Information Systems Security Board
CONCEPT PAPER
July 17, 1996

This is a concept paper developed by the National Information Infrastructure Task Force, a working body of the President's National Security Telecommunications Advisory Committee. Its purpose is to stimulate discussion and elicit comments regarding a private sector entity intended to improve the common understanding of the nature and purpose of information systems security. The entity would promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services.

Purpose

The National Information Infrastructure Task Force (NIITF) of the National Security Telecommunications Advisory Committee (NSTAC) is investigating the advisability of establishing an Information Systems Security Board (ISSB) to improve the common understanding of the nature and purpose of information systems security. The ISSB would promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services. In its investigation, the NIITF has developed the following proposed model to stimulate the development of a private-sector-based focal point to enhance the security component of the NII.

Background

The emergence of advanced information technologies and services has generated enormous benefits for the Nation. The introduction of new information technologies and services, however, generates a whole new set of vulnerabilities. The convergence of computing and telecommunications, while highly beneficial from a broad commercial perspective, has made information and information systems attractive targets for criminals. Unfortunately, in many instances, the implications of the vulnerabilities and threats to the NII and corporate commercial networks are not fully realized or appreciated. With information technology becoming so pervasive in society, information systems security has become increasingly important and national in scope.

The vulnerability of commercial and government information systems has become increasingly publicized. In a survey released in May 1996, the Computer Security Institute in San Francisco, working with the Federal Bureau of Investigation (FBI), discovered that 42 percent of more than 400 commercial, educational, and government organizations responding to its questionnaire had detected some "unauthorized" use of computer systems within the last 12 months.[1] A recent report by the General Accounting Office (GAO) stated that the Defense Department estimates as many as 250,000 attacks occurred on its information systems in 1995.[2] The Defense Department vulnerabilities raise significant national security concerns.

The vulnerabilities of commercial information systems represent potential losses reaching billions of dollars and also raise national security concerns. The frequency of losses due to computer hacking and other forms of economic espionage are estimated to have increased 323 percent since 1992, according to the American Society for Industrial Security International in Arlington, VA. The average loss per incident was $26 million, and losses to U.S. industry overall reached near $2 billion per month, the society claimed.[3]

Moreover, in an article published in the *Computer Security Journal*, Hal Tipton, President, International Information System Security Certification Consortium (ISC)2, noted an alarming increase in the number of suits filed by the Federal Government, stockholders, and employees, which resulted in corporate officers being held liable for negligence in exercising due care to ensure the integrity, confidentiality, and availability of proprietary information.[4] The consequences of information system vulnerabilities have led some to predict that the information systems security market will be driven in part by the business insurance industry. As organizations make insurance claims for losses related to hacker activity, the insurance industry will begin to mandate better information security software and hardware.[5]

---

[1]"1996 Computer Crime and Security Survey," Computer Security Institute, San Francisco.

[2]"Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," United States General Accounting Office, May 1996.

[3]"Firms Seek Legal Weapons Against Info Thieves," *Computer World*, May 27, 1996.

[4]"Liability of Corporate Officers for Security Problems," *Computer Security Journal*, Vol. X, Number 1.

[5]"Internet Security: The Impact of Firewalls on Client Server Applications.," *Disaster Recovery Journal*, April/May/June 1996.

In February 1996, the National Information Infrastructure Testbed (NIIT) issued a report that was a wake-up call to industry on the importance of the NII in driving United States competitiveness. Based on a survey of major U.S. corporations, the report concluded that infrastructure providers must join forces with users of information technology to develop applications that improve their productivity, business and management processes, and competitiveness. The survey indicated several challenges to the development of the National Information Infrastructure (NII). The greatest challenge was a lack of public understanding and user acceptance. The second greatest challenge was inadequate security.[6]

The Congress has legislated the responsibility for Federal computer security standards and guidelines to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). There is no analogous information systems security focal point for the private sector. The need for such an organization was previously identified by the National Research Council (NRC) in 1991. The NRC report entitled, *Computers at Risk -- Safe Computing in the Information Age* stated, "The public needs an institution that will accelerate the commercialization and adoption of safer and more secure computer and communications systems. To meet that need, the committee recommends the establishment of a new private organization - a consortium of computer users, vendors, and other interested parties (e.g., property and casualty insurers). This organization must not be, or even perceived to be a captive of the government, system vendors, or individual segment of the user community." [7]

Discussion

In developing the concept paper, the NIITF identified potential information security functions that an ISSB might perform and then surveyed a sample of private companies, associations, universities, and Government agencies known to have significant information security programs, to determine which functions were being addressed by those organizations. The NIITF discovered that many of the functions were being addressed primarily either by the Government or for the Government by contractors, but not for the private sector.

