SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

U. S. HOUSE OF REPRESENTATIVES

OCTOBER 17, 1983

TELECOMMUNICATIONS SECURITY AND PRIVACY

WITNESSES

NSA
WITNESS: Mr. Melville H. Klein
Director, DoD Computer Security Center

OBSERVERS: Colonel Roger R. Schell
Deputy Director, DoD Computer Security Center

Mr. James T. Tippett
Executive, DoD Computer Security Center

Mr. Charles J. Zeman
Legislative Affairs Office

STATEMENT ON

TELECOMMUNICATIONS SECURITY AND PRIVACY

PRESENTED BY

MR. MELVILLE H. KLEIN

DIRECTOR, DOD COMPUTER SECURITY CENTER

NATIONAL SECURITY AGENCY

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

U. S. HOUSE OF REPRESENTATIVES

ON

OCTOBER 17, 1983

INTRODUCTION

Mr. Chairman and members of the Subcommittee, I am pleased to have this opportunity to appear before you today to address NSA research activities relevant to your examination of security and privacy in the civil community.

Since the activities of the NSA are for the most part of a classified nature, my remarks are directed at those unclassified aspects of computer and telecommunications protection that can influence the directions taken outside the national security arena.

Over the past decade interest in information protection and privacy has spread with the rapid and pervasive use of computers in almost every facet of our every day lives. Efforts to counter the threats to privacy of citizens and the confidentiality of business and non-national security government information were undertaken by the private sector and civil agencies (NBS). I would like to address how these activities have benefited from the computer security and communications security research programs at NSA. First I will review the origin, purpose and operation of the DoD Computer Security Center.

PURPOSE AND OPERATION OF THE DOD COMPUTER SECURITY CENTER

The Center is an outgrowth of the DoD Computer Security Initiatives Consortium formed in 1978 under the Assistant Secretary of Defense for Command, Control and Intelligence to coordinate on-going computer security research within the Department. In January of 1981, the Deputy Secretary of Defense assigned to the Director of NSA, certain responsibilities for

computer security within the DoD. The Center began operation in June of 1981 as a separate and unique entity within the NSA. Its implementing directive (DoD Directive 5215.1) was issued by the Deputy Secretary of Defense in October 1982.

The Center has a five-pronged mission. First, to develop and promulgate uniform computer security criteria and standards that will lead to widespread availability of "trusted" products from computer vendors (Computer Security Evaluation Criteria). Second, to evaluate vendor products against these criteria and publish a listing for general use (Evaluated Products List). Third, to assist defense acquisition authorities in specifying and certifying trusted products in defense systems. Fourth, in conjunction with the DoD components to formulate and sponsor research to improve the state-of-the-art in trusted computer technology and verification tools and methodologies. And, lastly, to strengthen the computer security awareness and competence in the national security establishment through specialized training, seminars, information dissemination and ready access to evaluation resources.

By "trusted" computer systems, I mean those that employ sufficient hardware and software measures to allow their use to simultaneously process a range of sensitive or classified information (e.g. Confidential through Top Secret) for a diverse set of users without violating access privileges. This is a critical function in modern defense operations, i.e., reliably

handling sensitive data in electronic form in a time-sensitive manner. Similar situations exist in the civil community regarding access to proprietary data in commerce and to government records on citizens to which trusted computer technology could also be employed.

NSA ACTIVITIES IN THE COMMUNICATIONS AREA THAT AFFECT THE CIVIL COMMUNITY

I would now like to discuss our participation in the development of the Data Encryption Standard (DES). The DES was proposed by the National Bureau of Standards as a means for protecting unclassified Government data in computers. The cryptographic algorithm was derived as a result of a 1973 solicitation to the Industrial Community. The algorithm selected was one proposed by the International Business Machines Corporation. It was extensively analyzed in several public workshops as well as by the National Security Agency at the request of the NBS. Admiral B. R. Inman, then Director of NSA, issued this endorsement of DES in a June 1978 letter: "...NSA fully certified the Data Encryption Standard implemented by the Department of Commerce in July 1977, as a standard for the encryption of unclassified computer data...NSA will now endorse the use of the DES for encryption of unclassified national security-related information..."

