ILLEGIB

KEYNOTE ADDRESS

COMPUTER SECURITY INITIATIVE

August 10, 1981

It is a pleasure to welcome you to this Seminar and to speak briefly with you about computer security, the recent developments within the Department of Defense and the Intelligence Community and the challenges that lie ahead.

As Dr. Gerald P. Dinneen, former Assistant Secretary of Defense for C^3I defined at the first of these Seminars two years ago, a "trusted" computer system is one with sufficient hardware and software integrity to allow its use for the simultaneous processing of multiple levels of classified or sensitive information.

The need for trusted computer systems is very real and growing rapidly. Factors influencing this need are:

- the growing use of automated information handling systems throughout the DoD and the Intelligence Community and in particular the linking of these systems into major networks;
- increasing requirements for controlling access to compartmented and sensitive information;
- the requirement for broader dissemination of information both within and beyond the community;
- growing difficulties with obtaining required numbers of cleared personnel, both military and civilian.

Despite continuing internal efforts to develop special purpose trusted systems for unique needs, we already rely very heavily on the products of the computer industry to meet our information processing requirements, and this

dependence will continue to grow significantly in the future. It is therefore very gratifying to observe the progress being made by the computer industry in applying computer security technology as represented by the industry presentations at this and the previous Seminars.

It is very important, also, that the Department of Defense and the Intelligence Community develop sufficient expertise to be able to evaluate the integrity of computer software and systems developed by industry and government, and that we be able to determine suitable physical and administrative environments for their application. We have had scattered efforts over the past several years to evaluate specfic systems for specific installations. But these efforts have always been more or less ad hoc, and because of the extensive technical background required, expensive to carry out.

I am very pleased therefore to announce today the establishment of a Computer Security Technical Evaluation Center for the Department of Defense and the Intelligence Community at the National Security Agency. Last fall, as Director of NSA, I enthusiastically endorsed the establishment of this Center at NSA as a new and separate function. I am very pleased with the progress being made in setting up the Center and I remain strongly committed to its success.

I would like to make several observations about the Center and some of its relationships:

- Because the private sector computer manufacturing community is the primary source of ADP systems, the Center's role will be to work with the manufacturers, deriving as much system integrity as possible from industry developed systems. This is a rather sharp contrast to the NSA's more traditional communications security role where the government has the dominant technical role.

- The Center will have a difficult task developing procedures which assure protection of sensitive portions of a system which the government does not own. Simply classifying security related portions of a system built by industry won't work since the government represents such a small portion of the overall market that the manufacturers may well decide not to sell to the government rather than accepting the limitations imposed by classification. This, in the end, might lead to a highly undesirable situation where private sector users (e.g., banks, insurance companies) have higher integrity systems than the government.
- But sensitive portions of systems and the known vulnerabilities that remain must be protected, in the interests of both the government and the manufacturers. It is quite likely therefore that the most sensitive portions of the government's analyses will be both classified and proprietary to the manufacturer. Careful, reasoned interaction between the government and industry will be needed to work out suitable working relationships.
- The Center will act in the interests and for the benefit of the Department of Defense and the Intelligence Community. Its evaluation will not be intended for use by other than the DoD. It will not make general product endorsements. But as with the Qualified Products List procedures (as prescribed in the DoD Defense Acquisition Regulations), the relative merit of a system in the hierarchy of evaluated products may be available publicly in order to provide incentive and encouragement for manufacturers to develop trusted systems and private sector users to employ them.

- Because of the wide range of sensitive environments that exist for information systems (ranging from privacy applications to compartmentation within the Intelligence Community, and from adjacent security levels (e.g., Secret and Top Secret) to full multi-level systems with Intelligence users and uncleared users), it will be vital for the Evaluated Products List to offer a range of technical categories and appropriate environments for specific systems. The approach of establishing levels of technical integrity which has evolved from the work of the Computer Security Initiative indicates the kinds of distinctions which will be made in evaluating systems. A range of suitable environments is possible with trusted systems because the security accreditation of ADP systems depends upon all of the aspects of the total system. The accreditation of a system to serve users cleared at both the Secret and the Top Secret level is not as difficult a problem as extending the use of such a system to uncleared users as well. The Department of Defense is now using Multics in such a limited environment serving both Secret and Top Secret cleared users. The Evaluated Products List should provide guidelines for implementing this type of operation where sufficient technical integrity of software products can be demonstrated.
- Finally, I would like to say that the establishment of an Evaluation Center, important as it is, must not be viewed as providing by itself the long sought answer to the computer security problem. Within the Department of Defense and the Intelligence Community, system builders will have to become aware of and properly employ the procedures for development of trusted system applications. The Services and Defense

Agencies are being encouraged to establish or enhance their own technical security test and evaluation capabilities to ensure widespread use and availability of trusted computer systems. The computer manufacturing community must work closely with the Center and these Service organizations to ensure that reasonable products are available for use in sensitive applications.

In conclusion, I would like to restate my awareness of the importance of this problem area, my enthusiasm for the establishment of the Evaluation Center, and my deep and continuing interest in its success. I encourage you to participate fully in this Seminar, ask the tough questions, learn all you can, and then go out and apply what you have learned so that we may all have trustworthy computers in the very near future.

