October 25, 1982
NUMBER 5215.1

Department of Defense Directive

SUBJECT: Computer Security Evaluation Center

References: (a) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972
(b) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by reference (a)
(c) OMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," July 27, 1978
(d) through (m), see enclosure 1

A. PURPOSE

This Directive establishes the DoD Computer Security Evaluation Center (CSEC), provides policy, and assigns responsibilities for the technical evaluation of computer system and network security, and related technical research.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. Its provisions govern the conduct of trusted computer system evaluation and technical research activities within the Department of Defense in support of overall computer system security evaluation and approval responsibilities assigned to the DoD Components under references (a), (b), (c), DoD Directives 5220.22, and 5400.11 (references (d) and (e)).

C. DEFINITIONS

1. Sensitive/Classified Information. Sensitive information as defined in reference (c), and classified information as defined in DoD 5200.1-R (reference (f)).

2. A Trusted Computer System. Employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

3. Generic Computer Security Research and Development. Has potential application over a very broad, generalized basis, and includes experimental exploration and development of feasible and potentially useful technology, reponsive to a broad class of computer security needs.

D. POLICY

1. It is DoD policy to encourage the easy availability of trusted computer systems. The establishment of the DoD CSEC, the consolidation of generic computer security research and development (R&D), the evaluation of computer security systems and the establishment of an Evaluated Products List (EPL) are designed to further this objective.

2. The DoD Consolidated Computer Security Program (CCSP) shall include resources for the operation of the CSEC and for generic computer security R&D activities in support of DoD Components. The DoD Components are responsible for DoD Component security research, development, test, and evaluation (RDT&E) efforts and application-dependent research and development for specific DoD Component systems.

3. The activities and products of the CSEC, including technical advice and support, shall complement the established responsibilities of DoD Components relating to the overall policy, security evaluation, and approval of computer systems as prescribed in DoD Directive 5200.28, DoD 5200.28-M, OMB Circular A-71, Directives 5220.22 and 5400.11 (references (a), (b), (c), (d), and (e)), for the processing, use, and production of sensitive and classified information.

4. The EPL is not intended to replace prescribed procurement practices in the acquisition of computers and computer services. The CSEC and EPL are established to assist procuring activities in evaluating available products; computer products or services will not be rejected on the basis that the product or service is not on an EPL.

E. PROCEDURES

Precedures for consolidated technical research are at enclosure 2.

F. RESPONSIBILITIES

1. The Under Secretary of Defense for Research and Engineering (USDR&E), or his designee, shall:

a. Provide overall policy direction, guidance, and management oversight for the CSEC in coordination with the Deputy Under Secretary of Defense (Policy) (DUSD(P)) and the Assistant Secretary of Defense (Comptroller) (ASD(C)).

b. Establish a steering committee composed of representatives of DoD Components to review center activities and recommend future directions.

c. In coordination with the Deputy Assistant Secretary of Defense (Policy) (DUSD(P)) and the Assistant Secretary of Defense (Comptroller) (ASD(C)) represent the Secretary of Defense with other government agencies, foreign

governments, the North Atlantic Treaty Organization (NATO), and to the extent permitted, industry, in trusted computer system evaluation policy matters. Enter into agreements, if appropriate, consistent with National Disclosure Policy (reference (g)), with other government agencies, foreign governments, and NATO.

d. Establish an information exchange forum on computer security matters among DoD Components.

2. The Director, National Security Agency (NSA), in cooperation with the USDR&E, shall:

a. Establish and operate the CSEC as a separate and unique entity within the NSA.

b. Program and budget for CCSP support resources under procedures prescribed for the DoD planning, programing, and budgeting processes, but excluding National Foreign Intelligence Program funds controlled by the Director of Central Intelligence (DCI) under E.O. 12333 (reference (h)).

c. Appoint a Director to manage the CSEC who shall:

(1) Establish and maintain technical standards and criteria for the evaluation of trusted computer systems that can be incorporated readily into the DoD Component life-cycle management process (DoD Directives 7920.1, 5000.29, 5000.1, 5000.2 (references (i),(k),(l),(m)). Provide assistance to the DoD Components in the application of the technical standards and criteria.

(2) Conduct evaluations of selected industry and government-developed trusted computer systems against these criteria. Request for evaluation of government-developed computer systems will be from the DoD Component responsible for the security of the system to be evaluated.

(3) Maintain and publish an EPL of the selected industry and government-developed trusted computer systems that is suitable for use by the DoD Components.

(4) Conduct and sponsor R&D for trusted computer systems, and for computer security evaluation and verification methods and techniques.

(5) Provide assistance to the DoD Components by conducting evaluations of selected DoD and DoD contractor trusted computer systems in response to requests from the DoD Component responsible for the security of the computer system to be evaluated.

(6) Serve as the focal point for technical matters concerning the use of trusted computer systems for the protection of sensitive and classified information and, in conjunction with DoD Component computer security test and evaluation activities, provide technical advice to the DoD Components.

(7) Sponsor DoD Component cooperative efforts, public seminars, and workshops for the purpose of technology transfer.