---

[6]"The Unfinished Business of the NII," National Information Infrastructure Testbed (NIIT), February 12, 1996.

[7]*Computers at Risk - Safe Computing in the Information Age*. National Research Council, 1991.

In addition, the NIITF conducted research into organizational models that might provide a conceptual framework for an ISSB. These models included the United Kingdom's (UK) Commercial Licensed Evaluation Facility (CLEF) and the NIST's commercial evaluation laboratories initiated under its Trust Technology Assessment Program (TTAP). Finally, the NIITF examined the accounting industry's Financial Accounting Standards Board (FASB). The proposed model for the ISSB is structured to achieve the institutional independence advocated by the NRC and accomplish those

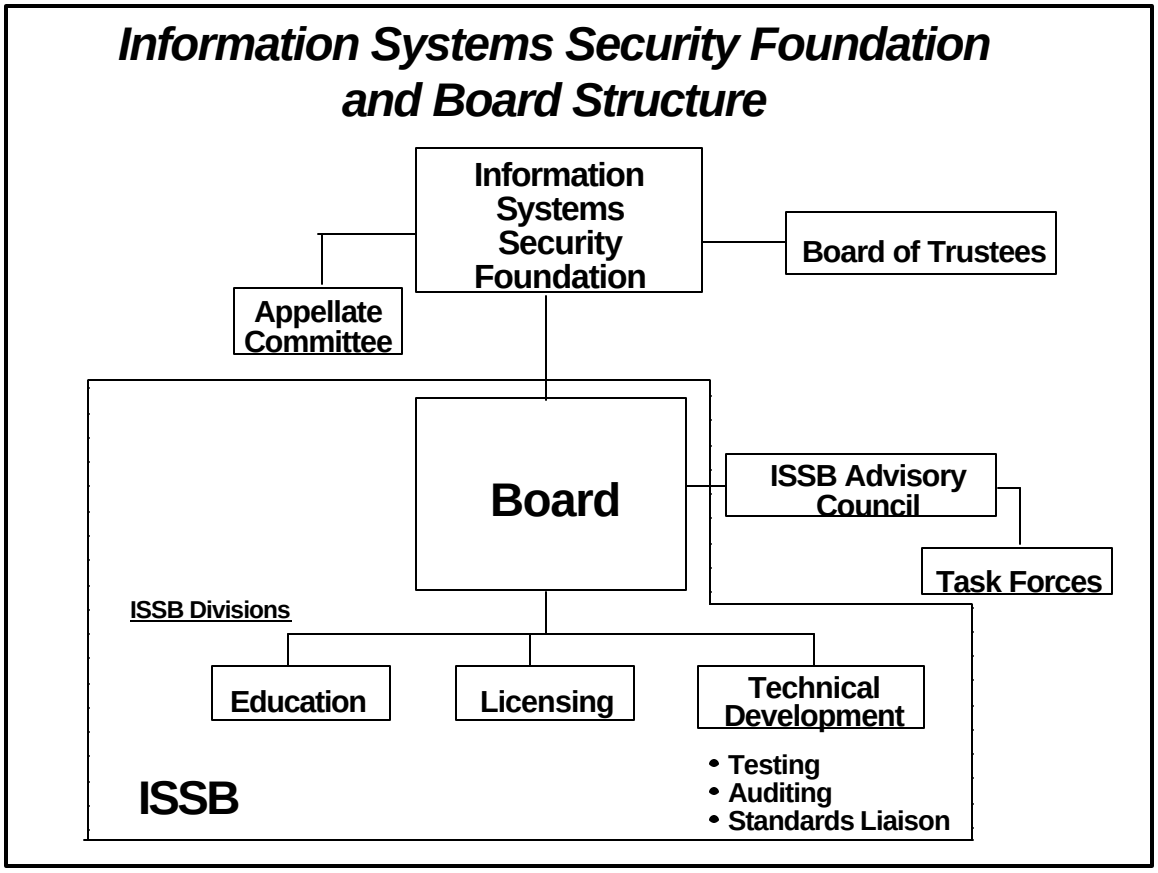

Figure 1: ISS Board and Foundation Structure

functions necessary to perform its mission.