PROCEEDINGS

OF THE

FOURTH SEMINAR
ON THE
DOD COMPUTER SECURITY
INITIATIVE

NATIONAL BUREAU OF STANDARDS
GAITHERSBURG, MARYLAND

AUGUST 10 - 12, 1981

KEYNOTE ADDRESS

COMPUTER SECURITY INITIATIVE

Admiral Bobby Inman
Deputy Director of Central Intelligence
Washington, D.C.

It is a pleasure to welcome you to this Seminar and to speak briefly with you about computer security, the recent developments within the Department of Defense and the Intelligence Community and the challenges that lie ahead.

As Dr. Gerald P. Dinneen, former Assistant Secretary of Defense for C^3I defined at the first of these Seminars two years ago, a "trusted" computer system is one with sufficient hardware and software integrity to allow its use for the simultaneous processing of multiple levels of classified or sensitive information.

The need for trusted computer systems is very real and growing rapidly. Factors influencing this need are:

- the growing use of automated information handling systems throughout the DoD and the Intelligence Community and in particular the linking of these systems into major networks;
- increasing requirements for controlling access to compartmented and sensitive information;
- the requirement for broader dissemination of information both within and beyond the community;
- growing difficulties with obtaining required numbers of cleared personnel, both military and civilian.

Despite continuing internal efforts to develop special purpose trusted systems for unique needs, we already rely very heavily on the products of the computer industry to meet our information processing requirements, and this

dependence will continue to grow significantly in the future. It is therefore very gratifying to observe the progress being made by the computer industry in applying computer security technology as represented by the industry presentations at this and the previous Seminars.

It is very important, also, that the Department of Defense and the Intelligence Community develop sufficient expertise to be able to evaluate the integrity of computer software and systems developed by industry and government, and that we be able to determine suitable physical and administrative environments for their application. We have had scattered efforts over the past several years to evaluate specfic systems for specific installations. But these efforts have always been more or less ad hoc, and because of the extensive technical background required, expensive to carry out.

I am very pleased therefore to announce today the establishment of a Computer Security Technical Evaluation Center for the Department of Defense and the Intelligence Community at the National Security Agency. Last fall, as Director of NSA, I enthusiastically endorsed the establishment of this Center at NSA as a new and separate function. I am very pleased with the progress being made in setting up the Center and I remain strongly committed to its success.

I would like to make several observations about the Center and some of its relationships:

- Because the private sector computer manufacturing community is the primary source of ADP systems, the Center's role will be to work with the manufacturers, deriving as much system integrity as possible from industry developed systems. This is a rather sharp contrast to the NSA's more traditional communications security role where the government has the dominant technical role.

- The Center will have a difficult task developing procedures which assure protection of sensitive portions of a system which the government does not own. Simply classifying security related portions of a system built by industry won't work since the government represents such a small portion of the overall market that the manufacturers may well decide not to sell to the government rather than accepting the limitations imposed by classification. This, in the end, might lead to a highly undesirable situation where private sector users (e.g., banks, insurance companies) have higher integrity systems than the government.
- But sensitive portions of systems and the known vulnerabilities that remain must be protected, in the interests of both the government and the manufacturers. It is quite likely therefore that the most sensitive portions of the government's analyses will be both classified and proprietary to the manufacturer. Careful, reasoned interaction between the government and industry will be needed to work out suitable working relationships.
- The Center will act in the interests and for the benefit of the Department of Defense and the Intelligence Community. Its evaluation will not be intended for use by other than the DoD. It will not make general product endorsements. But as with the Qualified Products List procedures (as prescribed in the DoD Defense Acquisition Regulations), the relative merit of a system in the hierarchy of evaluated products may be available publicly in order to provide incentive and encouragement for manufacturers to develop trusted systems and private sector users to employ them.

- Because of the wide range of sensitive environments that exist for information systems (ranging from privacy applications to compartmentation within the Intelligence Community, and from adjacent security levels (e.g., Secret and Top Secret) to full multi-level systems with Intelligence users and uncleared users), it will be vital for the Evaluated Products List to offer a range of technical categories and appropriate environments for specific systems. The approach of establishing levels of technical integrity which has evolved from the work of the Computer Security Initiative indicates the kinds of distinctions which will be made in evaluating systems. A range of suitable environments is possible with trusted systems because the security accreditation of ADP systems depends upon all of the aspects of the total system. The accreditation of a system to serve users cleared at both the Secret and the Top Secret level is not as difficult a problem as extending the use of such a system to uncleared users as well. The Department of Defense is now using Multics in such a limited environment serving both Secret and Top Secret cleared users. The Evaluated Products List should provide guidelines for implementing this type of operation where sufficient technical integrity of software products can be demonstrated.
- Finally, I would like to say that the establishment of an Evaluation Center, important as it is, must not be viewed as providing by itself the long sought answer to the computer security problem. Within the Department of Defense and the Intelligence Community, system builders will have to become aware of and properly employ the procedures for development of trusted system applications. The Services and Defense

Agencies are being encouraged to establish or enhance their own technical security test and evaluation capabilities to ensure widespread use and availability of trusted computer systems. The computer manufacturing community must work closely with the Center and these Service organizations to ensure that reasonable products are available for use in sensitive applications.

In conclusion, I would like to restate my awareness of the importance of this problem area, my enthusiasm for the establishment of the Evaluation Center, and my deep and continuing interest in its success. I encourage you to participate fully in this Seminar, ask the tough questions, learn all you can, and then go out and apply what you have learned so that we may all have trustworthy computers in the very near future.