SUBCHAPTER F—SECURITY

PART 154—DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM REGULATION

Subpart A—General Provisions

Subpart B—Policies

Subpart C—Personnel Security Investigative Requirements

Subpart D—Reciprocal Acceptance of Prior Investigations and Personnel Security Determinations

Subpart E—Requesting Personnel Security Investigations

Subpart F—Adjudication

Subpart G—Issuing Clearance and Granting Access

Subpart H—Unfavorable Administrative Actions

Subpart I—Continuing Security Responsibilities

Subpart J—Safeguarding Personnel Security Investigative Records

Subpart K—Program Management

AUTHORITY: E.O. 10450, 18 FR 2489, 3 CFR, 1949–1953 Comp., p. 936; E.O. 12356, 47 FR 14874 and 15557, 3 CFR, 1982 Comp., p. 166; E.O. 10865, 25 FR 1583, 3 CFR, 1959–1963 Comp., p. 398; E.O. 12333, 46 FR 59941, 3 CFR, 1981 Comp., p. 200.

SOURCE: 52 FR 11219, Apr. 8, 1987, unless otherwise noted.

Subpart A—General Provisions

§ 154.1 Purpose.

(a) To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense (DoD), and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.

(b) This part: (1) Establishes DoD personnel security policies and procedures;

(2) Sets forth the standards, criteria and guidelines upon which personnel security determinations shall be based;

(3) Prescribes the kinds and scopes of personnel security investigations required;

(4) Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

(5) Assigns overall program management responsibilities.

§ 154.2 Applicability.

(a) This part implements the Department of Defense Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

(b) All provisions of this part apply to DoD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, contractor personnel and other personnel who are affiliated with the Department of Defense except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22–R and in 32 CFR part 155.

(c) The policies and procedures which govern the National Security Agency are prescribed by Public Laws 88–290 and 86–36, Executive Orders 10450 and 12333, DoD Directive 5210.45[1], Director of Central Intelligence Directive (DCID) 1/14[2] and regulations of the National Security Agency.

(d) Under combat conditions or other military exigencies, an authority in paragraph A, Appendix E, may waive such provisions of this part as the circumstances warrant.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61024, Nov. 19, 1993]

§ 154.3 Definitions.

(a) *Access*. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

(b) *Adverse action*. A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

(c) *Background Investigation (BI)*. A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph 3, Appendix A, this part, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

(d) *Classified information*. Official information or material that requires protection in the interests of national security and that is classified for such

[1] Copies may be obtained, at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

[2] Copies may be obtained, if needed from Central Intelligence Agency (CCISCMS/ICS), 1225 Ames Building, Washington, DC 20505.

purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356.

(e) *Defense Clearance and Investigative Index (DCII).* The DCII is the single, automated, central DoD repository which identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities.

(f) *DoD component.* Includes the Office of the Secretary of Defense; the Military Departments; Chairman of the Joint Chiefs of Staff; Directors of Defense Agencies and the Unified and Specified Commands.

(g) *Entrance National Agency Check (ENTNAC).* A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

(h) *Head of DoD component.* The Secretary of Defense; the Secretaries of the Military Departments; the Chairman of Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands; and the Directors of Defense Agencies.

(i) *Immigrant alien.* Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

(j) *Interim security clearance.* A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

(k) *Limited access authorization.* Authorization for access to Confidential or Secret information granted to non-US. citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (paragraph 3, Appendix A).

(l) *Minor derogatory information.* Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

(m) *National Agency check (NAC).* A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, Appendix A, this part, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

(n) *National Agency Check Plus Written Inquiries (NACI).* A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

(o) *National security.* National security means the national defense and foreign relations of the United States.

(p) *Need-to-know.* A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official U.S. Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

(q) *Periodic Reinvestigation (PR).* An investigation conducted every five years for the purpose of updating a previously completed background investigation, special background investigation, single scope background investigation or PR on persons occupying positions referred to in §154.19. Investigative requirements are as prescribed in appendix A to part 154, section 5. The period of investigation will not normally exceed the most recent 5-year period.

(r) *Personnel Security Investigation (PSI).* Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see §154.9(d)) conducted for the purpose of

making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

(s) *Scope.* The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

(t) *Security clearance.* A determination that a person is eligible under the standards of this part for access to classified information.

(u) *Senior Officer of the Intelligence Community (SOIC).* The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

(v) *Sensitive position.* Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in §154.13(b).

(w) *Significant derogatory information.* Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

(x) *Special access program.* Any program imposing ''need-to-know'' or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need-to-know.

(y) *Special Background Investigation (SBI).* A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph 4, Appendix B, this part. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

(z) *Special Investigative Inquiry (SII).* A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provisions of this part.

(aa) *Service.* Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DoD contractor or as a consultant involving access under the DoD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

(bb) *Unfavorable administrative action.* Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this part.

(cc) *Unfavorable personnel security determination.* A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this part; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

(dd) *United States Citizen (Native Born).* A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the United States).

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61024, Nov. 19, 1993]

Subpart B—Policies

§ 154.6 Standards for access to classified information or assignment to sensitive duties.

(a) *General.* Only U.S. citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in Appendix E has determined that, based on all available information, there are compelling reasons in furtherance of the Department of Defense mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a Limited Access Authorization to classified information. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management, pursuant to E.O. 11935. Exceptions to these requirements shall be permitted only for compelling national security reasons.

(b) *Clearance and sensitive position standard.* The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

(c) *Military service standard.* The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

§ 154.7 Criteria for application of security standards.

The ultimate decision in applying either of the security standards set forth in §154.6 (b) and (c) must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance under the security standard shall include, but not be limited to the following:

(a) Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

(b) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

(c) Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

(d) Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the U.S. or of any State or which seeks to overthrow the Government of the U.S. or any State or subdivision thereof by unlawful means.

(e) Unauthorized disclosure to any person of classified information, or of other information, disclosure of which

is prohibited by statute, Executive Order or regulation.

(f) Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve or which could be expected to serve the interests of another government in preference to the interests of the United States.

(g) Disregard of public law, statutes, Executive Orders or regulations including violation of security regulations or practices.

(h) Criminal or dishonest conduct.

(i) Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

(j) Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

(k) Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be

(1) The presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or

(2) Any other circumstances that could cause the applicant to be vulnerable.

(l) Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

(m) Habitual or episodic use of intoxicants to excess.

(n) Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

(o) Any knowing and willful falsification, coverup, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal agency.

(p) Failing or refusing to answer or to authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment.

(q) Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

§ 154.8 Types and scope of personnel security investigations.

(a) *General.* The types of personnel security investigations authorized below vary in scope of investigative effort required to meet the purpose of the particular investigation. No other types are authorized. The scope of a PSI may be neither raised nor lowered without the approval of the Deputy Under Secretary of Defense for Policy.

(b) *National Agency Check.* Essentially, a NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An ENTNAC is a NAC (scope as outlined in paragraph 1, Appendix A) conducted on inductees and first-term enlistees, but lacking a technical fingerprint search. A NAC is also an integral part of each BI, SBI, and Periodic Reinvestigation (PR). Subpart C prescribes when an NAC is required.

(c) *National Agency Check plus written inquiries.* The Office of Personnel Management (OPM) conducts a NAC plus Written Inquiries (NACIs) on civilian employees for all departments and agencies of the Federal Government, pursuant to E.O. 10450. NACIs are considered to meet the investigative requirements of this regulation for a nonsensitive or noncritical sensitive position and/or up to a Secret clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

(d) *DoD National Agency check plus written inquiries.* DIS will conduct a DNACI, consisting of the scope contained in paragraph 2, Appendix A, for DoD military and contractor personnel

for access to Secret information. Subpart C prescribes when a DNACI is required.

(e) *Background investigation.* The BI is the principal type of investigation conducted when an individual requires Top Secret clearance or is to be assigned to a critical sensitive position. The BI normally covers a 5-year period and consists of a subject interview, NAC, LACs, credit checks, developed character references (3), employment records checks, employment references (3), and select scoping as required to resolve unfavorable or questionable information. (See paragraph 3, Appendix A). Subpart C prescribes when a BI is required.

(f) *Special background investigation.* (1) An SBI is essentially a BI providing additional coverage both in period of time as well as sources of information, scoped in accordance with the provisions of DCID 1/14 but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to SCI, DoD has adopted this coverage for certain other Special Access programs. Subpart C prescribes when an SBI is required.

(2) The OPM, FBI, Central Intelligence Agency (CIA), Secret Service, and the Department of State conduct specially scoped BIs under the provisions of DCID 1/14. Any investigation conducted by one of the above-cited agencies under DCID 1/14 standards is considered to meet the SBI investigative requirements of this part.

(3) The detailed scope of an SBI is set forth in paragraph 4, Appendix A.

(g) *Special investigative inquiry.* (1) A Special Investigative Inquiry is a personnel security investigation conducted to prove or disprove allegations relating to the criteria outlined in §154.7(a) of this part except current criminal activities (see §154.9(c)(4)), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

(2) Special Investigative Inquiries are scoped as necessary to address the specific matters requiring resolution in the case concerned and generally consist of record checks and/or interviews with potentially knowledgeable persons. An SII may include an interview with the subject of the investigation when necessary to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information.

(3) In those cases when there is a disagreement between Defense Investigative Service (DIS) and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense for Policy for resolution.

(h) *Periodic reinvestigation.* As referred to in §154.19(a) and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every five years according to the scope outlined in paragraph 5, Appendix A. The PR scope applies to military, civilian, contractor, and foreign national personnel.

(i) *Personal interview.* Investigative experience over the years has demonstrated that, given normal circumstances, the subject of a personnel security investigation is the best source of accurate and relevant information concerning the matters under consideration. Further, restrictions imposed by the Privacy Act of 1974 dictate that Federal investigative agencies collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Accordingly, personal interviews are an integral part of the DoD personnel security program and shall be conducted in accordance with the requirements set forth in the following paragraphs of this section.

(1) *BI/PR.* A personal interview shall be conducted by a trained DIS agent as part of each BI and PR.

(2) *Resolving adverse information.* A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations), when necessary, as part of each

Special Investigative Inquiry, as well as during the course of initial or expanded investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future Federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

(3) *Hostage situation.* A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See §154.9(d).

(4) *Applicants/potential nominees for DoD military or civilian positions requiring access to SCI or other positions requiring an SBI.* A personal interview of the individual concerned shall be conducted, to the extent feasible, as part of the selection process for applicants/potential nominees for positions requiring access to SCI or completion of an SBI. The interview shall be conducted by a designee of the Component to which the applicant or potential nominee is assigned. Clerical personnel are not authorized to conduct these interviews. Such interviews shall be conducted utilizing resources in the order of priority indicated below:

(i) Existing personnel security screening systems (e.g., Air Force Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

(ii) Commander of the nominating organization or such official as he or she has designated in writing (e.g., Deputy Commander, Executive Officer, Security Officer, Security Manager, S–2, Counterintelligence Specialist, Personnel Security Specialist, or Personnel Officer); or

(iii) Agents of investigative agencies in direct support of the Component concerned.

(5) *Administrative procedures.* (i) The personal interview required by paragraph (i)(4) of this section shall be conducted in accordance with Appendix F.

(ii) For those investigations requested subsequent to the personal interview requirements of paragraph (i)(4) of this section the following procedures apply:

(A) The DD Form 1879 (Request for Personnel Security Investigation) shall be annotated under Item 20 (Remarks) with the statement ''Personal Interview Conducted by (cite the duty assignment of the designated official (e.g., Commander, Security Officer, Personnel Security Specialist, etc.))'' in all cases in which an SBI is subsequently requested.

(B) Unfavorable information developed through the personal interview required by paragraph (i)(4) of this section, will be detailed in a written report attached to the DD Form 1879 to include full identification of the interviewer. Failure to provide such information may result in conduct of an incomplete investigation by DIS.

(C) Whenever it is determined that it is not feasible to conduct the personal interview required by paragraph (i)(4) of this section prior to requesting the SBI, the DD Form 1879 shall be annotated under Item 20 citing the reason for not conducting the interview.

(j) *Expanded investigation.* If adverse or questionable information relevant to a security determination is developed during the conduct of a personnel security investigation, regardless of type, the investigation shall be expanded, consistent with the restrictions in §154.10(e) to the extent necessary to substantiate or disprove the adverse or questionable information.

§154.9 Authorized personnel security investigative agencies.

(a) *General.* The DIS provides a single centrally directed personnel security investigative service to conduct personnel security investigations within the 50 States, District of Columbia, and Commonwealth of Puerto Rico for DoD Components, except as provided for in DoD Directive 5100.23.[1] DIS will request the Military Departments or other appropriate Federal Agencies to

[1] See footnote 1 to §154.2(c).

accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Under Secretary of Defense for Policy. In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

(b) *Subversive affiliations*—(1) *General.* In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

(i) Overthrowing the Government of the United States or the government of a State;

(ii) Substantially impairing for the purpose of influencing U.S. Government policies or decisions:

(A) The functions of the Government of the United States, or

(B) The functions of the government of a State;

(iii) Depriving persons of their civil rights under the Constitution or laws of the United States.

(2) *Military Department/FBI jurisdiction.* Allegations of activities covered by §154.7 (a) through (f) are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI. Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a personnel security investigation conducted by DIS, they shall be referred immediately to either the FBI or to a military department counterintelligence agency, as appropriate.

(3) *DIS jurisdiction.* Allegations of activities limited to those set forth in §154.7 (g) through (j) of this part shall be investigated by DIS.

(c) *Suitability information*—(1) *General.* Most derogatory information developed through personnel security investigations of DoD military or civilian personnel is so-called suitability information, that is, information pertaining to activities or situations covered by §154.7 (g) through (q). Almost all unfavorable personnel security determinations made by DoD authorities are based on derogatory suitability information, although such information is often used as a basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal from Federal employment under OPM regulations.

(2) *Pre-clearance investigation.* Derogatory suitability information, except that covered in paragraph (c)(4) of this section, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to §154.7 (g) through (q).

(3) *Postadjudication investigation.* Derogatory suitability allegations, except those covered by paragraph (c)(4) of this section arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a Special Investigative Inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when §154.19(b) applies. Postadjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations lie outside the DoD personnel security program and are not a

proper investigative function for departmental counterintelligence organizations, Component personnel security authorities, or DIS.

(4) *Allegations of criminal activity*. Any allegations of conduct of a nature indicating possible criminal conduct, including any arising during the course of a personnel security investigation, shall be referred to the appropriate DoD, military department or civilian criminal investigative agency. Military department investigative agencies have primary investigative jurisdiction in cases where there is probable cause to believe that the alleged conduct will be the basis for prosecution under the Uniform Code of Military Justice.

(d) *Hostage situations*—(1) *General*. A hostage situation exists when a member of an individual's immediate family or such other person to whom the individual is bound by obligation or affection resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this category of investigation is based on the possibility that an individual in such a situation might be coerced, influenced, or pressured to act contrary to the best interests of national security.

(2) *DIS jurisdiction*. In the absence of evidence of any coercion, influence or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by DIS.