Model

Figure 1 represents the Information Systems Security Foundation (ISSF) and ISSB structure. The structure consists of the Information Security Foundation, the foundation's Appellate Committee and Board of Trustees, and the ISSB. In addition,

there would be an Information Systems Security Advisory Council. The ISSB will be independent of all other business and professional organizations. It will coordinate closely with other organizations, particularly those in the standards, product validation, and systems evaluation communities. Figure 2 illustrates these relationships. A discussion of the ISSF and ISSB structure follows Figure 2.

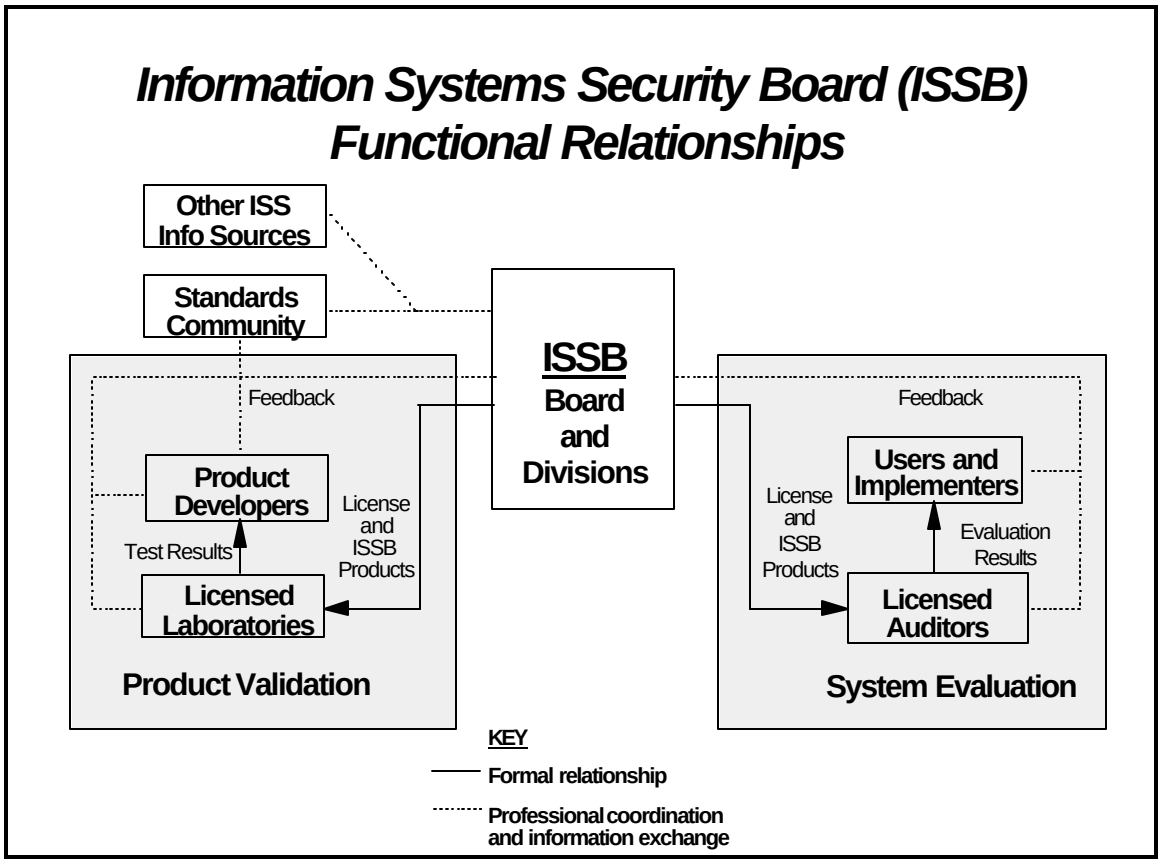

Figure 2: ISSB Functional Relationships

Information Systems Security Foundation (ISSF)

The Information Systems Security Foundation will be incorporated to operate exclusively for charitable, educational, scientific, and literary purposes within the meaning of Section 501(c)(3) of the Internal Revenue Code, and membership will be open to sponsoring organizations with a demonstrated interest in information systems security. The general purpose of the ISSF will be to

promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services. That function will be performed by the ISSB with the advice and counsel of the ISSB Advisory Council.

