STATEMENT OF

JOHN W. LYONS, ACTING DIRECTOR

NATIONAL BUREAU OF STANDARDS

U.S. DEPARTMENT OF COMMERCE

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

HEARINGS ON TELECOMMUNICATIONS SECURITY AND PRIVACY

OCTOBER 17, 1983

## 1. Introduction

I am John Lyons, Acting Director of the National Bureau of Standards (NBS). I am accompanied today by Dr. Dennis Branstad, Manager of the Computer Integrity and Security Technology Group in the Bureau's Institute for Computer Sciences and Technology (ICST). We are pleased to have this opportunity to testify before this Subcommittee on the important topics of computer communications security and privacy.

I would like to present an overview of the Institute's Computer Security and Risk Management Program which covers the subjects of computer communications security and privacy. I will then highlight the technology of computer network security being developed for reducing the vulnerabilities of computers and communications.

## 2. A Perspective on Computer Security and Privacy

Computer security is a complex area that involves numerous scientific disciplines and related management issues. Computer security has been discussed for nearly twenty years, but various

publicized incidents have recently brought to the nation's attention the need for computer security, and especially telecommunications security.

Every organization which uses a computer, especially those providing remote access to the computer, should be acquainted with the vulnerabilities that were exploited in these incidents, and should then consider its own vulnerabilities and related risks. Following this procedure, generally called a risk analysis or risk assessment, the organization should select a set of safeguards for minimizing the overall risk. When selecting safeguards, an overall balance must be maintained among security, cost and residual risk.

3. Purpose and Scope of the NBS Activities in Computer Security and Privacy

NBS is the nation's central reference laboratory, providing measurement methods, standards, and data that are used throughout the government and industry. It is a technical organization that encourages and performs research, technological development and standards in many specific disciplines. NBS works with the technical leaders and managers throughout government and industry in performing its activities. The Institute for Computer Sciences and Technology, one of NBS's three major technical elements, has played a leading role in developing standards, guidelines and technical publications specifying cost-effective means for improving security in a variety of Federal and private sector applications where national security is not at stake. National security applications generally require more stringent safeguards

which are used on a case-by-case basis.

Computer security thus covers a spectrum of solutions which must be applied to a spectrum of problems. The problems range from accidental errors and omissions of people performing their authorized duties to high technology attacks on classified systems. The ICST program addresses the spectrum of problems and recommended solutions up to those related to classified computer systems. We feel that the administrative procedures and a majority of the technology comprising the common problem solutions are presently available. In certain areas implementation standards and guidelines are still needed even though the technology is available. Our program includes plans for performing research needed to solve several technical problems in specific application areas at the top of our problem spectrum. Our overall goal is to have a wide range of cost-effective solutions to be selected based on the results of a risk assessment. Automated solutions which are integrated into computers and terminals as standard features or standard options are desired in applying this needed technology.

I would like to specifically address the areas of interest detailed in your letter of invitation. I will outline our activities in computer and communications security; the generic vulnerabilities of computers and computer networks that are addressed by our technical activities; several areas of research necessary to support these activities; and some of the security technology being used in government and private sector applications.

## 3.1 General Computer Security Activities

To place our computer telecommunications security activities in context, I would like to present a synopsis of our range of computer security and risk management activities and then to focus on the telecommunications aspects. In each of the following areas of computer security, we have published, or are about to publish, documents containing technical information and related administration guidance for implementing and using this technology.

*RISK ASSESSMENT

Risk assessment is a procedure for estimating potential losses related to accidents or intentional misuse of ADP systems. The results of a risk assessment are used in selecting cost effective safeguards.

*CERTIFICATION AND ACCREDITATION

Certification is a procedure of evaluating the effectiveness of safeguards selected for a particular computer system. Accreditation is the process of approving the system for use.

*CONTINGENCY PLANNING

Contingency planning is the administrative preparation to assure continuity of ADP services should an unexpected event occur.

*SECURITY OF SMALL SYSTEMS

The widespread use of personal and professional computers and computer-based word processors has raised many questions regarding the security requirements and capabilities of small systems. We are investigating the security issues and technology of these systems.

*PERSONAL IDENTIFICATION

The fundamental requirement for controlling access to computer systems and networks is being able to accurately identify the authorized users. Over the past several years, we have investigated fingerprint readers, voice recognizers, automated human signature verifiers, hand geometry readers and palmprint readers. These devices rely on accurately differentiating among people based on a particular physical characteristic.

*PASSWORD USAGE

Passwords are the least expensive method of identifying computer users and, if properly implemented and used, provide a reasonable level of initial access control for a distributed computer system or network. We are completing a proposed standard on password usage which specifies ten factors and related security criteria that must be considered when designing and implementing a password system.