(3) *Military Department and/or FBI jurisdiction*. Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned—or should there exist any other evidence that the individual is actually being coerced, influenced, or pressured by an element inimical to the interests of national security—then the case becomes a counterintelligence matter (outside of investigative jurisdiction of DIS) to be referred to the appropriate military department or the FBI for investigation.

(e) *Overseas personnel security investigations*. Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate military department investigative organization. Only postadjudication investigations involving an overseas subject may be referred by the requester directly to the military department investigative organization having investigative responsibility in the overseas area concerned (see Appendix I) with a copy of the investigative request sent to DIS. In such cases, the military department investigative agency will complete the investigation, forward the completed report of investigation directly to DIS, with a copy to the requester.

§ 154.10 Limitations and restrictions.

(a) *Authorized requesters and personnel security determination authorities.* Personnel security investigations may be requested and personnel security clearances (including Special Access authorizations as indicated) granted only by those authorities designated in §154.31 and Appendix E.

(b) *Limit investigations and access*. The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the requirements of operations. Special attention shall be given to eliminating unnecessary clearances and requests for personnel security investigations.

(c) *Collection of investigative data*. To the greatest extent practicable, personal information relevant to security determinations shall be obtained directly from the subject of a personnel security investigation. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate from knowledgeable personal sources, particularly the subject's peers, and through checks of relevant records including school, employment, credit, medical, and law enforcement records.

(d) *Privacy Act notification*. Whenever personal information is solicited from an individual preparatory to the initiation of a personnel security investigation, the individual must be informed of—

(1) The authority (statute or Executive order that authorized solicitation);

(2) The principal purpose or purposes for which the information is to be used;

(3) The routine uses to be made of the information;

(4) Whether furnishing such information is mandatory or voluntary;

(5) The effect on the individual, if any, of not providing the information and

(6) That subsequent use of the data may be employed as part of an aperiodic, random process to screen and evaluate continued eligibility for access to classified information.

(e) *Restrictions on investigators.* Investigation shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health thus should be avoided unless the question is relevant to the criteria of §154.7. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this part, investigators shall:

(1) Investigate only cases or persons assigned within their official duties.

(2) Interview sources only where the interview can take place in reasonably private surroundings.

(3) Always present credentials and inform sources of the reasons for the investigation. Inform sources of the subject's accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of personnel security investigations are outlined in paragraph (d) of this section.

(4) Furnish only necessary identity data to a source, and refrain from asking questions in such a manner as to indicate that the investigator is in possession of derogatory information concerning the subject of the investigation.

(5) Refrain from using, under any circumstances, covert or surreptitious investigative methods, devices, or techniques including mail covers, physical or photographic surveillance, voice analyzers, inspection of trash, paid informants, wiretap, or eavesdropping devices.

(6) Refrain from accepting any case in which the investigator knows of circumstances that might adversely affect his fairness, impartiality, or objectivity.

(7) Refrain, under any circumstances, from conducting physical searches of the subject or his property.

(8) Refrain from attempting to evaluate material contained in medical files. Medical files shall be evaluated for personnel security program purposes only by such personnel as are designated by DoD medical authorities. However, review and collection of medical record information may be accomplished by authorized investigative personnel.

(f) *Polygraph restrictions.* The polygraph may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DoD Directive 5210.48. [1]

Subpart C—Personnel Security Investigative Requirements

§154.13 Sensitive positions.

(a) *Designation of sensitive positions.* Certain civilian positions within the Department of Defense entail duties of such a sensitive nature, including access to classified information, that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptably adverse impact upon the national security. These positions are referred to in this part as sensitive positions. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions. Similarly, it is important that only positions which truly meet one or more of the criteria set forth in paragraph (b) of this section be designated as sensitive.

(b) *Criteria for security designation of positions.* Each civilian position within the Department of Defense shall be categorized, with respect to security sensitivity, as either nonsensitive, noncritical-sensitive, or critical-sensitive.

(1) The criteria to be applied in designating a position as sensitive are:

(i) Critical-sensitive.

[1] See footnote 1 to §154.2(c).

(A) Access to Top Secret information.

(B) Development or approval of plans, policies, or programs that affect the overall operations of the Department of Defense or of a DoD Component.

(C) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(D) Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.

(E) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(F) Duties falling under Special Access programs.

(G) Category I automated data processing (ADP) positions.

(H) Any other position so designated by the head of the Component or designee.

(ii) Noncritical-sensitive.

(A) Access to Secret or Confidential information.

(B) Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DoD personnel and property.

(C) Category II automated data processing positions.

(D) Duties involving education and orientation of DoD personnel.

(E) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DoD personnel and property.

(F) Any other position so designated by the head of the Component or designee.

(2) All other positions shall be designated as nonsensitive.

(c) *Authority to designate sensitive positions.* The authority to designate sensitive positions is limited to those authorities designated in paragraph G, Appendix E. These authorities shall designate each position within their jurisdiction as to its security sensitivity and maintain these designations current vis-a-vis the specific duties of each position.

(d) *Limitation of sensitive positions.* It is the responsibility of those authorities authorized to designate sensitive positions to insure that only those positions are designated as sensitive that meet the criteria of paragraph (b) and (c) of this section that the designation of sensitive positions is held to a minimum consistent with mission requirements. Designating authorities shall maintain an accounting of the number of sensitive positions by category, i.e., critical or non-critical sensitive. Such information will be included in annual report required in subpart K.

(e) *Billet control system for Top Secret.* (1) To standardize and control the issuance of Top Secret clearances within the Department of Defense, a specific designated billet must be established and maintained for all DoD military and civilian positions requiring access to Top Secret information. Only persons occupying these billet positions will be authorized a Top Secret clearance. If an individual departs from a Top Secret billet to a billet/position involving a lower level clearance, the Top Secret clearance will be administratively rescinded. This Top Secret billet requirement is in addition to the existing billet structure maintained for SCI access.

(2) Each request to DIS for a BI or SBI that involves access to Top Secret or SCI information will require inclusion of the appropriate billet reference, on the request for investigation. Each Component head should in corporate, to the extent feasible, the Top Secret billet structure into the component Manpower Unit Manning Document. Such a procedure should minimize the time and effort required to maintain such a billet structure.

(3) A report on the number of established Top Secret billets will be submitted each year to the DUSD(P) as part of the annual clearance report referred to in subpart K.

§ 154.14 Civilian employment.

(a) *General.* The appointment of each civilian employee in any DoD Component is subject to investigation, except for reappointment when the break in employment is less than 12 months. The type of investigation required is set forth in this section according to position sensitivity.

(b) *Nonsensitive positions.* In accordance with the OPM Federal Personnel Manual, a NACI shall be requested not later than 3 working days after a person is appointed to a nonsensitive position. Although there is normally no investigation requirement for per diem, intermittent, temporary or seasonal employees in nonsensitive positions provided such employment does not exceed an aggregate of 120 days in either a single continuous or series of appointments, a NAC may be requested of DIS where deemed appropriate by the employing activity.

(c) *Noncritical-sensitive positions.* (1) An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see paragraph (e) (1) and (2) of this section). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

(2) Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information the appropriate investigation is required. The request for the NAC (or NACI) should be submitted to DIS by entering ''SH'' (summer hire) in red letters approximately one inch high on the DD Form 398–2, Personnel Security Questionnaire (National Agency Checklist). Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

(d) *Critical-sensitive positions.* A BI shall be favorably completed prior to appointment to critical-sensitive positions (for exceptions see paragraph (e) (1) and (2) of this section. Certain critical-sensitive positions require a preappointment SBI in accordance with §154.17. Preappointment BIs and SBIs will be conducted by DIS.

(e) *Exceptions*—(1) *Noncritical-sensitive.* In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made part of the record. In such instances, the position may be filled only after the NACI has been requested.

(2) *Critical-sensitive.* In an emergency, a critical-sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record. In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC or ENTNAC has been completed and favorably adjudicated.

(f) *Mobilization of DoD civilian retirees.* The requirements contained in paragraph (a) of this section, regarding the type of investigation required by position sensitivity for DoD civilian retirees temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of title 5, United States Code, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph (a) of this section.

§154.15 Military appointment, enlistment, and induction.

(a) *General.* The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve Components shall be subject to the favorable completion of a personnel security investigation. The types of investigation required are set forth in this section.

(b) *Entrance investigation.* (1) An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, except as

permitted by paragraph (d) of this section, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of appointment. A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

(2) If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized. This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

(3) All derogatory information revealed during the enlistment or appointment process that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398–2.

(c) *Reserve Components and National Guard.* Reserve Component and National Guard personnel not on active duty are subject to the investigative requirements of this section.

(d) *Exceptions for certain commissioned officers of Reserve Components.* The requirements for entrance investigation shall be rigidly adhered to except as follows. Health professionals, chaplains, and attorneys may be commissioned in the Reserve Components prior to completion of a DNACI provided that:

(1) A DNACI is initiated at the time an application for a commission is received; and

(2) The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys.

(e) *Mobilization of military retirees.* The requirements contained in paragraph (c) of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve who has been separated from service for a period of greater than 12 months, should be waived for the purposes of partial or full mobilization under provisions of title 10, (title 14, pertaining to the U.S. Coast Guard as an element of the Navy) U.S. Code, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities.

§ 154.16 Security clearance.

(a) *General.* (1) The authorities designated in paragraph A, Appendix E are the only authorities authorized to grant, deny or revoke DoD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

(2) Military, DoD civilian, and contractor personnel who are employed by or serving in a consultant capacity to the DoD, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has been adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.

(b) *Investigative requirements for clearance*—(1) *Top Secret.* (i) Final Clearance:

(A) BI.

(B) Established billet per §154.13(e) (1) through (3) (except contractors).

(ii) Interim Clearance:

(A) Favorable NAC, ENTNAC, DNACI, or NACI completed

(B) Favorable review of DD Form 398/SF–86/SF–171/DD Form 49

(C) BI or SBI has been initiated

(D) Favorable review of local personnel, base/military police, medical, and other security records as appropriate.

(E) Established billet per §154.13(e) (1) through (3) (except contractors)

(F) Provisions of paragraph §154.14(e) (1) and (2) have been met regarding civilian personnel.

(2) *Secret.* (i) Final Clearance:

(A) DNACI: Military (except first-term enlistees) and contractor employees

(B) NACI: Civilian employees

(C) ENTNAC: First-term enlistees

(ii) Interim Clearance:

(A) When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in paragraphs (b)(2)(ii) (B) through (E) of this section have been complied with.

(B) Favorable review of DD Form 398–2/SF–85/SF–171/DD Form 48.

(C) NACI, DNACI, or ENTNAC initiated.

(D) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(E) Provisions of §154.14(e) have been complied with regarding civilian personnel.

(3) *Confidential.* (i) Final Clearance:

(A) NAC or ENTNAC: Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed.)

(B) NACI: Civilian employees (except for summer hires who may be granted a final clearance on the basis of a NAC).

(ii) Interim Clearance:

(A) Favorable review of DD Form 398–2/SF 85/SF 171/ DD Form 48.

(B) NAC, ENTNAC or NACI initiated.

(C) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(D) Provisions of §154.14(e) (1) and (2) have been complied with regarding civilian personnel.

(4) *Validity of previously granted clearances.* Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is required, investigative requirements of this directive will be followed.

(c) *Access to classified information by non-U.S. citizens.* (1) Only U.S. citizens are eligible for a security clearance. Therefore, every effort shall be made to ensure that non-United States citizens are not employed in duties that may require access to classified information. However, when there are compelling reasons to grant access to classified information to an immigrant alien or a foreign national in furtherance of the mission of the Department of Defense, such individuals may be granted a ''Limited Access Authorization'' (LAA) under the following conditions:

(i) LAAs will be limited to Secret and Confidential level only; LAAs for Top Secret are prohibited.

(ii) Access to classified information is not inconsistent with that determined releasable by designated disclosure authorities, in accordance with DoD Directive 5230.11[1] to the country of which the individual is a citizen.

(iii) Access to classified information must be limited to information relating to a specific program or project.

(iv) Favorable completion of an BI (scoped for 10 years); where the full investigative coverage cannot be completed, a counterintelligence scope polygraph examination will be required in accordance with the provisions of DoD Directive 5210.48.

(v) Security clearances previously issued to immigrant aliens will be reissued as LAAs.

(vi) The Limited Access Authorization determination shall be made only by an authority designated in paragraph B, Appendix E.

(vii) LAAs issued by the Unified and Specified Commands shall be reported to the central adjudicative facility of the appropriate military department in accordance with the assigned responsibilities in DoD Directive 5100.3[1] for inclusion in the Defense Central Index of Investigation (DCII).

(2) In each case of granting a Limited Access Authorization, a record shall be maintained as to:

(i) The identity (including current citizenship) of the individual to whom the Limited Access Authorization is granted, to include name and date and place of birth;

(ii) Date and type of most recent investigation to include the identity of the investigating agency;

(iii) The nature of the specific program material(s) to which access is authorized (delineated as precisely as possible);

[1] See footnote 1 to §154.2(c).

(iv) The classification level to which access is authorized; and

(v) The compelling reasons for granting access to the materials cited in (iii).

(vi) Status of the individual (i.e., immigrant alien or foreign national).

(3) Individuals granted LAAs under the foregoing provisions shall be the subject of a 5-year periodic reinvestigation as set forth in paragraph 5, Appendix A.

(4) Foreign nationals who are LAA candidates must agree to submit to a counterintelligence-scope polygraph examination prior to being granted access in accordance with DoD Directive 5210.48.

(5) If geographical and political situations prevent the full completion of the BI (and/or counterintelligence-scope polygraph) issuance of an LAA shall not be authorized; exceptions to the policy may only be authorized by the DUSD(P).

(6) A report on all LAAs in effect, including the data required in paragraphs (d)(2) (i) through (vi) of this section shall be furnished to the Deputy Under Secretary of Defense for Policy within 60 days after the end of each fiscal year. (See §154.77).

(d) *Access by persons outside the Executive Branch.* (1) Access to classified information by persons outside the Executive Branch shall be accomplished in accordance with 32 CFR part 159. The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

(2) Members of the U.S. Senate and House of Representatives do not require personnel security clearances. They may be granted access to DoD classified information which relates to matters under the jurisdiction of the respective Committees to which they are assigned and is needed to perform their duties in connection with such assignments.

(3) Congressional staff members requiring access to DoD classified information shall be processed for a security clearance in accordance with 32 CFR part 353 and the provisions of this part. The Director, Washington Headquarters Services (WHS) will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

(4) State governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a ''need-to-know'' basis, based upon affirmation by the Secretary of Defense or the head of a DoD Component or single designee, that access, under the circumstances, serves the national interest. Staff personnel of a governor's office requiring access to classified information shall be investigated and cleared in accordance with the prescribed procedures of this part when the head of a DoD Component, or single designee, affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a ''need-to-know'' basis.

