document may arise during 1992. 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 1992 WORK ITEMS FOR CSSPAB

A. Action Items. The Board will examine the following new topics during its 1992 program year:

A.1. 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.

A.2. Data Encryption Standard (DES) Revalidation. The DES will come up for revalidation in early 1993; however, the public policy issues underlying any decision to revalidate DES or move to another encryption standard will be decided during 1992. The Advisory 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.3. Public Key Cryptography. The Board will 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.4. Computer Security Guidelines and Standards. The Board will monitor NIST and 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 NIST/NSA Work Plan on Trusted System Technology. NIST program updates should be scheduled in March 1992 and September 1992. NSA program updates should be scheduled for June and December 1992. Each briefing should

B.7. Implementation of the Computer Security Act. Subsumed under this heading are the various related issues the Board would like to address in 1992. These include an examination of Office of Management and Budget policies, including the anticipated rewrite of OMB Circular A-130. Also of interest is the role of the Inspector General in computer security. Computer security training and its effectiveness are also to be studied. Lastly, the Board would look into the status of OMB/NIST/NSA security planning agency visits. What lessons have been learned? What are the plans for a followup activity?

B.8. 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.9. 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.

V. Conclusions

During its third year, the Board continued to build the foundation toward progress in the years ahead. It developed a work plan and established its priorities for 1992. The Board has begun to examine those issues which it should study further and has heard from a number of agencies and organizations as to its role and duties. While the Board has initiated an action plan to identify emerging computer security and privacy issues, much remains to be accomplished in successfully addressing the challenges of the 1990s.