Additional efforts are underway between the Government and the industrial sector to introduce DES products to meet Government needs for the protection of unclassified information.

Standards have now been issued for this purpose by the Federal Government (Federal Standard 1027). Domestic manufacturers may now submit DES-based equipments to NSA for evaluation against this standard. NSA will formally endorse those equipments that meet FS1027. This program is operating very successfully with over 20 manufacturers of DES products participating. A direct result of this process is a rapidly growing set of endorsed commercially available equipments available in the U.S. to meet both national security related and private sector telecommunications protection needs.

VOLUNTARY REVIEW OF RESEARCH PAPER

In 1979 Admiral Inman spoke out publicly about articles and monographs written on cryptography. While he recognized the growing need for cryptography in the public sector, he believed that uncontrolled publication of cryptographic papers could be harmful to the foreign intelligence and COMSEC missions of the NSA. In response to this concern, the American Council of Education, through a National Science Foundation grant, sponsored a study group to review the issues.

That Group, the Public Cryptography Study Group, was composed of members of various professional organizations and technical societies (e.g., IEEE and its Association for Computing Machinery) and NSA's General Counsel. In 1981 the Group issued a report calling for a system for voluntary pre-publication review. NSA, in complying with the recommendations of the

report, issued an invitation to authors, Professional Societies and publications to submit manuscripts for pre-publication review. This invitation was also placed in the Federal Register in March 1982. The Study Group recommended, and NSA established, an advisory committee to resolve disputes that might arise between NSA and authors over the security implications of a paper. The Committee is composed of three members recommended by the President's Science Advisor and two by the Director, NSA. There has never been a need for it to meet.

It is important to point out that this is a voluntary process. We at NSA believe it is working to the mutual satisfaction of all parties. We have reviewed over 100 papers. Our stated objective is to staff and respond to these papers within 30 days. We have met this goal on over 90% of the cases.

Only a handful have raised some security concerns with our reviewers. Several of those were resolved with only minor modification to the text. We have asked that three papers not be published. In all of these situations the authors were most cooperative.

There was concern by some in the A.C.E. Study Group that a review procedure would have a "chilling effect" on research. I don't believe this has been the case. Our reviews are timely and responsive to the author's concerns.

Needs for Future Research in OCREAE PROGRAM

The OCREAE program is a small grant program operated by NSA to provide University researchers support for carrying out basic research related to Cryptology. This program has had beneficial impact on the NSA-academe relationship in that it has provided an excellent liaison mechanism between the academics and NSA researchers, it has produced quality research of potential interest to NSA, and it has helped create a source of talented young scientists for prospective recruitment.

Needs for Future Computer Security Research

Some examples of the types of research needed in the future that will benefit computer security are in the areas of artificial intelligence, security modeling, proofs of correctness, and secure operating systems. This research is being performed by the government, academia, and private industry, and is expected to expand not only to meet our needs but those of others in software reliability and supercomputer design.

Needs for Future Communications Security Research

The rapid expansion in the use of communications throughout the government, and the many new types of systems being introduced, presents a significant challenge to the ability to provide adequate protection technology in the future. Cellular radio, electronic mail, local area networks, and direct termination systems are but a few examples of the new

communications technology which will find increased use in both the Government and private sectors. The amount of research and development resources directed at meeting these challenges in the private sector needs to be expanded.

Areas in Which NSA Can Make Contributions to Our Society's General Need for Security and Privacy in the Future

We believe that NSA can continue to make significant contributions to our society's general need for security and privacy through its programs of security awareness, good security practice and administrative controls, and continued selective technology transfer from our on-going communications security research to the private and public sectors. We are placing emphasis on the fact that much of the computer security technology of interest to defense is also applicable to a much larger public and private market in privacy of electronic records, computer fraud, crime and abuse, and as a counter to potential terrorist activity. We are thus encouraging computer vendors to apply this technology to their future computer products so that we in DoD can also reap the benefits.

This concludes my statement. I will be pleased to try and answer any questions that you may have.