(5) Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual States do not require personnel security clearances. They may be granted access to DoD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

(6) Attorneys representing DoD military, civilian or contractor personnel, requiring access to DoD classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph (b) of this section. This shall be done upon certification of the General Counsel of the DoD Component involved in the litigation that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent his or her client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of §154.16(b), access may be granted with the written approval of an authority designated in Appendix E provided that as a minimum: a favorable name check of the FBI and the DCII has been completed, and a DoD Non-

Disclosure Agreement has been executed. In post-indictment cases, after a judge has invoked the security procedures of the Classified Information Procedures Act (CIPA) the Department of Justice may elect to conduct the necessary background investigation and issue the required security clearance, in coordination with the affected DoD Component.

(e) *Restrictions on issuance of personnel security clearances.* Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements. Personnel security clearances shall *not* be issued:

(1) To persons in nonsensitive positions.

(2) To persons whose regular duties do not require authorized access to classified information.

(3) For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

(4) To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

(5) To persons working in shipyards whose duties do not require access to classified information.

(6) To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

(7) To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

(8) To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

(9) To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

(10) To perimeter security personnel who have no access to classified information.

(11) To drivers, chauffeurs and food service personnel.

(f) *Dual citizenship.* Persons claiming both U.S. and foreign citizenship shall be processed under §154.16(b) and adjudicated in accordance with the ''Foreign Preference'' standard in Appendix I.

(g) *One-time access.* Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for compelling reasons in furtherance of the DoD mission, an authority referred to in paragraph (h)(1) of this section, may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

(1) Authorization for such one-time access shall be granted by a flag or general officer, a general court-martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security officials.

(2) The recipient of the one-time access authorization must be a U.S. citizen, possess a current DoD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

(3) Such access, once granted, shall be cancelled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

(4) The employee to be afforded the higher level access shall have been continuously employed by a DoD Component or a cleared DoD contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees.

(5) Pertinent local records concerning the employee concerned shall be reviewed with favorable results.

(6) Whenever possible, access shall be confined to a single instance or at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be cancelled at or before 90 days from original date of access.

(7) Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for:

(i) Recording the higher-level information actually revealed,

(ii) The date(s) such access is afforded; and

(iii) The daily retrieval of the material accessed.

(8) Access at the next higher level shall not be authorized for COMSEC, SCI, NATO, or foreign government information.

(9) The exercise of this provision shall be used sparingly and repeat use within any 12 month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved:

(i) The name, and SSN of the employee afforded higher level access.

(ii) The level of access authorized.

(iii) Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DoD mission would be furthered.

(iv) An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

(v) A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

(vi) The approving authority's signature certifying (h)(9) (i) through (v) of this section.

(vii) Copies of any pertinent briefing/debriefings administered to the employee.

(h) *Access by retired flag/general officers.* (1) Upon determination by an active duty flag/general officer that there are compelling reasons, in furtherance of the Department of Defense mission, to grant a retired flag/general officer access to classified information in connection with a specific DoD program or mission, for a period not greater than 90 days, the investigative requirements of this part may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement—not including access to SCI.

(2) The flag/general officer approving issuance of the clearance shall, provide the appropriate DoD Component central clearance facility a written record to be incorporated into the DCII detailing:

(i) Full identifying data pertaining to the cleared subject;

(ii) The classification of the information to which access was authorized.

(3) Such access may be granted only after the compelling reason and the specific aspect of the DoD mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the confines of a government installation or other area approved for storage of DoD classified information.

[52 FR 11219, Apr. 8, 1987, as amended at 55 FR 3223, Jan. 31, 1990]

§ 154.17 Special access programs.

(a) *General.* It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, national regulations, or international agreement. In this

connection, there are certain Special Access programs originating at the national or international level that require personnel security investigations and procedures of a special nature. These programs and the special investigative requirements imposed by them are described in this section. A Special Access program is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to section 4–2 of Executive Order 12356 and prior Orders. Title 32 CFR part 159 governs the establishment of Departmental Special Access Programs.

(b) *Sensitive Compartmented Information (SCI).* (1) The investigative requirements for access to SCI is an SBI (See paragraph 4, appendix A) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the Personnel Security standards of DCID 1/14 are met.

(2) A previous investigation conducted within the past five years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individual's military service, DoD civilian employment, or access to classified information under the Industrial Security Program greater than 12 months. The individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI.

(c) *Single Integrated Operation Plan—Extremely Sensitive Information (SIOP-ESI).* The investigative requirement for access to SIOP-ESI is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are U.S. citizens other than by birth or who are resident aliens.

(d) *Presidential support activities.* (1) DoD Directive 5210.55[1] prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DoD military and civilian personnel and contractor employees assigned to or utilized in Presidential Support activities. The type of investigation of individuals assigned to Presidential Support activities varies according to whether the person investigated qualifies for Category One or Category Two as indicated below:

(i) *Category one.* (A) Personnel assigned on a permanent or full-time basis to duties in direct support of the President (including the office staff of the Director, White House Military Office, and all individuals under his control):

(*1*) Presidential aircrew and associated maintenance and security personnel.

(*2*) Personnel assigned to the White House communications activities and the Presidential retreat.

(*3*) White House transportation personnel.

(*4*) Presidential mess attendants and medical personnel.

(*5*) Other individuals filling administrative positions at the White House.

(B) Personnel assigned on a temporary or part-time basis to duties supporting the President:

(*1*) Military Social Aides.

(*2*) Selected security, transportation, flight-line safety, and baggage personnel.

(*3*) Others with similar duties.

(C) Personnel assigned to the Office of the Military Aide to the Vice President.

(ii) *Category two.* (A) Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential functions and facilities.

(B) Employees of contractors who provide services or contractors employees who require unescorted access to Presidential Support areas, activities, or equipment—including maintenance of the Presidential retreat, communications, and aircraft.

(C) Individuals in designated units requiring a lesser degree of access to the President or Presidential Support activities.

(2) Personnel nominated for Category One duties must have been the subject of an SBI, including a NAC on the

[1] See footnote 1 to §154.2(c).

spouse and all members of the individual's immediate family of 18 years of age or over who are U.S. citizens other than by birth or who are resident aliens. The SBI must have been completed within the 12 months preceding selection for Presidential Support duties. If such an individual marries subsequent to the completion of the SBI, the required spouse check shall be made at that time.

(3) Personnel nominated for Category Two duties must have been the subject of a BI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are U.S. citizens other than by birth or who are resident aliens. The BI must have been completed within the 12 months preceding selection for Presidential Support duties. It should be noted that duties (separate and distinct from their Presidential Support responsibilities) of some Category Two personnel may make it necessary for them to have special access clearances which require an SBI.

(4) The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation.

(5) A limited number of Category One personnel having especially sensitive duties have been designated by the Director, White House Military Office as ''Category A.'' These personnel shall be investigated under special scoping in accordance with the requirements of the Memorandum of Understanding between the Director, White House Military Office and the Special Assistant to the Secretary and Deputy Secretary of Defense, July 30, 1980.

(e) *Nuclear Weapon Personnel Reliability Program (PRP).* (1) DoD Directive 5210.42[1] sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

(i) *Critical position: BI.* In the event that it becomes necessary to consider an individual for a critical position and the required BI has not been completed, interim certification may be made under carefully controlled conditions as set forth below.

(A) The individual has had a favorable DNACI, NAC (or ENTNAC) within the past 5 years without a break in service or employment in excess of 1 year.

(B) The BI has been requested.

(C) All other requirements of the PRP screening process have been fulfilled.

(D) The individual is identified to supervisory personnel as being certified on an interim basis.

(E) The individual is not used in a two-man team with another such individual.

(F) Justification of the need for interim certification is documented by the certifying official.

(G) Should the BI not be completed within 150 days from the date of the request, the certifying official shall query the Component clearance authority, who shall ascertain from DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

(ii) *Controlled position: DNACI/NACI.* (A) An ENTNAC completed for the purpose of first term enlistment or induction into the Armed Forces does not satisfy this requirement.

(B) Interim certification is authorized for an individual who has not had a DNACI/NACI completed within the past 5 years, subject to the following conditions:

(*1*) The individual has had a favorable ENTNAC/NAC, or higher investigation, that is more than 5 years old and has not had a break in service or employment in excess of 1 year.

(*2*) A DNACI/NACI has been requested at the time of interim certification.

(*3*) All other requirements of the PRP screening process have been fulfilled.

(*4*) Should the DNACI/NACI not be completed within 90 days from the date of the request, the procedures set forth in paragraph (e)(1)(i)(G) of this section for ascertaining the delay of the investigation in the case of a critical position shall apply.

[1] See footnote 1 to §154.2(c).

(iii) *Additional requirements apply.* (A) The investigation upon which certification is based must have been completed within the last 5 years from the date of initial assignment to a PRP position and there must not have been a break in service or employment in excess of 1 year between completion of the investigation and initial assignment.

(B) In those cases in which the investigation was completed more than 5 years prior to initial assignment or in which there has been a break in service or employment in excess of 1 year subsequent to completion of the investigation, a reinvestigation is required.

(C) Subsequent to initial assignment to the PRP, reinvestigation is not required so long as the individual remains in the PRP.

(D) A medical evaluation of the individual as set forth in DoD Directive 5210.42.

(E) Review of the individual's personnel file and other official records and information locally available concerning behavior or conduct which is relevant to PRP standards.

(F) A personal interview with the individual for the purpose of informing him of the significance of the assignment, reliability standards, the need for reliable performance, and of ascertaining his attitude with respect to the PRP.

(G) Service in the Army, Navy and Air Force Reserve does not constitute active service for PRP purposes.

(f) *Access to North Atlantic Treaty Organization (NATO) classified information.* (1) Personnel assigned to a NATO staff position requiring access to NATO Cosmic (Top Secret), Secret, or Confidential information shall have been the subject of a favorably adjudicated BI (10 year scope), DNACI/NACI or NAC/ENTNAC, current within five years prior to the assignment, in accordance with USSAN Instruction 1–69 and §154.19(f).

(2) Personnel *not* assigned to a NATO staff position, but requiring access to NATO Cosmic, Secret or Confidential information in the normal course of their duties, must possess the equivalent final U.S. security clearance based upon the appropriate personnel security investigation (appendix A) required by §§154.16(b) and 154.19(j) of this part.

(g) *Other special access programs.* Special investigative requirements for Special Access programs not provided for in this paragraph may not be established without the written approval of the Deputy Under Secretary of Defense for Policy.

§154.18 Certain positions not necessarily requiring access to classified information.

(a) *General.* DoD Directive 5200.8[1] outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this part should suffice to enable a commander to determine the trustworthiness of individuals whose duties require access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although not requiring access to classified information, if performed by untrustworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

(b) *Access to restricted areas, sensitive information or equipment not involving access to classified information.* (1) Access to restricted areas, sensitive information or equipment by DoD military, civilian or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate component agency or activity prior to permitting such access. DoD Components shall not request, and

[1] See footnote 1 to §154.2(c).

shall not direct or permit their contractors to request, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In determining trustworthiness under this paragraph, the provisions of §154.7 and appendix H will be utilized.

(2) In meeting the requirements of this paragraph, approval shall be obtained from one of the authorities designated in paragraph A, appendix E of this part, for authority to request NACs on DoD military, civilian or contractor employees. A justification shall accompany each request which shall detail the reasons why escorted access would not better serve the national security. Requests for investigative requirements beyond a NAC shall be forwarded to the Deputy Under Secretary of Defense for Policy for approval.

(3) NAC requests shall—

(i) Be forwarded to DIS in accordance with the provisions of paragraph B, appendix C,

(ii) Contain a reference to this paragraph on the DD Form 398–2, and

(iii) List the authority in appendix E who approved the request.

(4) Determinations to deny access under the provisions of this paragraph must not be exercised in an arbitrary, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DoD Directive 5200.8.

(c) *Nonappropriated fund employees.* Each Nonappropriated Fund employee who is employed in a position of trust as designated by an official authorized in paragraph H, appendix E, shall have been the subject of a NAC completed no longer than 12 months prior to employment or a prior personnel security investigation with no break in Federal service or employment greater than 12 months in accordance with DoD Manual 1401.1–M. An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. Issuance of a Confidential or Secret clearance will be based on a DNACI or NACI in accordance with §154.16(b).

(d) *Customs inspectors.* DoD employees appointed as customs inspectors, under waivers approved in accordance with DoD 5030.49–R shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DoD employment greater than 1 year in which case a current NAC is required.

(e) *Red Cross/United Service Organizations personnel.* A favorably adjudicated NAC shall be accomplished on Red Cross or United Service Organizations personnel as prerequisite for assignment with the Armed Forces overseas (32 CFR part 253).

(f) *Officials authorized to issue security clearances.* Any person authorized to adjudicate personnel security clearances shall have been the subject of a favorably adjudicated BI.

(g) *Personnel security clearance adjudication officials.* Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated BI.

(h) *Persons requiring DoD building passes.* Pursuant to DoD Directive 5210.46[1] each person determined by the designated authorities of the Components concerned as having an official need for access to DoD buildings in the National Capital Region shall be the subject of a favorably, adjudicated NAC prior to issuance of a DoD building pass. Conduct of a BI for this purpose is prohibited unless approved in advance by ODUSD(P).

(i) *Foreign national employees overseas not requiring access to classified information.* Foreign nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate military department investigative organization consistent with §154.9(e) prior to employment:

(1) Host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and

(2) DCII.

[1] See footnote 1 to §154.2(c).

(3) FBI-HQ/ID. (Where information exists regarding residence by the foreign national in the United States for one year or more since age 18).

(j) *Special agents and investigative support personnel.* Special agents and those noninvestigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

(k) *Persons requiring access to chemical agents.* Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DoD Directive 5210.65.[1]

(l) *Education and orientation personnel.* Persons selected for duties in connection with programs involving the education and orientation of military personnel shall have been the subject of a favorably adjudicated NAC prior to such assignment. This does not include teachers/administrators associated with university extension courses conducted on military installations in the United States. Non-US citizens from a country listed in appendix G shall be required to undergo a BI if they are employed in a position covered by this paragraph.

(m) *Contract guards.* Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC prior to such assignment.

(n) *Transportation of arms, ammunition and explosives (AA&E).* Any DoD military, civilian or contract employee (including commercial carrier) operating a vehicle or providing security to a vehicle transporting Category I, II or Confidential AA&E shall have been the subject of a favorably adjudicated NAC or ENTNAC.

(o) *Personnel occupying information systems positions designated ADP-I, ADP-II & ADP-III.* DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with appendix J) and investigated as follows:

ADP-I:	BI
ADP-II:	DNACI/NACI
ADP-III:	NAC/ENTNAC

Those personnel falling in the above categories who require access to classified information will, of course, be subject to the appropriate investigative scope contained in §154.16(b).

(p) *Others.* Requests for approval to conduct an investigation on other personnel, not provided for in §154.18 (b) through (o) considered to fall within the general provisions of §154.18(a) shall be submitted, detailing the justification therefor, for approval to the Deputy Under Secretary of Defense for Policy. Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

§154.19 Reinvestigation.