(8) Serve as the DoD principal technical point of contact on trusted computer system matters with other government agencies, industry, foreign governments, and NATO under the policy guidance of the USDR&E or designee, consistent with National Disclosure Policy (reference (g)).

(9) Develop and maintain the CCSP, in conjunction with DoD Components. (See procedures at enclosure 2).

3. Heads of DoD Components, or designees, shall:

a. Make maximum use of the standards, technical criteria, and evaluations promulgated by the CSEC in meeting their responsibilities for overall automatic data processing (ADP) system security evaluation, approval, and maintenance as set forth in DoD Directive 5200.28, DoD 5200.28-M, DoD Directives 5220.22, and 5400.11 (references (a), (b), (d), and (e)).

b. Establish overall ADP security policy for specific types of sensitive and classified information under their security cognizance, and prescribe the security procedures and constraints appropriate for the classes of trusted computer systems as defined in the EPL.

c. Designate central DoD Component focal points for interaction with the CSEC in the development of Component trusted computer systems.

d. Formulate jointly the CCSP and manage directly the execution of their respective portions of the CCSP in accordance with enclosure 2.

e. Conduct RDT&E to meet specific operational needs identified by Component requirements.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing document to the Under Secretary of Defense for Research and Engineering within 120 days.

Frank C. Carlucci
Deputy Secretary of Defense

Enclosures - 2
1. References
2. Summary of Procedures for Consolidated Technical Research

REFERENCES, continued

(d) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
(e) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
(f) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
(g) DoD Instruction 5230.17, "Procedures and Standards for Disclosure of Military Information to Foreign Activities," August 17, 1979
(h) Executive Order 12333, "United States Intelligence Activities" December 4, 1981
(i) DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS)," October 17, 1978
(j) DoD Directive 7200.1, "Administrative Control of Appropriations," November 15, 1978
(k) DoD Directive 5000.29, "Management of Computer Resources in Major Defense Systems," April 26, 1976
(l) DoD Directive 5000.1, "Major Systems Acquisition," March 9, 1982
(m) DoD Directive 5000.2, "Major Systems Acquisition Process," March 19, 1980

PROCEDURES FOR CONSOLIDATED TECHNICAL RESEARCH

This establishes the procedures for developing the generic computer security R&D portion of the CCSP, as defined in subsection C.3. of this Directive. Portions of the CCSP relating solely to the operations of the CSEC are not included in this summary.

1. Under paragraph F.2.b. of this Directive, the Director, NSA, shall issue a data call for each fiscal year to the DoD Components for the CCSP. The data call shall request identification of major tasks and milestones for that fiscal year.

2. DoD Components shall submit to NSA their proposed projects for generic computer security R&D in the format prescribed. This shall include a program-quality technical description, cost estimates, and recommendation for the execution responsibility, namely, the submitting Component, another Component, or the CSEC. The CSEC similarly shall prepare its own proposals.

3. The CSEC shall convene the technical review group (TRG) composed of an identified principal from each DoD Component with participation by the working level engineering, scientific, communications and data processing personnel of DoD Components and the CSEC. The purpose and function of this group is to review the Component submissions for redundancies, completeness, and resource requirements, and to determine initial priorities. The TRG deliberations are directed toward an understanding and agreement among all principals of the nature and scope of the proposed CCSP research and development projects.

4. The CSEC shall compile the TRG-reviewed projects and provide the DoD Components a copy of the draft program for review and comment.

5. The Director, CSEC, shall chair the program working group (PWG) which is composed of a principal from each DoD Component. The function of the PWG is to review and refine the priorities for the generic security R&D portion of the CCSP under published OSD guidance. The PWG shall recommend the generic computer security R&D program to the Director, NSA. The CSEC shall prepare the draft consolidated computer security R&D program and provide the Components a copy for review and comment.

6. The Director, NSA, shall chair the program manager's review group (PMRG) consisting of representatives from DoD Components, including the Deputy Assistant Secretary of Defense (Communications, Command, Control, and Intelligence) and the Deputy Assistant Secretary of Defense (Research and Advanced Technology) as members, with additional observers, as appropriate. A formal briefing on the overall CCSP shall be presented to the Director and this group.

7. The Director, NSA, shall approve the CCSP after considering the changes or modifications suggested by this review group. This shall constitute the basis for the CCSP portion of the NSA Program Objectives Memorandum (POM) submission.

8. Acting upon published guidance and based on the approved CCSP, NSA shall make the budget submission for the CCSP. The CSEC shall distribute the CCSP portion of the NSA POM submission to the DoD Components.

9. Before anticipated appropriation, the PWG shall refine further priorities, confirm execution responsibilities, and identify possible candidates in the event of program reductions. These actions shall be the basis for suballocation of funding.

10. Following receipt of obligational authority, NSA shall suballocate CCSP funds to DoD Components for their approved tasks under DoD Directive 7200.1 (reference (j)). The suballocation process requires that each DoD Component provide to NSA by the 15th of each month a status report of commitments and obligations of the CCSP funds.