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.

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.

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.