(a) *General.* DoD policy prohibits unauthorized and unnecessary investigations. There are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under the provisions of this part. It is the policy to limit reinvestigation of individuals to the scope contained in paragraph 5, appendix A to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

(1) To prove or disprove an allegation relating to the criteria set forth in §154.7 of this part with respect to an individual holding a security clearance or assigned to a position that requires a trustworthiness determination;

(2) To meet the periodic reinvestigation requirements of this part with respect to those security programs enumerated below; and

(3) Upon individual request, to assess the current eligibility of individuals

[1] See footnote 1 to §154.2(c).

who did not receive favorable adjudicative action after an initial investigation, if a potential clearance need exists and there are reasonable indications that the factors upon which the adverse determination was made no longer exists.

(b) *Allegations related to disqualification.* Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in §154.7 that could have an adverse impact on an individual's security status, a Special Investigative Inquiry (SII), psychiatric, drug or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject, and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with §154.56(b).

(c) *Access to Sensitive Compartmented Information (SCI).* Each individual having current access to SCI shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, appendix A.

(d) *Critical-sensitive positions.* Each DoD civilian employee occupying a critical sensitive position shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, appendix A.

(e) *Presidential support duties.* Each individual assigned Presidential Support duties shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, appendix A.

(f) *NATO staff.* Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, appendix A. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5-year recurring basis.

(g) *Extraordinarily sensitive duties.* In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special compartmentation and other special security measures. In such instances, a Component SOIC may, with the approval of the Deputy Under Secretary of Defense for Policy, request PR's at intervals of less than 5 years as outlined in paragraph 5, appendix A. Such requests shall include full justification and a recommendation as to the desired frequency. In reviewing such requests, the Deputy Under Secretary of Defense for Policy shall give due consideration to:

(1) The potential damage that might result from the individual's defection or abduction.

(2) The availability and probable effectiveness of means other than reinvestigation to evaluate factors concerning the individual's suitability for continued SCI access.

(h) *Foreign nationals employed by DoD organizations overseas.* Foreign nationals employed by DoD organizations overseas who have been granted a ''Limited Access Authorization'' pursuant to §154.16(d) shall be the subject of a PR, as set forth in paragraph 5, appendix A, conducted under the auspices of DIS by the appropriate military department or other U.S. Government investigative agency consistent with §154.9(e) and appendix I of this part.

(i) *Persons accessing very sensitive information classified Secret.* (1) Heads of DoD Components shall submit a request to the Deputy Under Secretary of Defense for Policy for approval to conduct periodic reinvestigations on persons holding Secret clearances who are exposed to very sensitive Secret information.

(2) Generally, the Deputy Under Secretary of Defense for Policy will only approve periodic reinvestigations of persons having access to Secret information if the unauthorized disclosure of the information in question could reasonably be expected to:

(i) Jeopardize human life or safety.

(ii) Result in the loss of unique or uniquely productive intelligence sources or methods vital to U.S. security.

(iii) Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

(3) Each individual accessing very sensitive Secret information who has been designated by an authority listed

in paragraph A, appendix E as requiring periodic reinvestigation, shall be the subject of a PR conducted on a 5-year recurring basis scoped as stated in paragraph 5, appendix A.

(j) *Access to Top Secret information.* Each individual having current access to Top Secret information shall be the subject of a PR conducted on a 5-year recurring basis scoped as outlined in paragraph 5, appendix A.

(k) *Personnel occupying computer positions designated ADP–1.* All DoD military, civilians, consultants, and contractor personnel occupying computer positions designated ADP-I, shall be the subject of a PR conducted on a 5-year recurring basis as set forth in paragraph 5, appendix A.

§ 154.20 Authority to waive investigative requirements.

Authorized officials. Only an official designated in paragraph G, appendix E, is empowered to waive the investigative requirements for appointment to a sensitive position, assignment to sensitive duties or access to classified information pending completion of the investigation required by this section. Such waiver shall be based upon certification in writing by the designated official that such action is necessary to the accomplishment of a DoD mission. A minor investigative element that has not been met should not preclude favorable.

Subpart D—Reciprocal Acceptance of Prior Investigations and Personnel Security Determinations

§ 154.23 General.

Previously conducted investigations and previously rendered personnel security determinations shall be accepted within DoD in accordance with the policy set forth below.

§ 154.24 Prior investigations conducted by DoD investigative organizations.

As long as there is no break in military service/civilian employment greater than 12 months, any previous personnel security investigation conducted by DoD investigative organizations that essentially is equivalent in scope to an investigation required by this part will be accepted without requesting additional investigation. There is no time limitation as to the acceptability of such investigations, subject to the provisions of §§ 154.8(h) and 154.25(b) of this part.

§ 154.25 Prior personnel security determinations made by DoD authorities.

(a) Adjudicative determinations for appointment in sensitive positions, assignment to sensitive duties or access to classified information (including those pertaining to SCI) made by designated DoD authorities will be mutually and reciprocally accepted by all DoD Components without requiring additional investigation, unless there has been a break in the individual's military service/civilian employment of greater than 12 months or unless derogatory information that occurred subsequent to the last prior security determination becomes known. A check of the DCII should be conducted to accomplish this task.

(b) Whenever a valid DoD security clearance or Special Access authorization (including one pertaining to SCI) is on record, Components shall not request DIS or other DoD investigative organizations to forward prior investigative files for review unless:

(1) Significant derogatory information or investigation completed subsequent to the date of last clearance or Special Access authorization, is known to the requester; or

(2) The individual concerned is being considered for a higher level clearance (e.g., Secret or Top Secret) or the individual does not have a Special Access authorization and is being considered for one; or

(3) There has been a break in the individual's military service/civilian employment of greater than 12 months subsequent to the issuance of a prior clearance.

(4) The most recent SCI access authorization of the individual concerned was based on a waiver.

(c) Requests for prior investigative files authorized by this part shall be made in writing, shall cite the specific justification for the request (i.e., upgrade of clearance, issue Special Access

authorization, etc.), and shall include the date, level, and issuing organization of the individual's current or most recent security clearance or Special Access authorization.

(d) All requests for non-DoD investigative files, authorized under the criteria prescribed by paragraphs (a), (b)(1), (2), (3), and (4) and (c) of this section shall be:

(1) Submitted on DD Form 398–2 to DIS;

(2) Annotated as a ''Single Agency Check'' of whichever agency or agency developed the investigative file or to obtain the check of a single national agency.

(e) When further investigation is desired, in addition to an existing non-DoD investigative file, a DD Form 1879 will be submitted to DIS with the appropriate security forms attached. The submission of a Single Agency Check via DD Form 398–2 will be used to obtain an existing investigative file or check a single national agency.

(f) Whenever a civilian or military member transfers from one DoD activity to another, the losing organization's security office is responsible for advising the gaining organization of any pending action to suspend, deny or revoke the individual's security clearance as well as any adverse information that may exist in security, personnel or other files. In such instances the clearance shall not be reissued until the questionable information has been adjudicated.

§ 154.26 Investigations conducted and clearances granted by other agencies of the Federal government.

(a) Whenever a prior investigation or personnel security determination (including clearance for access to information classified under E.O. 12356 of another agency of the Federal Government meets the investigative scope and standards of this part, such investigation or clearance may be accepted for the investigative or clearance purposes of this part, provided that the employment with the Federal agency concerned has been continuous and there has been no break longer than 12 months since completion of the prior investigation, and further provided that inquiry with the agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation shall be requested.

(b) A NACI conducted by OPM shall be accepted and considered equivalent to a DNACI for the purposes of this part.

(c) Department of Defense policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set forth in DoD Directive 5210.2.[1]

Subpart E—Requesting Personnel Security Investigations

§ 154.30 General.

Requests for personnel security investigations shall be limited to those required to accomplish the Defense mission. Such requests shall be submitted only by the authorities designated in §154.31. These authorities shall be held responsible for determining if persons under their jurisdiction require a personnel security investigation. Proper planning must be effected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time it is needed to grant the required clearance or otherwise make the necessary personnel security determination.

§ 154.31 Authorized requesters.

Requests for personnel security investigation shall be accepted only from the requesters designated below:

(a) *Military Departments.* (1) Army.

(i) Central Clearance Facility.

(ii) All activity commanders.

(iii) Chiefs of recruiting stations.

(2) Navy (including Marine Corps).

(i) Central Adjudicative Facility.

(ii) Commanders and commanding officers of organizations listed on the Standard Navy Distribution List.

(iii) Chiefs of recruiting stations.

(3) Air Force.

(i) Air Force Security Clearance Office.

(ii) Assistant Chief of Staff for Intelligence.

[1] See footnote 1 to §154.2(c).

(iii) All activity commanders.

(iv) Chiefs of recruiting stations.

(b) Defense Agencies—Directors of Security and activity commanders.

(c) Organization of the Joint Chiefs of Staff—Chief, Security Division.

(d) Office of the Secretary of Defense—Director for Personnel and Security, Washington Headquarters Services.

(e) Commanders of Unified and Specified Commands or their designees.

(f) Such other requesters approved by the Deputy Under Secretary of Defense for Policy.

§ 154.32 Criteria for requesting investigations.

Authorized requesters shall use the tables set forth in appendix C to determine the type of investigation that shall be requested to meet the investigative requirement of the specific position or duty concerned.

§ 154.33 Request procedures.

To insure efficient and effective completion of required investigations, all requests for personnel security investigations shall be prepared and forwarded in accordance with Appendix B and the investigative jurisdictional policies set forth in §154.9.

§ 154.34 Priority requests.

To insure that personnel security investigations are conducted in an orderly and efficient manner, requests for priority for individual investigations or categories of investigations shall be kept to a minimum. DIS shall not assign priority to any personnel security investigation or categories of investigations without written approval of the Deputy Under Secretary of Defense for Policy.

§ 154.35 Personal data provided by the subject of the investigation.

(a) To conduct the required investigation, it is necessary that the investigative agency be provided certain relevant data concerning the subject of the investigation. The Privacy Act of 1974 requires that, to the greatest extent practicable, personal information shall be obtained directly from the subject individual when the information may result in adverse determinations affecting an individual's rights, benefits, and privileges under Federal programs.

(b) Accordingly, it is incumbent upon the subject of each personnel security investigation to provide the personal information required by this part. At a minimum, the individual shall complete the appropriate investigative forms, provide fingerprints of a quality acceptable to the FBI, and execute a signed release, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records, to provide relevant record information to the investigative agency. When the FBI returns a fingerprint card indicating that the quality of the fingerprints is not acceptable, an additional set of fingerprints will be obtained from the subject. In the event the FBI indicates that the additional fingerprints are also unacceptable, no further attempt to obtain more fingerprints need be made; this aspect of the investigation will then be processed on the basis of the name check of the FBI files. As an exception, a minimum of three attempts will be made for all Presidential Support cases, for SCI access nominations if the requester so indicates, and in those cases in which more than minor derogatory information exists. Each subject of a personnel security investigation conducted under the provisions of this part shall be furnished a Privacy Act Statement advising of the authority for obtaining the personal data, the principal purpose(s) for obtaining it, the routine uses, whether disclosure is mandatory or voluntary, the effect on the individual if it is not provided, and that subsequent use of the data may be employed as part of an aperiodic review process to evaluate continued eligibility for access to classified information.

(c) Failure to respond within the time limit prescribed by the requesting organization with the required security forms or refusal to provide or permit access to the relevant information required by this part shall result in termination of the individual's security clearance or assignment to sensitive duties utilizing the procedures of §154.59 or further administrative processing of the investigative request.

Subpart F—Adjudication

§ 154.40 General.

(a) The standard which must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

(b) The principal objective of the DoD personnel security adjudicative function, consequently, is to assure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

(c) Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility which could, if abused, have unacceptable consequences for the national security.

(d) While equity demands optimal uniformity in evaluating individual cases, assuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, and prior experience in similar cases. All information of record, both favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness, and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

§ 154.41 Central adjudication.

(a) To ensure uniform application of the requirement of this part and to ensure that DoD personnel security determinations are effected consistent with existing statutes and Executive orders, the head of each Military Department and Defense Agencies shall establish a single Central Adjudication Facility for his/her component. The function of such facility shall be limited to evaluating personnel security investigations and making personnel security determinations. The chief of each Central Adjudication Facility shall have the authority to act on behalf of the head of the Component concerned with respect to personnel security determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this part shall be reviewed and evaluated by personnel security specialists specifically designated by the head of the Component concerned, or designee.

(b) In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations:

(1) BI/SBI/PR/ENAC/SII:

(i) *Favorable:* Completely favorable investigations shall be reviewed and approved by an adjudicative official in the civilian grade of GS–7/9 or the military rank of O–3.

(ii) *Unfavorable:* Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS–11/12 or the military rank of O–4. When an unfavorable administrative action is contemplated under § 154.56(b), the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS–13/14 or the military rank

of O–5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS–14/15 or the military rank of O–6.

(2) *NACI/DNACI/NAC/ENTNAC:*

(i) *Favorable:* A completely favorable investigation may be finally adjudicated after one level of review provided that the decisionmaking authority is at the civilian grade of GS–5/7 or the military rank of 0–2.

(ii) *Unfavorable:* Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS–7/9 or the military rank of 0–3. When an unfavorable administrative action is contemplated under §154.56(b), the letter of intent to deny/revoke must be signed by an adjudicative official at the civilian grade of GS–11/12 or the military rank of 0–4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS–13 or the military rank of 0–5 or above.

(c) Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

§154.42 Evaluation of personnel security information.

(a) The criteria and adjudicative policy to be used in applying the principles at §154.40 are set forth in §154.7(a) and appendix H of this part. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly consistent with the interests of national security and shall be an overall common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

(1) The nature and seriousness of the conduct;

(2) The circumstances surrounding the conduct;

(3) The frequency and recency of the conduct;

(4) The age of the individual;

(5) The voluntariness of participation; and

(6) The absence or presence of rehabilitation.

(b) Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in appendix H. Adjudication policy for access to SCI is contained in DCID 1/14.

§154.43 Adjudicative record.

(a) Each adjudicative determinations, whether favorable or unfavorable, shall be entered into the Defense Clearance and Investigations Index (DCII) on a daily basis, but in no case to exceed 5 working days from the date of determination.

(b) The rationale underlying each unfavorable personnel security determination, to include the appeal process, and each favorable personnel security determination where the investigation or information upon which the determination was made included significant derogatory information of the type set forth in §154.7 and appendix H to part 154, shall be maintained in written or automated form and is subject to the provisions of 32 CFR part 285 and 32 CFR part 310. This information shall be maintained for a minimum of 5 years from the date of determination.

[58 FR 61025, Nov. 19, 1993]

Subpart G—Issuing Clearance and Granting Access

§154.47 General.

(a) The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to

perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of §154.56(b).

(b) Only the authorities designated in paragraph A, appendix E are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in §154.55(b) of this part are complied.

(c) All commanders and heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this part.

§154.48 Issuing clearance.