## 3.2 Specific Computer Communications Security Activities

The primary goal of the Institute's computer communications security activities is to encourage widespread availability of cost-effective telecommunications security technology for users throughout the government and private industry. Telecommunications security standards are necessary to assure that requested access from a terminal to a computer in any computer network is authorized, that the data being transmitted are not disclosed or modified without authorization, and that the terminal and the computer are mutually authenticated.

Our telecommunications security activities include developing

standards for assuring the security and integrity of computer networks being developed for use by government and private sector organizations which do not process national security information. Standards for Federal use are issued by the Department of Commerce as Federal Information Processing Standards (FIPS). We are also participating in the American National Standards Institute (ANSI) activities to develop voluntary standards for use throughout private industry. ANSI standards are adopted as Federal standards when they satisfy Federal requirements. Compatible Federal and ANSI standards will reduce the cost of commercial equipment meeting the standards because of the increased customer base and will allow secure telecommunications between Federal and private ADP organizations.

The Bureau's. Institute for Computer Sciences and Technology inititated a program in 1973 to establish a series of standards for assuring the integrity and security of computer networks. This cooperative program between government and industry has resulted in a number of activities that have resulted in Federal and ANSI compatible standards. The principal results of this program are:

*DATA ENCRYPTION STANDARD (DES)

In 1977, NBS published the Data Encryption Standard (DES) which specified a cryptographic algorithm for the protection of unclassified but sensitive computer data. This algorithm was developed in the private sector, submitted to the NBS in response to a public solicitation for such algorithms, and reviewed by the National Security Agency at the request of NBS.

The standard has been widely adopted, was published as ANSI standard X3.92-1981, and is recommended for use by the American Bankers Association for protecting electronic funds transfers.

*DES MODES OF OPERATION STANDARD

NBS published a FIPS on the Modes of Operation of the DES in 1980. This document specifies four modes of providing security to a variety of telecommunications applications, ranging from character oriented data transfer to protecting digital voice transmissions. ANSI published a standard specifying the same four modes of operation in 1983.

*DATA INTEGRITY STANDARD

Integrity is the assurance that data has not been modified, either accidentally or intentionally, without authorization. While integrity is important in all computer applications, it is especially important in financial transactions. A proposed Data Integrity Standard, scheduled for publication in 1984, can be used to put a cryptographic seal on data so that any unauthorized modification can be detected. The American Bankers Association, as Secretariat of ANSI activities on financial transactions, has published an ANSI standard for protecting the integrity of financial electronic funds transfers using this technique.

*OPEN SYSTEMS INTERCONNECTION (NETWORK) SECURITY

The open systems interconnection model of the International Organization of Standardization (ISO), is a conceptual architecture for communicating among a variety of information systems. The Institute has been active in ANSI activities developing integrity and security standards in this

internationally accepted computer communications model.

*USER ACCESS AUTHORIZATION

Once the identity of an authorized user of a computer system has been established, the system should control the user's further access to data and resources of the system. A guideline on how to establish access authorization requirements and to implement the necessary access control mechanisms is presently being developed.

## 4. Computer Communications Security Vulnerabilities and Countermeasures

The information processing age has brought us to the point where great quantities of information must be available at many locations. The information must be current, accurate and easily accessible. Computer networks, which are integrated systems of computers and digital telecommunications, provide the desired access to information. Examples of large scale information networks include: airline reservation systems; stock market information systems; and credit card verification systems. Scaled-down information networks called "electronic bulletin boards" allow widespread sharing of information on special interest subjects. The trend towards distributed processing, marked by the entrance of micro-computers and end-user computing, has emphasized the need for computer network security.

The general security requirements of computer networks can be summarized as follows:

*Availability - Assuring that the network is available to provide the desired access;

*Controlled Accessibility - Assuring that the network provides access only to authorized users performing authorized tasks;

*Integrity - Protection of data from unauthorized modification, insertion, deletion, or destruction;

*Privacy (Secrecy) - Protection of data from unauthorized disclosure;

*Traffic flow security - Assuring that the identities of the communicating users, the quantity of data communicated, and the time and duration of communication are protected.

These security requirements are based on a number of generic vulnerabilites of computer and communications networks. I would like to outline some of these generic vulnerabilities and discuss the technology that is available or being developed to counter many of the common security problems identified in existing systems and networks.

The news media have recently carried numerous stories about young "computer hackers" gaining unauthorized access to computers throughout the country. Our review of these accounts leads us to believe that the vulnerabilities which allowed the unauthorized access were in the personal identification and access authorization sub-systems. Much of the needed technology already exists, and if properly applied, would have prevented the success of these unauthorized accesses. Our highest priority in our computer security activities is to transfer this technology to manufacturers if electronic equipment is needed, to software developers if computer program enhancements are needed, and to users.