ISSF Board of Trustees

The ISSF will be governed by the 12 member Board of Trustees. The Trustees will be elected for 3-year terms with four new members elected each year. The initial terms will be for periods of 1, 2, and 3 years in order to establish a rotational membership. Nine trustees will be nominated by the sponsoring organizations of the ISSF. In addition, there would be three at-large trusteeships who in the judgement of the Board of Trustees would contribute to advancing the purposes of the ISSF and ISSB.

The Board of Trustees will select the members of the ISSB and its Advisory Council, fund their activities, and exercise general oversight (except with regard to the ISSB resolution of technical issues). The Board of Trustees will also raise funds and approve the ISSB budget.

ISSF Appellate Committee

The Board of Trustees will promulgate formal procedures for filing and adjudicating appeals. It is expected that most appeals will be resolved by the ISSB and its staff. However, the Board of Trustees will establish a standing Appellate Committee to review appeals that cannot be resolved by the ISSB. In the event of an appeal to the Committee, the Committee will chair a panel of experts selected from the membership of the Foundation to review the merits of the appeal and recommend a ruling to the Appellate Committee.

Information Systems Security Board

The ISSB will consist of seven recognized experts, one of whom will be designated chairman, selected by the ISSF from among the candidates nominated by the foundation members. The members will serve full-time and will be required to sever all connections with the firms or institutions they served before joining the Board. Board members will be appointed for 5 year terms

and be eligible for reappointment to one additional 5 year term. The ISSB will serve as the initial venue for appeals related to the ISSB process. The ISSB will provide clerical support to technical task forces convened by the ISSB Advisory Council (described below). Members of the Technical Development Division will participate as task force observers as appropriate.

Functions

The ISSB will perform the following functions:

- Evaluate and endorse information systems security standards and testing criteria developed by the standards community.
- Develop or endorse testing criteria.
- Develop and maintain information systems security principles (ISSP).
- Identify areas in which information systems security standards are lacking and new standards need to be developed, working with the standards community to initiate development.
- Develop rating criteria to identify varying levels of security.
- License testing laboratories and auditing organizations to use the ISSB logo and ratings to identify that a product or system meets ISSB endorsed standards for the intended application. The license would be issued based on application and proof of competence.
- Enhance the understanding of information security issue solutions and promote the use of ISSB endorsed standards and methodologies.
- Issue technical notes to license holders, product developers, and the standards community.
- Establish a process to adjudicate ISSB rules, testing results, and auditing determinations appeals.

The internal organization of the ISSB would be divided between education, licensing, and technical development divisions. The divisions would provide

support to the board and to special task forces of industry personnel convened to address specific technical issues. Each division of the proposed structure is discussed as follows.

Licensing Division

This division will issue licenses to testing laboratories and auditing organizations that have been recommended for approval by the Technical Development Division and approved by the ISSB.

Technical Development Division

This division will develop information bulletins, review standards and make recommendations for endorsement, identify needed standards, develop testing and auditing procedures, and ensure the competence of testing labs and auditing organizations. In addition, the division will develop and maintain information systems security principles.

Education Division

This division will be responsible for public relations, education, and outreach activities related to information security issues. The division will promote the use of ISSB endorsed principles, standards, and methodologies

ISSB Advisory Council

The ISSB Advisory Council will be responsible for consulting with the ISSB as to technical issues on the ISSB agenda, project priorities, and the selection and organization of specialized task forces. The Council will consist of technical experts, broadly representative of all elements of the information infrastructure, (e.g., commercial carriers, software developers, hardware manufacturers, information service providers, system integrators, and Government) selected by the Foundation. Provisions for rotation of Council membership must be developed. The Council will convene task forces to provide subject matter expertise, a diversity of view points, and a mechanism for communication with those who may be affected by a proposed action. The Council will receive and review reports of the task forces for forwarding to the ISSB.

Benefits

The ISSB can provide significant benefits in the areas of the information systems security market, business liability, cost reduction, and increased competitiveness. These are summarized as follows:

Market

The ISSB will contribute to an expanding commercial market for retail and wholesale networking and enhance the strength of private and government networking. An ISSB will foster fair and open innovation and competition while helping users to make intelligent choices among many potential solutions to arrive at ones appropriate to their application and individual situations.