(a) Authorities designated in paragraph A, appendix E shall record the issuance, denial or revocation of a personnel security clearance in the DCII (see §154.43). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate.

(b) A personnel security clearance remains valid until the individual is separated from the Armed Forces, separated from DoD civilian employment, has no further official relationship with DoD, official action has been taken to deny, revoke or suspend the clearance or access, or regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties. If an individual resumes his or her affiliation with DoD no single break in the individual's relationship with DoD exists greater than 24 months and/or, the need for regular access to classified information at or below the previous level recurs, and no record of an unfavorable administrative action exists, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

(c) Personnel security clearances of DoD military personnel shall be granted denied or revoked only by the designated authority of the parent Military Department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DoD Component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on Army, Navy, and Air Force personnel by DIS will be returned only to the parent service of the subject for adjudication regardless of the source of the original request. The adjudicative authority will be responsible for expeditiously transmitting the results of the clearance determination. As an exception, the employing DoD Component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility determination by the individual's parent Component. Whenever an employing DoD Component issues an interim clearance to an individual from another Component, written notice of the action shall be provided to the parent Component.

(d) When a Defense agency, to include Chairman of the Joint Chiefs of Staff, initiates an SBI (or PR) for access to SCI on a military member, DIS will return the completed investigation to the appropriate Military Department adjudicative authority in accordance with paragraph (c) of this section for issuance (or reissuance) of the Top Secret clearance. Following the issuance of the security clearance, the military adjudicative authority will forward the investigative file to the Defense agency identified in the ''Return Results To'' block of the DD Form 1879. The receiving agency will then forward the completed SBI on to DIA for the SCI adjudication in accordance with DCID 1/14.

(e) The interim clearance shall be recorded in the DCSI (§154.43) by the parent DoD Component in the same manner as a final clearance.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§ 154.49 Granting access.

(a) Access to classified information shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

(b) In the absence of derogatory information on the individual concerned, DoD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DoD authority authorized by this part to issue personnel security clearances, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

(c) The access level of cleared individuals will, wherever possible, be entered into the Defense Clearance and Investigations Index (DCII), along with clearance eligibility. However, completion of the DCII Access field is required effective October 1, 1993 in all instances where the adjudicator with a personnel security investigation. Agencies are encouraged to start completing this field as soon as possible.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§ 154.50 Administrative withdrawal.

As set forth in § 154.48 the personnel security clearance and access eligibility must be withdrawn when the events described therein occur. When regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties, the previously authorized access eligibility level must be administratively downgraded or withdrawn, as appropriate.

Subpart H—Unfavorable Administrative Actions

§ 154.55 Requirements.

(a) *General.* For purposes of this part, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at § 154.3 and any unfavorable personnel security determination, as defined at § 154.3. This subpart is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

(b) *Referral for action.* (1) Whenever derogatory information relating to the criteria and policy set forth in § 154.7(a) and appendix H of this part is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall insure that the parent Component of the individual concerned is informed promptly concerning the derogatory information developed and any actions taken or anticipated with respect thereto. However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with § 154.56(b), if such action is warranted and supportable by the criteria and policy contained in § 154.7(a) and appendix H. No unfavorable administrative action as defined in § 154.3 may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in § 154.56(b) or, in the case of SCI, Annex B, DCID 1/14.

(2) The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported

other than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General ''hotline'' to receive such reports for appropriate follow-up by DIS. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

(c) *Suspension.* (1) The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subject's security status unchanged or to take interim action to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability to intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the appropriate authority designated in appendix F to this part.

(2) Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), the individual concerned must be notified of the determination in writing by the commander, or head of the component or adjudicative authority, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

(3) Component field elements must promptly report all suspension actions to the appropriate central adjudicative authority, but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the DCII Eligibility and Access fields to alert all users to the individual's changed status.

(4) Every effect shall be made to resolve suspension cases as expeditiously as circumstances permit. Suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be reported to the DASD(CI&SCM) for review and appropriate action.

(5) A final security clearance eligibility determination shall be made for all suspension actions and the determination entered in the DCII. If, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the ''Z'' Code (adjudication action incomplete due to loss of jurisdiction) if the clearance eligibility field is appropriate. In no case shall a ''suspension'' code (Code Y) remain as a permanent record in the DCII.

(6) A clearance or access entry in the DCII shall not be suspended or downgraded based solely on the fact that a periodic reinvestigation was not conducted precisely within the 5 year time period for TOP SECRET/SCI or within the period prevailing for SECRET clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed time frame, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

(d) *Final unfavorable administrative actions.* The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in appendix E, except that the authority to terminate the employment of a civilian employee of a military department or Defense agency is vested solely in the head of the DoD component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DoD Components, on the basis of criteria listed in §154.7 (a) through (f), shall be coordinated with the Deputy Under Secretary

of Defense for Policy prior to final action by the head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this part if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the military departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the central adjudication facility to continue for process the individual for denial or revocation of a security clearance, access to classified information on or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this part.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§ 154.56 Procedures.

(a) *General.* No final personnel security determination shall be made on a member of the Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in paragraph (b) of this section when such determination results in an unfavorable administrative action (see §154.55(a)). As an exception, Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by 32 CFR part 253.

(b) *Unfavorable administrative action procedures.* Except as provided for below, no unfavorable administrative action shall be taken under the authority of this part unless the person concerned has been given:

(1) A written statement of the reasons why the unfavorable administrative action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of the Privacy Act of 1974 (5 U.S.C. 552a) and national security permit. The statement will also provide the name and address of the agencies (agencies) to which the individual may write to obtain a copy of the investigative file(s) upon which the unfavorable administrative action is being taken. Prior to issuing a statement of reasons to a civilian employee for suspension or removal action, the issuing authority must comply with the provisions of Federal Personnel Manual, chapter 732, subchapter 1, paragraph 1–6b. The signature authority must be as provided for in §154.41(b) (1)(ii) and (2)(ii).

(2) An opportunity to reply in writing to such authority as the head of the Component concerned may designate;

(3) A written response to any submission under subparagraph b. stating the final reasons therefor, which shall be as specific as privacy and national security considerations permit. The signature authority must be as provided for in §154.41(b) (1)(ii) and (2)(ii). Such response shall be as prompt as individual circumstances permit, not to exceed 60 days from the date of receipt of the appeal submitted under paragraph (b)(2) of this section provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the subject must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not, in any case, exceed a total of 90 days from the date of receipt of the appeal under paragraph (b) of this section.

(4) An opportunity to appeal to a higher level of authority designated by the Component concerned.

(c) *Exceptions to policy.* Notwithstanding paragraph (b) of this section or any other provision of this part, nothing in this part shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to section 7532, title 5, U.S. Code. Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph (b) of this section are not appropriate. Such determination shall be conclusive.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§ 154.57 Reinstatement of civilian employees.

(a) *General.* Any person whose civilian employment in the Department of Defense is terminated under the provisions of this part shall not be reinstated or restored to duty or reemployed in the Department of Defense unless the Secretary of Defense, or the head of a DoD Component, finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made a part of the personnel security record.

(b) *Reinstatement benefits.* A DoD civilian employee whose employment has been suspended or terminated under the provisions of this part and who is reinstated or restored to duty under the provisions of section 3571 of title 5 U.S. Code is entitled to benefits as provided for by section 3 of Pub. L. 89–380.

Subpart I—Continuing Security Responsibilities

§ 154.60 Evaluating continued security eligibility.

(a) *General.* A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to assure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process.

(b) *Management responsibility.* (1) Commanders and heads of organizations shall insure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this part) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

(2) The heads of all DoD components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long term, job-related security problems.

(c) *Supervisory responsibility.* Security programs shall be established to insure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individual's continued eligibility for access.

(1) In conjunction with the submission of PRs stated in § 154.19, and paragraph 5, appendix A, supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on

subject's continued eligibility for access to classified information is omitted.

(2) If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package.

I am aware of no information of the type contained at Appendix D, 32 CFR part 154, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information.

(3) If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

I am aware of information of the type contained in Appendix D, 32 CFR part 154, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s).

(4) In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs (c) (2) and (3) of this section as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

(d) *Individual responsibility.* (1) Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

(2) Moreover, individuals having access to classified information must report promptly to their security office:

(i) Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

(A) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(B) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

(ii) Any information of the type referred to in §154.7 or appendix H to this part.

(e) *Co-worker responsibility.* Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§154.61 Security education.

(a) *General.* The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, heads of DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

(b) *Initial briefing.* (1) All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this part shall be given an initial security briefing. The briefing shall be in accordance with the requirements of 32 CFR part 159 and consist of the following elements:

(i) The specific security requirements of their particular job.

(ii) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

(iii) The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

(iv) The penalties that may be imposed for security violations.

(2) If an individual declines to execute Standard Form 312, ''Classified Information Nondisclosure Agreement'' (replaced the Standard Form 189), the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with §154.56(b).

(c) *Refresher briefing.* Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in 32 CFR part 159 shall be tailored to fit the needs of experienced personnel.

(d) Foreign travel briefing. While world events during the past several years have diminished the threat to our national security from traditional cold-war era foreign intelligence services, foreign intelligence service continue to pursue the unauthorized acquisition of classified or otherwise sensitive U.S. Government information, through the recruitment of U.S. Government employees with access to such information. Through security briefings and education, the Department of Defense continues to provide for the protection of information and technology considered vital to the national security interests from illegal or unauthorized acquisition by foreign intelligence services.

(1) DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office all contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

(i) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(ii) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

(2) The DoD security manager, security specialist or other qualified individual will review and evaluate the reported information. Any facts or circumstances of a reported contact with a foreign national that appear to:

(i) Indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified information or technology;

(ii) Offer a reasonable potential for such; or

(iii) Indicate the possibility of continued contact with the foreign national for such purposes, shall be promptly reported to the appropriate counterintelligence agency.

(e) *Termination briefing.* (1) Upon termination of employment administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

(i) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD Regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(ii) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

(iii) An acknowledgment that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

(iv) An acknowledgment that the individual will report without delay to the FBI or the DoD Component concerned any attempt by any unauthorized person to solicit classified information.

(2) When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service who shall ensure that it is recorded in the Defense Clearance and Investigations Index.

(3) The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

(4) In addition to the provisions of paragraphs (e)(1), (e)(2), and (e)(3) of this section, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS–16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61026, Nov. 19, 1993]

Subpart J—Safeguarding Personnel Security Investigative Records

§ 154.65 General.

In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DoD military and civilian personnel, contractor employees, and other persons affiliated with the Department of Defense, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counterintelligence investigations. Other uses are subject to the specific written authorization of the Deputy Under Secretary of Defense for Policy.

§ 154.66 Responsibilities.

DoD authorities responsible for administering the DoD personnel security program and all DoD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this part and that such reports and records are safeguarded as prescribed herein. The heads of DoD Components and the Deputy Under Secretary of Defense for Policy for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by §§ 154.67 and 154.68.

§ 154.67 Access restrictions.

Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with 32 CFR parts 286 and 286a and with the following:

(a) DoD personnel security investigative reports shall be released outside of the DoD only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

(b) Within DoD, access to personnel security investigative reports shall be limited to those designated DoD officials who require access in connection with specifically assigned personnel security duties, or other activities specifically identified under the provisions of § 154.65.

(c) Access by subjects of personnel security investigative reports shall be afforded in accordance with 32 CFR part 286a.

(d) Access to personnel security clearance determination information shall be made available, other than provided for in paragraph (c) of this

section, through security channels, only to DoD or other officials of the Federal Government who have an official need for such information.

§ 154.68 Safeguarding procedures.

Personnel security investigative reports and personnel security determination information shall be safeguarded as follows:

(a) Authorized requesters shall control and maintain accountability of all reports of investigation received.

(b) Reproduction, in whole or in part, of personnel security investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

(c) Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lockbar and an approved three-position dial-type combination padlock or in a similarly protected area/container.

(d) Reports of DoD personnel security investigations shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows:

TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATION

(e) An individual's status with respect to a personnel security clearance or a Special Access authorization is to be protected as provided for in 32 CFR part 286.

§ 154.69 Records disposition.

(a) Personnel security investigative reports, to include OPM NACIs may be retained by DoD recipient organizations, only for the period necessary to complete the purpose for which it was originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with 32 CFR part 159.

(b) DoD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor derogatory nature 15 years after the date of the last action. That is, after the completion date of the investigation or the date on which the record was last released to an authorized user—whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of a significant nature due to information contained in the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and those of widespread public or congressional interest may be offered to the National Archives after 15 years.

(c) Personnel security investigative reports on persons who are considered for affiliation with DoD will be destroyed after 1 year if the affiliation is not completed.

§ 154.70 Foreign source information.

Information that is classified by a foreign government is exempt from public disclosure under the Freedom of Information and Privacy Acts. Further, information provided by foreign governments requesting an express promise of confidentiality shall be released only in a manner that will not identify or allow unauthorized persons to identify the foreign agency concerned.

Subpart K—Program Management

§ 154.75 General.

To ensure uniform implementation of the DoD personnel security program throughout the Department, program responsibility shall be centralized at DoD Component level.

§ 154.76 Responsibilities.

(a) The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31)) shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security

program matters within the Department:

(1) Provide program management through issuance of policy and operating guidance.

(2) Provide staff assistance to the DoD Components and defense agencies in resolving day-to-day security policy and operating problems.

(3) Conduct inspections of the DoD Components for implementation and compliance with DoD security policy and operating procedures.

(4) Provide policy, oversight, and guidance to the component adjudication functions.

(5) Approve, coordinate and oversee all DoD personnel security research initiatives and activities.

(b) The General Counsel shall ensure that the program is administered in a manner consistent with the laws; all proceedings are promptly initiated and expeditiously completed; and that the rights of individuals involved are protected, consistent with the interests of national security. The General Counsel shall also ensure that all relevant decisions of the courts and legislative initiatives of the Congress are obtained on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DoD personnel security program management authorities.

(c) The Heads of the Components shall ensure that:

(1) The DoD personnel security program is administered within their area of responsibility in a manner consistent with this part.

(2) A single authority within the office of the head of the DoD Component is assigned responsibility for administering the program within the Component.

(3) Information and recommendations are provided the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31)) and the General Counsel at their request concerning any aspect of the program.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61026, Nov. 19, 1993]

§ 154.77 Reporting requirements.

(a) The OASD(C31) shall be provided personnel security program management data by the Defense Data Manpower Center (DMDC) by December 31 each year for the preceding fiscal year. To facilitate accurate preparation of this report, all adjudicative determinations must be entered into the DC11 by all DoD central adjudication facilities no later than the end of the fiscal year. The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report shall cover the preceding fiscal year, broken out by clearance category, according to military (officer or enlisted), civilian or contractor status and by the central adjudication facility that took the action, using the enclosed format:

(1) Number of Top Secret, Secret, and Confidential clearances issued;

(2) Number of Top Secret, Secret, and Confidential clearances denied;

(3) Number of Top Secret, Secret, and Confidential clearances revoked;

(4) Number of SCI access determinations issued;

(5) Number of SCI access determinations denied;

(6) Number of SCI access determinations revoked; and

(7) Total number of personnel holding a clearance for Top Secret, Secret, Confidential and Sensitive Compartmented Information as of the end of the fiscal year.