The trend to distributed, "user friendly" computer capability has

posed new problems for ADP managers. Telephone numbers which provide remote electronic access to computers are often published (e.g., for public "electronic bulletin boards"). Even unpublished computer telephone numbers can be "guessed" with known probability (1/10,000 if the exchange of the computer is known) or can be electronically searched (as depicted in the movie "Wargames"). The technology exists to have the "called" computer request the identification of the "calling" party, verify that this party is on the approved access list, break the original connection, and then call back to the correct location of the acceptable authorized user. Thus, a person attempting to "masquerade" as an authorized user (from an unauthorized location) can be prevented from gaining even initial access to the computer.

Once initial access to the computer is gained, only a "password" generally stands between the user and access to the system. Password systems, while potentially capable of providing good security in many applications, are vulnerable to many failures of human nature in users and managers. Commercial computer systems are generally delivered with an initial set of "default" passwords which are used by the system's operators and maintenance personnel. These "default" passwords are often not deleted or changed to locally generated passwords following installation. The local system is then vulnerable to easy access by anyone who has purchased an identical system or knows the easily remembered "default" passwords.

Users often select passwords that are too short or are associated

with something personal about the user (for ease of memorization). Sometimes the passwords are "memorized" by writing the password on a piece of paper and attaching the password to the terminal. NBS has published several documents on how to use password systems effectively and we are completing a Federal Information Processing Standard on Password Usage. This proposed standard requires specific security criteria to be met in all Federal ADP installations and suggests many ways that the system can provide automated methods of good password control. We believe that the specific vulnerabilities of password systems that were depicted in "Wargames" (i.e., using the name of a relative as a password and hiding a password in a "secret" location) and in the stories about "computer hackers" (i.e., not changing passwords following system installation) could not have been exploited if the technical and management provisions specified in the proposed Password Usage Standard had been followed.

If electronic access to the computer and access to the system are initially achieved, few systems have additional security provisions to monitor and control the activity of the user. The User Access Authorization guideline presently being completed discusses some of the needed access control provisions.

The following generic vulnerabilities of computers and communications networks must be countered:

*Browsing - unauthorized reading of data available to authorized users of the system;

*Unauthorized modification, destruction, insertion or deletion of data;

*Passive "wiretapping" - unauthorized reading of data during transmission;

*Active "wiretapping" - unauthorized modification of data during transmission;

*Control signal logging - unauthorized recording of the dial pulses or tones of telephone networks;

*"Piggy backing" - attaching a terminal of an unauthorized user to a communications connection being used by an authorized user;

*"Spoofing" - an unauthorized user or device pretending to be an authorized user or device.

Proper use of the Data Encryption Standard, the standard Modes of Operation of the DES, and a good cryptographic key management system will prevent the success of any attempt to exploit these generic vulnerabilities of computer networks.

5. Research in Computer and Communications Security

While much of the technology needed to protect systems exists today, the major research thrust in computer communications security should lie in integrating this security technology into existing and newly emerging applications areas such as:

*Network integrity and security in the ISO layered communications architecture;

*Cryptographic key management in computer telecommunications networks;

*Improved methods of personal identification for controlling access to computer networks;

*Integrity/security architectures of personal computers;

*Integrity/security protocols of transactions initiated from

home telephones or home computers;

*Methods for generating digital "signatures" on electronic messages, contracts, etc.;

*Methods for providing security to voice initiated computer transactions and to computer generated voice responses;

*Assessment of traffic flow security/privacy procedures on computer telecommunications networks.

Many computer communications applications being developed could utilize the results of research in these areas. They include:

*Home banking

*Home voting/polling

*Electronic mail: voice and data

*Home initiated purchasing transactions

*Electronic contract negotiation

*Digital signature notarization of contracts

*Remote office operation

*Computer software copyright protection

Research in the above areas will involve several technical disciplines. Personal identification technology must be investigated to determine what characteristics can be easily determined to distinguish one person from another. Computer, electronic and telephony technologies must be used in developing cost-effective methods of implementing the needed security provisions. Many of the specialty fields of mathematics must be used to develop and evaluate cryptographic methods for assuring adequate integrity and security. Inexpensive methods for assuring physical and electronic security for the devices implementing

computer and telecommunications security must be investigated.

6. Opportunities for Leadership in Computer and Communications Security

ICST has played a significant leadership role in the development of computer security technology, management procedures, standards and guidelines. The thrust of this role has been through the Federal and ANSI standards development activities. To support these standards development activities, the Institute has performed applied research and development in computer security technology, identified generic requirements for computer security, prepared technical specifications of proposed standards and assisted various organizations in utilizing the standards after adoption.