Broad representation in the Information Systems Security Foundation will ensure that ISSB principles, endorsed standards, and audit methodologies reflect a thorough knowledge of consumer information systems security needs At the same time, consumer confidence in the selection of ISS products and services will be enhanced. Consumers will have an authoritative source to rely on as various vendors employ ISSB-licensed products to help those customers achieve the sufficient and necessary protection they desire. The improved level of understanding and a common set of principles, standards, and methods will ensure that providers will have a better defined marketplace into which they can introduce enhanced and innovative products.

Reduced Liability

With passage of the Telecommunications Act of 1996, information system (including telecommunications) providers will be free to provide products and services and to compete in ways they previously were not allowed. This new freedom promises to unveil many new and exciting products and services for consumers and opens exciting new business opportunities to all companies that are either involved in or dependent on information systems and services.

This new freedom also brings with it greater responsibility for service providers. New and enhanced information services will flourish. Users will depend on these services for economic well being. Users will also expect a higher degree of confidentiality and privacy - not well-defined terms today - as these services are utilized. Service providers must supply the degree of reliability and security users demand and expect. Users must also accept responsibility for protection

of information processing. End-to-end protection of information requires a coordinated approach to information system security. The ISSB will provide an independent, verifiable source for use in the due diligence process.

Cost Reduction

By providing a basis for evaluating products and services, the ISSB will contribute to lower costs for both consumers and sellers It lowers the cost of the buying decision for consumers by providing an accepted criteria for the level of risk they wish to assume. Consumers are provided with a common basis of comparison that will be consistent over time. Similarly, it lowers the selling decision costs for the provider. Providers can target the particular market niche they intend to pursue based on the evaluation principles, endorsed standards, and auditing methodologies of the ISSB.

Global Competitiveness

Finally, the ISSB will allow the United States to approach the world market with an organized set of information systems security products and services that customers can intelligently evaluate on a consistent scale consistent with their intended use. Establishment of the ISSB will represent an organizing force that will encourage other nations to work with the United States to resolve differences related to international information systems security. Information systems security inherently requires interoperability, and the internationalization of most businesses today requires that information systems security solutions truly be global in their application.

Resources

The expense for establishing and operating the ISSB, its oversight foundation, and its supporting staff is not expected to be large relative to the benefits gained. This paper does not attempt to quantify costs in detail. However, the paper is intended to elicit discussion, reaction, and suggestions, which may affect detailed cost estimates.

The seven members of the ISSB will sever all ties to their previous organizations and will be paid a salary through the ISSF. ISSB members are expected to be prominent professionals from various sectors representing broad, in-depth knowledge of information systems security technology and issues, and an understanding of their application and use. Support for the board will consist of a director and staff.

Funding Sources

Funding for the ISSB should be addressed in two parts, startup and continuing. The mission of the ISSB is extremely supportive of the goals of the Federal Government for the National Information Infrastructure and the role of the United States in the Global Information Infrastructure. Therefore, up-front government seed money may be appropriate to ensure a successful startup and transition to full private sector support.

Continuing funding will be supplied by a variety of sources. The largest of these will be membership fees in the ISSF. The ISSF membership has significant advantages and should attract many organizations.

Other sources of income will include licensing fees for use of the ISSB logo, products, and services. Income could also include residuals from products or services sold bearing the logo and ISSB rating. Sale of ISSB documents (endorsed standards, principles, evaluation methodologies, etc.) will also contribute to the budget. Finally, any conferences, symposia, etc., hosted by the ISSB should be conducted so as to ensure a positive net flow to the budget.

Questionnaire

The purpose of this white paper is to stimulate discussion and elicit comments regarding the Information Systems Security Board concept. Attached is a questionnaire developed by the NIITF. Please respond to each question, and add any additional comments accordingly. If you would like to discuss this project further, please contact Mr. Guy Copeland, Computer Sciences Corporation (CSC), the NIITF chair, at 703-867-3562 or the NIITF's coordinator, Brad Bigelow, at the Office of the Manager, National Communications System, 703-607-6211 (phone), 703-607-4826 (fax), or bigelowb@ncr.disa.mil (EMail).