(b) The Defense Investigative Service (DIS) shall provide the OASD(C3I) a quarterly report that reflects investigative cases opened and closed during the most recent quarter, by case category type, and by major requester. The information provided by DIS is essential for evaluating statistical data regarding investigative workload and the manpower required to perform personnel security investigations. Case category types include National Agency Checks (NACs); Expanded NACs; Single Scope Background Investigations (SSBIs), Periodic Reinvestigations (PRs); Secret Periodic Reinvestigations (SPRs); Post Adjudicative (PA); Special Investigative Inquiries (SIIs); and Limited Inquiries (LIs). This report shall be forwarded to OASD(C3I) within 45 days after the end of each quarter.

(c) The reporting requirement for DMDC and DIS has been assigned Report Control Symbol DD-C3I(A) 1749.

[58 FR 61026, Nov. 19, 1993]

§ 154.78 Inspections.

The heads of DoD Components shall assure that personnel security program matters are included in their administrative inspection programs.

APPENDIX A TO PART 154—INVESTIGATIVE SCOPE

This appendix prescribes the scope of the various types of personnel security investigations.

1. *National Agency Check (NAC).* Components of a NAC. At a minimum, the first three of the described agencies (DCII, FBI/HQ, and FBI/ID) below shall be included in each complete NAC; however, a NAC may also include a check of any or all of the other described agencies, if appropriate.

a. DCII records consist of an alphabetical index of personal names and impersonal titles that appear as subjects or incidentals in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the three military departments, DIS, Defense Criminal Investigative Service (DCIS), and the National Security Agency. DCII records will be checked on all subjects of DoD investigations.

b. FBI/HQ has on file copies of investigations conducted by the FBI. The FBI/HQ check, included in every NAC, consists of a review of files for information of a security nature and that developed during applicant-type investigations.

c. An FBI/ID check, included in every NAC (but not ENTNAC), is based upon a technical fingerprint search that consists of a classification of the subject's fingerprints and comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a ''name check only'' of these files is automatically conducted.

d. OPM. The files of OPM contain the results of investigations conducted by OPM under Executive Orders 9835 and 10450, those requested by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE) and those requested since August 1952 to serve as a basis for ''Q'' clearances. Prior to that date, ''Q'' clearance investigations were conducted by the FBI. A ''Q'' clearance is granted to individuals who require access to DOE information. In order to receive a ''Q'' clearance, a full field background investigation must be completed on the individual requiring access in accordance with the Atomic Energy Act of 1954. Also on file are the results of investigations on the operation of the Merit System, violations of the Veterans Preference Act, appeals of various types, fraud and collusion in Civil Service examinations and related matters, data on all Federal employment, and an index of all BIs on civilian employees or applicants completed by agencies of the Executive Branch of the U.S. Government. The OPM files may also contain information relative to U.S. citizens who are, or who were, employed by a United Nations organization or other public international organization such as the Organization of American States. OPM records are checked on all persons who are, or who have been, civilian employees of the U.S. Government; or U.S. citizens who are, or who have been, employed by a United Nations organization or other public international organization; and on those who have been granted security clearances by the NRC or DOE.

e. Immigration and Naturalization Service (I&NS). The files of I&NS contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declaration of intention, visitors' visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the U.S. I&NS records are checked when the subject is:

(1) An alien in the U.S., or

(2) A naturalized citizen whose naturalization has not been verified, or

(3) An immigrant alien, or

(4) A U.S. citizen who receives derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

f. State Department. The State Department maintains the following records:

(1) Security Division (S/D) files contain information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

(2) Passport Division (P/D) shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where he was born. Verification of this registration is verification of citizenship.

g. Central Intelligence Agency (CIA). The files of CIA contain information on present and former employees, including members of the Office of Strategic Services (OSS), applicants for employment, foreign nationals, including immigrant aliens in the U.S., and

U.S. citizens traveling outside the U.S. after July 1, 1946. These files shall be checked under the following guidelines.

Investigation	Criteria for CIA Checks
NAC, DNACI or ENTNAC.	Residence anywhere outside of the U.S. for a year or more since age 18 except under the auspices of the U.S. Government; and, travel, education, residence, or employment since age 18 in any designated country (Appendix G).
BI	Same as NAC, DNACI, and ENTNAC requirements plus travel, residence, employment, and education outside the U.S. for more than a continuous 3-month period during the past 5 years, or since age 18, except when under the auspices of the Government.
SBI	Same as BI requirements except the period of the investigation will cover the past 15 years, or since age 18. Also when subject's employment, education or residence has occurred overseas for a period of more than one year under the auspices of the U.S. Government, such checks will be made.

These files shall also be checked if subject has been an employee of CIA or when other sources indicate that CIA may have pertinent information.

h. Military Personnel Record Center files are maintained by separate departments of the Armed Forces, General Services Administration and the Reserve Records Centers. They consist of the Master Personnel Records of retired, separated, reserve, and active duty members of the Armed Force. These records shall be checked when the requester provides required identifying data indicating service during the last 15 years.

i. Treasury Department. The files of Treasury Department agencies (Secret Service, Internal Revenue Service, and Bureau of Customs) will be checked only when available information indicates that an agency of the Treasury Department may be reasonably expected to have pertinent information.

j. The files of other agencies such as the National Guard Bureau, the Defense Industrial Security Clearance Office (DISCO), etc., will be checked when pertinent to the purpose for which the investigation is being conducted.

2. *DoD National Agency Check plus Written Inquires (DNACI):*

a. *Scope:* The time period covered by the DNACI is limited to the most recent five (5) years, or since the 18th birthday, whichever is shorter, provided that the investigation covers at least the last two (2) full years of the subject's life, although it may be extended to the period necessary to resolve any questionable or derogatory information. No investigation will be conducted prior to an individual's 16th birthday. All DNACI investigation information will be entered on the DD Form 398–2 and FD-Form 258 and forwarded to the Defense Investigative Service (paragraph D, Appendix B).

b. *Components of a DNACI:*

(1) *NAC.* This is the same as described in paragraph 1, above.

(2) *Credit.* (a) A credit bureau check will be conducted to cover the 50 States, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, at all locations where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months (cumulative) during the past five (5) years.

(b) When information developed reflects unfavorably upon a person's current credit reputation or financial responsibility, the investigation will be expanded as necessary.

(3) *Employment*—(a) *Non-Federal Employment. (1)* Verify, via written inquiry, all employment within the period of investigation with a duration of six (6) months or more. Current employment will be checked regardless of duration.

(2) If all previous employments have been less than 6 months long, the most recent employment, in addition to the current, will be checked in all cases.

(3) Seasonal holiday, part-time and temporary employment need not be checked unless subparagraph 2 above applies.

(b) *Federal employment.* All Federal employment (to include military assignments) within the period of investigation will be verified by the requester through locally available records, and a statement reflecting that such checks have been favorably accomplished will be contained in the investigative request. Those that cannot be verified in this fashion will be accomplished via written inquiry by DIS (within the 50 United States, Puerto Rico, Guam, and the Virgin Islands).

3. *Background Investigation (BI).* The period of investigation for the BI is 5 years and applies to military, civilian, and contractor personnel.

a. *NAC.* See paragraph 1, above.

b. *Local Agency Checks (LAC).* Same as paragraph 4j, below, except period of coverage is five years.

c. *Credit checks.* Same as paragraph 4i, below.

d. *SUBJECT Interview (SI).* This is the principal component of a BI. In some instances an issue will arise after the primary SI and a secondary interview will be conducted. Interviews in the latter category are normally ''issue'' interviews that will be reported in the standard BI narrative format.

e. *Employment records.* Employment records will be checked at all places where employment references are interviewed with the exception of current Federal employment when the requester indicates that such employment has been verified with favorable results.

f. *Employment reference coverage.* A minimum of *three references, either supervisors or*

co-workers, who have knowledge of the SUBJECT's activities in the work environment will be interviewed. At least one employment reference at the current place of employment will always be interviewed with the exception of an individual attending military basic training, or other military training schools lasting less than 90 days. However, if the SUBJECT has only been at the current employment for less than 6 months, it will be necessary to go not only to his or her current employment (for example, for one employment reference) but also to the preceding employment of at least 6 months for additional employment references. If the SUBJECT has not had prior employment of at least 6 months, interview(s) will be conducted at the most recent short-term employment in addition to the current employment.

g. *Developed and Listed Character References*. A minimum of three developed character references (DCR) whose combined association with the SUBJECT covers the entire period of investigation will be interviewed. If coverage cannot be obtained through the DCRs, listed character reference (LCR) will be contacted to obtain coverage.

h. *Unfavorable information*. Unfavorable information developed in the field will be expanded.

4. *Special Background Investigation (SBI)*—a. *Components of an SBI*. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is the shorter period, provided that the investigation covers at least the last 2 full years of the subject's life. No investigation will be conducted for the period prior to an individual's 16th birthday. Emphasis shall be placed on peer coverage whenever interviews are held with personal sources in making education, employment, and reference (including developed) contact.

b. *NAC*. In addition to conducting a NAC on the subject of the investigation, the following additional requirements apply.

(1) A DCII, FBI/ID name check only and FBI/HQ check shall be conducted on subject's current spouse or cohabitant. In addition, such other national agency checks as deemed appropriate based on information on the subject's SPH or PSQ shall be conducted.

(2) A check of FBI/HQ files on members of subject's immediate family who are aliens in the U.S. or immigrant aliens who are 18 years of age or older shall be conducted. As used throughout the part, members of subject's immediate family include the following:

(a) Current spouse.

(b) Adult children, 18 years of age or older, by birth, adoption, or marriage.

(c) Natural, adopted, foster, or stepparents.

(d) Guardians.

(e) Brothers and sisters either by birth, adoption, or remarriage of either parent.

(3) The files of CIA shall be reviewed on alien members of subject's immediate family who are 18 years of age or older, regardless of whether or not these persons reside in the U.S.

(4) I&NS files on members of subject's immediate family 18 years of age or older shall be reviewed when they are:

(a) Aliens in the U.S., or

(b) Naturalized U.S. citizens whose naturalization has not been verified in a prior investigation, or

(c) Immigrant aliens, or

(d) U.S. citizens born in a foreign country of American parent(s) or U.S. citizens who received derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

c. *Birth*. Verify subject's date and place of birth (DPOB) through education, employment and/or other records. Verify through Bureau of Vital Statistics (BVS) records if not otherwise verified under d., below, or if a variance is developed.

d. *Citizenship*. Subject's citizenship status must be verified in all cases. U.S. citizens who are subjects of investigation will be required to produce documentation that will confirm their citizenship. Normally such documentation should be presented to the DoD Component concerned prior to the initiation of the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that the designated authority in the DoD Component will be provided with the documentation prior to the issuance of a clearance. DIS will not check the BVS for native-born U.S. citizens except as indicated in 4.c. above. In the case of foreign-born U.S. citizens, DIS will check I&NS records. The citizenship status of all foreign-born members of subject's immediate family shall be verified. Additionally, when the investigation indicates that a member of subject's immediate family has not obtained U.S. citizenship after having been eligible for a considerable period of time, an attempt should be made to determine the reason. The documents listed below are acceptable for proof of U.S. citizenship for personnel security determination purposes:

(1) A birth certificate must be presented if the individual was born in the United States. To be acceptable, the certificate must show that the birth record was filed shortly after birth and must be certified with the registrar's signature and the raised, impressed, or multicolored seal of his office except for States or jurisdictions which, as a matter of policy, do not issue certificates with a raised or impressed seal. Uncertified copies of birth certificates are not acceptable.

(a) A delayed birth certificate (a record filed more than one year after the date of birth) is acceptable provided that it shows

that the report of birth was supported by acceptable secondary evidence of birth as described in subparagraph (b), below.

(b) If such primary evidence is not obtainable, a notice from the registrar stating that no birth record exists should be submitted. The notice shall be accompanied by the best combination of secondary evidence obtainable. Such evidence may include a baptismal certificate, a certificate of circumcision, a hospital birth record, affidavits of persons having personal knowledge of the facts of the birth, or other documentary evidence such as early census, school, or family bible records, newspaper files and insurance papers. Secondary evidence should have been created as close to the time of birth as possible.

(c) All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

(2) A certificate of naturalization shall be submitted if the individual claims citizenship by naturalization.

(3) A certificate of citizenship issued by the I&NS shall be submitted if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

(4) A Report of Birth Abroad of A Citizen of The United States of America (Form FS–240), a Certification of Birth (Form FS–545 or DS–1350), or a Certificate of Citizenship is acceptable if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

(5) A passport or one in which the individual was included will be accepted as proof of citizenship.

e. *Education.* (1) Verify graduation or attendance at institutions of higher learning in the U.S. within the last 15 years, if such attendance was not verified during a prior investigation.

(2) Attempts will be made to review records at overseas educational institutions when the subject resided overseas in excess of one year.

(3) Verify attendance or graduation at the last secondary school attended within the past 10 years if there was no attendance at an institution of higher learning within the period of investigation.

(4) Verification of attendance at military academies is only required when the subject failed to graduate.

f. *Employment.* (1) Non-Federal employment. Verify all employment within the period of investigation to include seasonal, holiday, Christmas, part-time, and temporary employment. Interview one supervisor and one co-worker at subject's current place of employment as well as at each prior place of employment during the past 10 years of six months duration or longer. The interview requirement for supervisors and coworkers does not apply to seasonal, holiday, Christmas, part-time, and temporary employment (4 months or less) unless there are unfavorable issues to resolve or the letter of inquiry provides insufficient information.

(2) *Federal employment.* All Federal employment will be verified within the period of investigation to include Christmas, seasonal temporary, summer hire, part-time, and holiday employment. Do not verify Federal employment through review of records if already verified by the requester. If Federal employment has not been verified by the requester, then subject's personnel file at his/her current place of employment will be reviewed. All previous Federal employment will be verified during this review. In the case of former Federal employees, records shall be examined at the Federal Records Center in St. Louis, Missouri. Interview one supervisor and one co-worker at all places of employment during the past 10 years if so employed for 6 months or more.

(3) *Military employment.* Military service for the last 15 years shall be verified. The subject's duty station, for the purpose of interview coverage, is considered as a place of employment. One supervisor and one co-worker shall be interviewed at subject's current duty station if subject has been stationed there for 6 months or more; additionally, a supervisor and a co-worker at subject's prior duty stations where assigned for 6 months or more during the past 10 years shall be interviewed.

(4) *Unemployment.* Subject's activities during all periods of unemployment in excess of 30 consecutive days, within the period of investigation, that are not otherwise accounted for shall be verified.