We have served a technology transfer role between the public and private sectors. Our activities include identifying the needs for security technology by both industry and Federal computer users and then stimulating the sharing of technical information among these users. We sponsor, or participate in, numerous conferences, workshops and meetings on computer security. We encourage the development and use of off-the-shelf automated solutions to security problems when such solutions are known and cost-effective. We develop standards through participation in, and leadership of, voluntary industry standards activities.

NBS works closely with other Federal organizations, both in developing security technology and in transfering the technology. We have worked with the National Security Agency in developing computer communications security standards. We have assisted the

DOD Computer Security Center in transferring "Trusted System" technology to users in government and the private sector. We have participated with the National Communications System and the General Services Administration in developing Federal Standards for Telecommunications. We have provided technical inputs to the Office of Management and Budget on its Circular A-71, Transmittal Memorandum Number 1. We have cosponsored several workshops on computer security evaluation with the General Accounting Office. We have presented computer security conferences with the Department of Defense, the Office of Personnel Management, the Department of Agriculture and the Federal ADP Users Group. Many lectures on computer security have been given at the DOD Computer Institute and at meetings sponsored by the Department of Energy, Department of Health and Human Services and at the National Aeronautical and Space Administration.

7. Summary

I have summarized only the highlights of the computer and communications security activities at the National Bureau of Standards, concentrating on the activities specified in your letter of invitation to appear before this Subcommittee. I have mentioned our relationships with some of the Federal organizations having a lead role in computer security. We also work very closely with private industry and state governments in need of the technology and information we have available.

Thank you for inviting us to appear before you. We will be happy to answer any questions at this time.

JOHN W. LYONS

Date of Birth: November 5, 1930

Birthplace: Reading, Massachusetts

Education: Degrees

Harvard University, A.B., Chemistry
1952
Washington University, A.M., Physical Chemistry
1963
Washington University, Ph.D., Physical Chemistry
1964

Positions:

Acting Deputy Director
National Bureau of Standards

Dr. Lyons was appointed in April 1983 as Acting Deputy Director of the National Bureau of Standards. In this position, Dr. Lyons is responsible for the efficient execution of the Bureau's operational programs. He coordinates, monitors, and assesses progress of all NBS technical projects, and of the supporting services.

(NBS is the Nation's central reference laboratory, providing measurement methods, standards, and data that are used in industry, commerce, government, and universities. Bureau headquarters are located in Gaithersburg, Maryland, with a second laboratory at Boulder, Colorado. Total staff numbers about 3,200).

As Director of the National Engineering Laboratory from December 1977 until April 1983, Dr. Lyons was responsible for NBS's research in applied mathematics, building technology, electronics and electrical engineering, energy conservation, engineering standards development, fire, manufacturing engineering and chemical engineering.

Dr. Lyons was Director of the NBS Center for Fire Research until December 18, 1977, and was responsible for providing scientific and technical knowledge applicable to the prevention and control of fires.

Dr. Lyons served in various research and development positions at the Monsanto Company from 1955 to 1973. He specialized in the chemistry and uses of phosphorus-based chemicals including fire retardants. He served from 1971 to 1973 as a member of the ad hoc panel of fire research, a National Academy of Sciences evaluation panel for the National Bureau of Standards.

Dr. Lyons is author of two books: Viscosity and Flow Measurements and The Chemistry and Uses of Fire Retardants. He has contributed chapters to five other books and has written numerous papers and articles on technical or research topics. His early research interest was the physical chemistry of polyelectrolyte solutions, especially formation of complexes with metal ions. This work emphasized the behavior of inorganic polyphosphates and desoxy ribonucleic acid (DNA).

Dr. Lyons is a Fellow of the American Association for the Advancement of Science, Fellow of the Washington Academy of Science, member of the American Chemical Society (past chairman of the St. Louis Section), member of the American Institute of Chemical Engineers and member of Sigma Xi. He serves on the Advisory Committee for Engineering, National Science Foundation; Advisory Council, College of Engineering, University of Maryland; Board of Directors, National Fire Protection Association. He is serving on a special committee of the Maryland State Board for Higher Education to study the needs for engineering education. He was chairman of the Products Research Committee (1974-1979), a nine-member charitable trust administering a $5M research fund on fire research; co-chairman of the US-Japan Natural Resources Panel of Fire Research (1975-1978). He received the Presidential Management Improvement Award in 1977 and the U.S. Department of Commerce Gold Medal, also in 1977. In 1981 he received the Presidential Rank Award of Distinguish Executive.

4/20/83