e. For DIS to fulfill its responsibilities under DoD 5220.22–R and the Privacy Act of 1974 all inquiries conducted in its behalf must be set forth in an ROI for the permanent file, whether the case is completed, terminated early, or referred to another agency.

10. Referral

A case may require premature closing at any time after receipt of the DD Form 1879 by the investigative component if the information accompanying the request, or that which is later developed, is outside DIS jurisdiction. For example, alleged violations of law, a counterintelligence matter, or actual coercion/influence in a hostage situation (see paragraph 4.b. of this Appendix) must be referred to the appropriate agency, and DIS involvement terminated. The requester will be informed by letter or indorsement to the DD Form 1879 of the information developed that, due to jurisdictional consideration, the case was referred to (fill in appropriate address) and that the DIS case is closed. The agency to which referral was made and PIC will be furnished with the results of all investigations conducted under DIS auspices. DIS, however, has an interest in the referral agency's actions and no information should be solicited from that agency.

APPENDIX J TO PART 154—ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS

OMB Circular A–71 (and Transmittal Memo #B1), July 1978 OMB Circular A–130, December 12, 1985, and FPM Letter 732, November 14, 1978 contain the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating ADP and ADP related positions. This policy is outlined below:

ADP Position Categories

1. Critical-Sensitive Positions

ADP-I positions. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

2. Noncritical-Sensitive Positions

ADP-II positions. Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

3. Nonsensitive Positions

ADP-III positions. All other positions involved in computer activities.

In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the agency's judgement as to the unique characteristics of the system or the safeguards protecting the system.

Criteria for Designating Positions

Three categories have been established for designating computer and computer-related positions—ADP-I, ADP-II, and ADP-III. Specific criteria for assigning positions to one of these categories is as follows:

Category	Criteria
ADP-I	Responsibility or the development and administration of agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.
	Significant involvement in life-critical or mission-critical systems.
	Significant involvement in life-critical or mission-critical systems.
	Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
	Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the ADP-I category to ensure the integrity of the system.
	Positions involving *major* responsibility for the direction planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
	Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.
ADP-II	Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP-I category, includes, but is not limited to:
	(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

Category	Criteria
	(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP-I positions.
ADP-III	All other positions involved in Federal computer activities.

PART 155—DEFENSE INDUSTRIAL PERSONNEL SECURITY CLEARANCE PROGRAM

Sec.
155.1 Purpose.
155.2 Applicability and scope.
155.3 Definitions.
155.4 Policy.
155.5 Responsibilities.
155.6 Procedures.

APPENDIX A TO PART 155—ADDITIONAL PROCEDURAL GUIDANCE

AUTHORITY: E.O. 10865, 3 CFR 1959–1963 Comp., p. 398, as amended by E.O. 10909, 3 CFR 1959–1963 Comp., p. 437; E.O. 11382, 3 CFR 1966–1970 Comp., p. 690; and E.O. 12829, 3 CFR 1993 Comp., p. 570.

SOURCE: 57 FR 5383, Feb. 14, 1992, unless otherwise noted.

§ 155.1 Purpose.

This part updates policy, responsibilities, and procedures of the Defense Industrial Personnel Security Clearance Review Program implementing E.O. 10865, as amended.

[57 FR 5383, Feb. 14, 1992, as amended at 59 FR 48565, Sept. 22, 1994]

§ 155.2 Applicability and scope.

This part:

(a) Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Inspector General of the Department of Defense (IG, DoD), and the Defense Agencies (hereafter referred to collectively as ''the DoD Components'').

(b) By mutual agreement, also extends to other Federal Agencies that include:

(1) Department of Agriculture.

(2) Department of Commerce.

(3) Department of Interior.

(4) Department of Justice.

(5) Department of Labor.

(6) Department of State.

(7) Department of Transportation.

(8) Department of Treasury.

(9) Environmental Protection Agency.

(10) Federal Emergency Management Agency.

(11) Federal Reserve System.

(12) General Accounting Office.

(13) General Services Administration.

(14) National Aeronautics and Space Administration.

(15) National Science Foundation.

(16) Small Business Administration.

(17) United States Arms Control and Disarmament Agency.

(18) United States Information Agency.

(19) United States International Trade Commission.

(20) United States Trade Representative.

(c) Applies to cases that the Defense Industrial Security Clearance Office (DISCO) forwards to the ''Defense Office of Hearings and Appeals (DOHA)'' for action under this part to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant.

(d) Provides a program that may be extended to other security cases at the direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C^3I)).

(e) Does not apply to cases in which:

(1) A security clearance is withdrawn because the applicant no longer has a need for access to classified information;

(2) An interim security clearance is withdrawn by the DISCO during an investigation; or

(3) A security clearance is withdrawn for administrative reasons that are without prejudice as to a later determination of whether the grant or continuance of the applicant's security clearance would be clearly consistent with the national interest.

(f) Does not apply to cases for access to sensitive compartmented information or a special access program.

[57 FR 5383, Feb. 14, 1992, as amended at 59 FR 35464, July 12, 1994]