(5) When an individual has resided outside the U.S. continuously for over one year, attempts will be made to confirm overseas employments as well as conduct required interviews of a supervisor and co-worker.

g. *References.* Three developed character references who have sufficient knowledge of subject to comment on his background, suitability, and loyalty shall be interviewed personally. Efforts shall be made to interview developed references whose combined association with subject covers the full period of the investigation with particular emphasis on the last 5 years. Employment, education, and neighborhood references, in addition to the required ones, may be used as developed references provided that they have personal knowledge concerning the individual's character, discretion, and loyalty. Listed character references will be interviewed only when developed references are not available or when it is necessary to identify and locate additional developed character references or when it is necessary to verify subject's activities (e.g., unemployment).

h. *Neighborhood investigation.* Conduct a neighborhood investigation to verify each of subject's residences in the U.S. of a period of 6 months or more on a cumulative basis, during the past 5 years or during the period of

investigation, whichever is shorter. During each neighborhood investigation, interview two neighbors who can verify subject's period of residence in that area and who were sufficiently acquainted to comment on subject's suitability for a position of trust. Neighborhood investigations will be expanded beyond this 5-year period only when there is unfavorable information to resolve in the investigation.

i. *Credit.* Conduct credit bureau check in the 50 States, the District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided) at all places where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months or more, on a cumulative basis, during the last 7 years or during the period of the investigation, whichever is shorter. When coverage by a credit bureau is not available, credit references located in that area will be interviewed. Financial responsibility, including unexplained affluence, will be stressed in all reference interviews.

j. *Local Agency Checks (LAC's).* LACs, including State central criminal history record repositories, will be conducted on subject at all places of residence to include duty stations and/or home ports, in the 50 States, the District of Columbia, and Puerto Rico, where residence occurred during the past 15 years or during the period of investigation, whichever is shorter. If subject's place of employment and/or education is serviced by a different law enforcement agency than that servicing the area of residence, LACs shall be conducted also in these areas.

k. *Foreign travel.* If subject has been employed, educated, traveled or resided outside of the U.S. for more than 90 days during the period of investigation, except under the auspices of the U.S. Government, additional record checks during the NAC shall be made in accordance with paragraph 1.f. of this Appendix. In addition, the following requirements apply:

(1) Foreign travel not under the auspices of the U.S. Government. When employment, education, or residence has occurred overseas for more than 90 days during the past 15 years or since age 18, which was not under the auspices of the U.S. Government, a check of records will be made at the Passport Office of the Department of State, the CIA, and other appropriate agencies. Efforts shall be made to develop sources, generally in the U.S., who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. If the individual has worked or lived outside of the U.S. continuously for over one year, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

(2) Foreign travel under the auspices of the U.S. Government. When employment, education, or residence has occurred overseas for a period of more than one year, under the auspices of the U.S. Government, a record check will be made at the Passport Office of the Department of State, the CIA and other appropriate agencies. Efforts shall be made to develop sources (generally in the U.S.) who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. Additionally, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

1. *Foreign connections.* All foreign connections (friends, relatives, and/or business connections) of subject and immediate family in the U.S. or abroad, except where such association was the direct result of subject's official duties with the U.S. Government, shall be ascertained. Investigation shall be directed toward determining the significance of foreign connections on the part of subject and the immediate family, particularly where the association is or has been with persons whose origin was within a country whose national interests are inimical to those of the U.S. When subject or his spouse has close relatives residing in a Communist-controlled country, or subject has resided, visited, or traveled in such a country, not under U.S. Government auspices, the provisions of §154.8(i)(3) of this part apply.

m. *Organizations.* Efforts will be made during reference interviews and record reviews to determine if subject and/or the immediate family has, or formerly had, membership in, affiliation with, sympathetic association towards, or participated in any foreign or domestic organization, association, movement, group, or combination of persons of the type described in §154.7(a) through (d) of this part.

n. *Divorce.* Divorces, annulments, and legal separations of subject shall be verified only when there is reason to believe that the grounds for the action could reflect on subject's suitability for a position of trust.

o. *Military service.* All military service and types of discharge during the last 15 years shall be verified.

p. *Medical records.* Medical records shall not be reviewed unless:

(1) The requester indicates that subject's medical records were unavailable for review prior to submitting the request for investigation, or

(2) The requester indicates that unfavorable information is contained in subject's medical records, or

(3) The subject lists one or more of the following on the SPH or PSQ:

(a) A history of mental or nervous disorders.

(b) That subject is now or has been addicted to the use of habit-forming drugs such as narcotics or barbiturates or is now or has been a chronic user to excess of alcoholic beverages.

q. *Updating a previous investigation to SBI standards.* If a previous investigation does not substantially meet the minimum standards of an SBI or if it is more than 5 years old, a current investigation is required but may be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements of an SBI. Should new information be developed during the current investigation that bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

5. *Periodic Reinvestigation (PR).* a. Each DoD military, civilian, consultant and contractor employee (to include non-U.S. citizens (foreign nationals and/or immigrant aliens) holding a limited access authorization) occupying a critical sensitive position, possessing a TOP SECRET clearance, or occupying a special access program position shall be the subject of a PR initiated 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

b. *Minimum investigative requirements.* A PR shall include the following minimum scope.

(1) *NAC.* A valid NAC on the SUBJECT will be conducted in all cases. Additionally, for positions requiring SCI access, checks of DCII, FBI/HQ, FBI/ID name check only, and other agencies deemed appropriate, will be conducted on the SUBJECT's current spouse or cohabitant, if not previously conducted. Additionally, NACs will be conducted on immediate family members, 18 years of age or older, who are aliens and/or immigrant aliens, if not previously accomplished.

(2) *Credit.* Credit bureau checks covering all places where the SUBJECT resided for 6 months or more, on a cumulative basis, during the period of investigation, in the 50 States, District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided), will be conducted.

(3) *Subject interview.* The interview should cover the entire period of time since the last investigation, not just the last 5-year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, need not be explored again unless additional relevant information warrants further coverage. An SI is not required if one of the following conditions exists:

(a) The SUBJECT is aboard a deployed ship or in some remote area that would cause the interview to be excessively delayed.

(b) The SUBJECT is in an overseas location serviced by the State Department or the FBI.

(4) *Employment.* Current employment will be verified. Military and Federal service records will not routinely be checked, if previously checked by the requester when PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted. Records need be checked only when they are locally available, unless unfavorable information has been detected.

(5) *Employment references.* Two supervisors or co-workers at the most recent place of employment or duty station of 6 months; if the current employment is less than 6 months employment reference interviews will be conducted at the next prior place of employment, which was at least a 6-month duration.

(6) *Developed Character References (DCRs).* Two developed character references who are knowledgeable of the SUBJECT will be interviewed. Developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

(7) *Local Agency Checks (LACs).* DIS will conduct local agency checks on the SUBJECT at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations.

(8) *Neighborhood Investigation.* Conduct a neighborhood investigation to verify subjects' current residence in the United States. Two neighbors who can verify subject's period of residence in that area and who are sufficiently acquainted to comment on the subject's suitability for a position of trust will be interviewed. Neighborhood investigations will be expanded beyond the current residence when unfavorable information arises.

(9) *Ex-spouse interview.* If the subject of investigation is divorced, the ex-spouse will be interviewed when the date of final divorce action is within the period of investigation.

(10) *Select scoping.* When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61026, Nov. 19, 1993]

APPENDIX B TO PART 154—REQUEST PROCEDURES

A. *General.* To conserve investigative resources and to insure that personnel security investigations are limited to those essential

to current operations and are clearly authorized by DoD policies, organizations requesting investigations must assure that continuing command attention is given to the investigative request process.

In this connection, it is particularly important that the provision of Executive Order 12356 requiring strict limitations on the dissemination of official information and material be closely adhered to and that investigations requested for issuing clearances are limited to those instances in which an individual has a clear need for access to classified information. Similarly, investigations required to determine eligibility for appointment or retention in DoD, in either a civilian or military capacity, must not be requested in frequency or scope exceeding that provided for in this part.

In view of the foregoing, the following guidelines have been developed to simplify and facilitate the investigative request process:

1. Limit requests for investigation to those that are essential to current operations and clearly authorized by DoD policies and attempt to utilize individuals who, under the provisions of this part, have already met the security standard;

2. Assure that military personnel on whom investigative requests are initiated will have sufficient time remaining in service after completion of the investigation to warrant conducting it;

3. Insure that request forms and prescribed documentation are properly executed in accordance with instructions;

4. Dispatch the request directly to the DIS Personnel Investigations Center;

5. Promptly notify the DIS Personnel Investigations Center if the investigation is no longer needed (notify OPM if a NACI is no longer needed); and

6. Limit access through strict need-to-know, thereby requiring fewer investigations.

In summary, close observance of the above-cited guidelines will allow the DIS to operate more efficiently and permit more effective, timely, and responsive service in accomplishing investigations.

B. *National Agency Check (NAC).* When a NAC is requested an original only of the DD Form 398–2 (National Agency Check Request) and a completed FD 258 (Applicant Fingerprint Card) are required. If the request is for an ENTNANC, an original only of the DD Form 398–2 and a completed DD Form 2280 (Armed Forces Fingerprint Card) are required. Those forms should be sent directly to: Personnel Investigation Center, Defense Investigative Service, P.O. Box 1083, Baltimore, Maryland 21203.

C. *National Agency Check plus written Inquiries (NACI).* When a NACI is requested, an original and one copy of the SF 85 (Data for Nonsensitive or Noncritical-sensitive Position), an SF 171 (Personal Qualifications Statement), and an SF 87 (U.S. Civil Service Commission Fingerprint Chart) shall be sent directly to: Office of Personnel Management, Bureau of Personnel Investigations, NACI Center, Boyers, Pennsylvania 16018.

The notation ''ALL REFERENCES'' shall be stamped immediately above the title at the top of the Standard Form 85.

D. *DoD National Agency Check with Inquiries (DNACI).* 1. When a DNACI is requested, one copy of DD Form 1879, an original and two copies of the DD Form 398–2 (National Agency Check Request), two copies of FD 258 (Fingerprint Card), and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to: Personnel Investigations Center, Defense Investigative Service, P.O. Box 1083, Baltimore, Maryland 21203.

2. The DD Form 398–2 must be completed to cover the most recent five year period. All information, to include items relative to residences and employment, must be complete and accurate to avoid delays in processing.

E. *Special Background Investigation (SBI)/ Background Investigation (BI).* 1. When requesting a BI or SBI, one copy of DD Form 1879 (Request for Personnel Security Investigation), an original and four copies of DD Form 398 (Statement of Personnel History), two copies of FD 258, and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to the: Personnel Investigations Center, Defense Investigative Service, P.O. Box 454, Baltimore, Maryland 21203.

2. For the BI and SBI, the DD Form 398 must be completed to cover the most recent five and 15 year period, respectively, or since the 18th birthday, whichever is shorter.

F. *Periodic Reinvestigation (PR).* 1. PRs shall be requested only in such cases as are authorized by §154.19 (a) through (k) of this part.

a. For a PR requested in accordance with §154.19 (a) and (k) and the DD Form 1879 must be accompanied by the following documents:

(1) Original and four copies of DD Form 398.

(2) Two copies of FD–258.

(3) Original copy of DD Form 2221.

b. In processing PRs, previous investigative reports will not be requested by the requesting organization, unless significant derogatory or adverse information, postdating the most recent favorable adjudication, is developed during the course of reviewing other locally available records. In the latter instance, requests for previous investigative reports may only be made if it is determined by the requesting organization that the derogatory information is so significant that a review of previous investigative reports is

necessary for current adjudicative determinations.

2. No abbreviated version of DD Form 398 may be submitted in connection with a PR.

3. The PR request shall be sent to the address in paragraph E.1.

G. *Additional investigation to resolve derogatory or adverse information.* 1. Requests for additional investigation required to resolve derogatory or adverse information shall be submitted by DD Form 1879 (Request for Personnel Security Investigation) to the: Defense Investigative Service, P.O. Box 454, Baltimore, Maryland 21203.

Such requests shall set forth the basis for the additional investigation and describe the specific matter to be substantiated or disproved.

2. The request should be accompanied by an original and four copies of the DD Form 398, where appropriate, two copies of FD–258 and an original copy of DD Form 2221, unless such documentation was submitted within the last 12 months to DIS as part of a NAC or other personnel security investigation. If pertinent, the results of a recently completed NAC, NACI, or other related investigative reports available should also accompany the request.

H. *Obtaining results of prior investigations.* Requesters requiring verification of a specified type of personnel security investigation, and/or requiring copies of prior investigations conducted by the DIS shall submit requests by letter or message to: Defense Investigative Service Investigative Files Division, P.O. Box 1211, Baltimore, Maryland 21203, Message Address: DIS PIC BALTIMORE MD/ /D0640.

The request will include subject's name, grade, social security number, date and place of birth, and DIS case control number if known.

I. *Requesting postadjudication cases.* 1. Requests pertaining to issues arising after adjudication of an investigation (postadjudication cases) shall be addressed to DIS on a DD Form 1879 accompanied by a DD Form 398, where appropriate.

2. All requests for initial investigations will be submitted to PIC regardless of their urgency. If, however, there is an urgent need for a postadjudication investigation, or the mailing of a request to PIC for initiation of a postadjudication case would prejudice timely pursuit of investigative action, the DD Form 1879 may be directed for initiation, in CONUS, to the nearest DIS Field Office, and in overseas locations, to the military investigative service element supporting the requester (Appendix I). The field element (either DIS or the military investigative agency) will subsequently forward either the DD Form 1879 or completed investigation to PIC.

3. A fully executed DD Form 1879 and appropriate supporting documents may not be immediately available. Further, a case that is based on sensitive security issues may be compromised by a request that the subject submit a DD Form 398. A brief explanation should appear on DD Form 1879s which does not include complete supporting documentation.

J. *Requests involving contractor employees.* To preclude duplicative investigative requests and double handling of contractor employee cases involving access to classified information, all requests for investigation of contractor personnel must be submitted, using authorized industrial security clearance forms, for processing through the Defense Industrial Security Clearance Office, except for programs in which specific approval has been obtained from the Deputy Under Secretary of Defense for Policy to utilize other procedures.

K. *Responsibility for proper documentation of requests.* The official signing the request for investigation shall be responsible for insuring that all documentation is completed in accordance with these instructions.

APPENDIX C TO PART 154—TABLES FOR REQUESTING INVESTIGATIONS

GUIDE FOR REQUESTING BACKGROUND INVESTIGATIONS (BI) (TABLE 1)

A If the individual is a:	B And duties require:	C Then a BI is required before:
U.S. national military member, civilian, consultant, or contractor employee.	Top Secret clearance	Granting final clearance.
U.S. national civilian employee	Assignment to a ''Critical'' sensitive position.	Assignment to the position.
U.S. national military member, DoD civilian or contractor employee.	Occupying a ''critical'' position in the Nuclear Weapon Personnel Reliability Program (PRP).	Occupying a ''critical'' position.
U.S. national military member or civilian employee.	Granting, denying clearances	Performing clearance functions.
U.S. national military member or civilian employee.	Membership on security screening, hearing, or review board.	Appointment to the board.
Immigrant alien	Limited access to Secret or Confidential information.	Issuing limited access authorization (Note 1).

GUIDE FOR REQUESTING BACKGROUND INVESTIGATIONS (BI) (TABLE 1)—Continued

A If the individual is a:	B And duties require:	C Then a BI is required before:
Non-U.S. national employee excluding immigrant alien.	Limited access to Secret or Confidential information.	Issuing limited access authorization.
Non-U.S. national nominee military education and orientation program (from a country listed at Appendix G).	Education and orientation for of military personnel.	Before performing duties.
U.S. national military member DoD civilian or contractor employee.	Assignment to a category two Presidential Support position.	Assignment.
U.S. national military member, DoD civilian or contractor employee assigned to NATO.	Access to NATO COSMIC information	Access may be granted.

Note 1: BI will cover a 10 year scope.

GUIDE FOR REQUESTING SPECIAL BACKGROUND INVESTIGATIONS (SBI) (TABLE 2)

A If the individual is a:	B And duties require:	C Then a SBI is required before:
U.S. national military member, DoD civilian, consultant, or contractor employee.	Access to SCI	Granting Access.
	Assisgnment to a category one Presidential Support position.	Assignment.
	Access to SIOP-ESI	Granting access.
	Assignment to the National Security Agency.	Assignment.
	Access to other Special Access programs approved under § 154.17(g).	Granting access.
	Assignment to personnel security, counterintelligence, or criminal investigative or direct investigative support duties.	Assignment.

GUIDE FOR REQUESTING PERIODIC REINVESTIGATIONS (PR) (TABLE 3)

A If the individual is a:	B And duties require:	C Then a PR is required before:
U.S. national military member, DoD civilian, consultant, or contractor employee.	Access to SCI	5 years from date of last SBI/BI or PR.
	Top Secret Clearance	5 years from date of last SBI/BI or PR.
	Access to NATO COSMIC	5 years from date of last SBI/BI or PR.
	Assignment to Presidential Support activities.	5 years from date of last SBI/BI or PR.
U.S. national civilian employee	Assignment to a ''Critical'' sensitive position.	5 years from last SBI/BI or PR.
Non-U.S. national employee	Current limited access authorization to Secret or Confidential information.	5 years from last SBI/BI or PR.

GUIDE FOR REQUESTING DOD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI) OR NACI (TABLE 4)

A If the individual is a:	B And duties require:	C Then DNACI/NACI is required
U.S. national military member or contractor	Secret clearance	Before granting clearance (note 1).
	.....	May be automatically issued (note 2).
	Interim Secret Clearance	
U.S. national civilian employee or consultant.	Secret clearance	Before granting clearance.
	Interim Secret Clearance	May be automatically issued (note 3).
	Appointment to ''Non Critical'' sensitive position.	Before appointment.
U.S. national military member, DoD civilian or contractor employee.	Occupying a ''controlled'' position in the Nuclear Weapon PRR.	Before assignment.

GUIDE FOR REQUESTING DOD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI) OR NACI (TABLE 4)—Continued

A If the individual is a:	B And duties require:	C Then DNACI/NACI is required
Applicant for appointment as a commissioned officer.	Commission in the Award Forces	Before appointment (after appointment for health professionals, chaplains, and attorneys, under conditions authorized by §154.15(d) of this part).
Naval Academy Midshipman, Military Academy Cadet, or Air Force Academy Cadet.	Enrollment	To be initiated 90 days after entry.
Reserve Officer Training Corps Cadet of Midshipman.	Entry to advanced course or College Scholarship Program.	Then a DNACI is required to be initiated 90 days after entry.

Note 1: First term enlistees shall require an ENTNAC.
Note 2: Provided DD Form 398–2 is favorably reviewed, local records check favorably accomplished, and DNACI initiated.
Note 3: Provided an authority designated in Appendix E finds delay in such appointment would be harmful to national security; favorable review of DD Form 398–2; NACI initiated; favorable local records check accomplished. Table 5.

GUIDE FOR REQUESTING NATIONAL AGENCY CHECKS (NAC) (TABLE 5)

A If the individual is a:	B And duties require:	C Then a NAC is required:
A first-term enlistee	Retention in the Armed Forces (including National Guard and Reserve).	To be initiated NLT three work days after entry (note 1).
Prior service member reentering military service after break in Federal employment exceeding 1 year.	Retention in the Armed Forces (including National Guard and Reserve).	To be initiated NLT three work days after reentry.
Nominee for military education and orientation program.	Education and orientation of military personnel.	Before performing duties (note 2).
U.S. national military, DoD civilian, or contractor employee.	Access to restricted areas, sensitive information, or equipment as defined in §154.18(b).	Before authorizing entry.
Nonappropriated fund instrumentality (NAFI) civilian employee.	Appointment as NAFI custodian	Before appointment.
	Accountability for non appropriated funds	Before completion of probationary period.
	Fiscal responsibility as determined by NAFI custodian.	Before completion of probationary period.
	Other ''positions of trust''	Before appointment.
Persons requiring access to chemical agents.	Access to or security of chemical agents	Before assignment.
U.S. national, civilian employee nominee for customs inspection duties.	Wavier under provisions of §154.18(d)	Before appointment (note 3).
Red Cross/United States Organization personnel.	Assignment with the Armed Forces overseas.	Before assignment (See note 4 for foreign national personnel).
U.S. national	DoD building pass	Prior to issuance.
Foreign national employed overseas	No access to classified information	Prior to employment (note 4).

Note 1: Request ENTNAC only.
Note 2: Except where personnel whose country of origin is a country listed at Appendix G, a BI will be required (See §154.18(1)).
Note 3: A NAC not over 5 years old suffices unless there has been a break in employment over 12 months. Then a current NAC is required.
Note 4: In such cases, the NAC shall consist of: (a) Host government law enforcement and security agency record checks at the city, state (province), and national level, and (b) DCII.

APPENDIX D TO PART 154—REPORTING OF NONDEROGATORY CASES

Background Investigation (BI) and Special Background Investigation (SBI) shall be considered as devoid of significant adverse information unless they contain information listed below:

1. Incidents, infractions, offenses, charges, citations, arrests, suspicion or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, unreliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

2. All indications of moral turpitude, heterosexual promiscuity, aberrant, deviant, or bizarre sexual conduct or behavior, transvestitism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, wife-swapping, window-peeping, and similar situations from whatever source. Unlisted full-time employment or education; full-time education or employment that cannot be verified by any

reference or record source or that contains indications of falsified education or employment experience. Records or testimony of employment, education, or military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness, or stability of the individual.

3. Foreign travel, education, visits, correspondence, relatives, or contact with persons from or living in a foreign country or foreign intelligence service.

4. Mental, nervous, emotional, psychological, psychiatric, or character disorders/behavior or treatment reported or alleged from any source.

5. Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy, or evidence of living beyond the individual's means.

6. Any other significant information relating to the criteria included in paragraphs (a) through (q) of §154.7 or Appendix H of this part.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61026, Nov. 19, 1993]

APPENDIX E TO PART 154—PERSONNEL SECURITY DETERMINATION AUTHORITIES

A. *Officials authorized to grant, deny or revoke personnel security clearances (Top Secret, Secret, and Confidential):*

1. Secretary of Defense and/or designee
2. Secretary of the Army and/or designee
3. Secretary of the Navy and/or designee
4. Secretary of the Air Force and/or designee
5. Chairman, Joint Chiefs of Staff and/or designee
6. Directors of the Defense Agencies and/or designee
7. Commanders of the Unified and Specified Commands and/or designee

B. *Officials authorized to grant Limited Access Authorizations:*

1. Secretaries of the Military Departments and/or designee
2. Director, Washington Headquarters Service for OSD and/or designee
3. Chairman, JCS and/or designee
4. Directors of the Defense Agencies and/or designee
5. Commanders, Unified and Specified Commands and/or designee

C. *Officials authorized to grant access to SCI:*

Director, NSA—for NSA
Director, DIA—for OSD, OJCS, and Defense Agencies
Senior Officers of the Intelligence Community of the Army, Navy, and Air Force—for their respective Military Departments, or their single designee.

D. Officials authorized to certify personnel under their jurisdiction for access to Restricted Data (to include Critical Nuclear Weapon Design Information): see enclosure to DoD Directive 5210.2.

E. Officials authorized to approve personnel for assignment to Presidential Support activities: The Executive Secretary to the Secretary and Deputy Secretary of Defense or designee.

F. *Officials authorized to grant access to SIOP-ESI:*

1. Director of Strategic Target Planning
2. Director, Joint Staff, OJCS
3. Chief of Staff, U.S. Army
4. Chief of Naval Operations
5. Chief of Staff, U.S. Air Force
6. Commandant of the Marine Corps
7. Commanders of Unified and Specified Commands
8. The authority to grant access delegated above may be further delegated in writing by the above officials to the appropriate subordinates.

G. *Officials authorized to designate sensitive positions:*

1. Heads of DoD Components or their designees for critical-sensitive positions.

2. Organizational commanders for noncritical-sensitive positions.

H. *Nonappropriated Fund Positions of Trust:*

Officials authorized to designate nonappropriated fund positions of trust: Heads of DoD Components and/or their designees.

APPENDIX F TO PART 154—GUIDELINES FOR CONDUCTING PRENOMINATION PERSONAL INTERVIEWS

A. *Purpose.* The purpose of the personal interview is to assist in determining the acceptability of an individual for nomination and further processing for a position requiring an SBI.

B. *Scope.* Questions asked during the course of a personal interview must have a relevance to a security determination. Care must be taken not to inject improper matters into the personal interview. For example, religious beliefs and affiliations, beliefs and opinions regarding racial matters, political beliefs and affiliations of a nonsubversive nature, opinions regarding the constitutionality of legislative policies, and affiliations with labor unions and fraternal organizations are not proper subjects for inquiry. Department of Defense representatives conducting personal interviews should always be prepared to explain the relevance of their inquiries. Adverse inferences shall not be drawn from the refusal of a person to answer questions the relevance of which has not been established.

C. *The interviewer.* Except as prescribed in paragraph B. above, persons conducting personal interviews normally will have broad

latitude in performing this essential and important function and, therefore, a high premium must necessarily be placed upon the exercise of good judgment and common sense. To insure that personal interviews are conducted in a manner that does not violate lawful civil and private rights or discourage lawful political activity in any of its forms, or intimidate free expression, it is necessary that interviewers have a keen and well-developed awareness of and respect for the rights of interviewees. Interviewers shall never offer an opinion as to the relevance or significance of information provided by the interviewee to eligibility for access to SCI. If explanation in this regard is required, the interviewer will indicate that the sole function of the interview is to obtain information and that the determination of relevance or significance to the individual's eligibility will be made by other designated officials.

D. *Interview procedures.* 1. The Head of the DoD Component concerned shall establish uniform procedures for conducting the interview that are designed to elicit information relevant to making a determination of whether the interviewee, on the basis of the interview and other locally available information (DD 398, Personnel Security Investigation Questionnaire, personnel records, security file, etc.), is considered acceptable for nomination and further processing.

2. Such procedures shall be structured to insure the interviewee his full rights under the Constitution of the United States, the Privacy Act of 1974 and other applicable statutes and regulations.

E. *Protection of interview results.* All information developed during the course of the interview shall be maintained in personnel security channels and made available only to those authorities who have a need-to-know in connection with the processing of an individual's nomination for duties requiring access to SCI or those who need access to information either to conduct the required SBI or to adjudicate the matter of the interviewee's eligibility for access to SCI, or as otherwise authorized by Executive order or statute.

F. *Acceptability determination.* 1. The determination of the interviewee's acceptability for nomination for duties requiring access to sensitive information shall be made by the commander, or designee, of the DoD organization that is considering nominating the interviewee for such duties.

2. Criteria guidelines contained in DCID 1/14 upon which the acceptability for nomination determination is to be based shall be provided to commanders of DoD organizations who may nominate individuals for access to SCI and shall be consistent with those established by the Senior Officer of the Intelligence Community of the Component concerned with respect to acceptability for nomination to duties requiring access to SCI.

APPENDIX G TO PART 154 [RESERVED]

APPENDIX H TO PART 154—ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

1. *Introduction.* The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees, and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in all final clearance determinations. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitments to the United States, including the commitment to protect classified information, and any other compelling loyalty. Accesses decisions also take into account a person's reliability, trustworthiness and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's secrets as the most effective means of protecting them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

2. *The adjudicative process.*

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) The nature, extent, and seriousness of the conduct;

(2) The circumstances surrounding the conduct, to include knowledgeable participation;
(3) The frequency and recency of the conduct;
(4) The individual's age and maturity at the time of the conduct;
(5) The extent to which participation is voluntary;
(6) The presence or absence of rehabilitation and other permanent behavioral changes;
(7) The motivation for the conduct;
(8) The potential for pressure, coercion, exploitation, or duress; and
(9) The likelihood of continuation or recurrence;
(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security.
(c) The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.
(1) GUIDELINE A: Allegiance to the United States;
(2) GUIDELINE B: Foreign Influence;
(3) GUIDELINE C: Foreign Preference;
(4) GUIDELINE D: Sexual Behavior;
(5) GUIDELINE E: Personal Conduct;
(6) GUIDELINE F: Financial Considerations;
(7) GUIDELINE G: Alcohol Consumption;
(8) GUIDELINE H: Drug Involvement;
(9) GUIDELINE I: Psychological Conditions;
(10) GUIDELINE J: Criminal Conduct;
(11) GUIDELINE K: Handling Protected Information;
(12) GUIDELINE L: Outside Activities;
(13) GUIDELINE M: Use of Information Technology Systems
(d) Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.
(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:
(1) Voluntarily reported the information;
(2) Was truthful and complete in responding to questions;
(3) Sought assistance and followed professional guidance, where appropriate;
(4) Resolved or appears likely to favorably resolve the security concern;
(5) Has demonstrated positive changes in behavior and employment;
(6) Should have his or her access temporarily suspended pending final adjudication of the information.
(f) If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

GUIDELINE A: ALLEGIANCE TO THE UNITED STATES

3. *The concern.* An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.
4. *Conditions that could raise a security concern and may be disqualifying include:*
(a) Involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America;
(b) Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
(c) Association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:
(1) Overthrow or influence the government of the United States or any state or local government;
(2) Prevent Federal, state, or local government personnel from performing their official duties;
(3) Gain retribution for perceived wrongs caused by the Federal, state, or local government;
(4) Prevent others from exercising their rights under the Constitution or laws of the United States or of any state.
5. *Conditions that could mitigate security concerns include:*
(a) The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
(b) The individual's involvement was only with the lawful or humanitarian aspects of such an organization;
(c) Involvement in the above activities occurred for only a short period of time and

was attributable to curiosity or academic interest;

(d) The involvement or association with such activities occurred under such unusual circumstances, or so much time has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

GUIDELINE B: FOREIGN INFLUENCE

6. *The concern.* Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

7. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) Connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(c) Counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

(d) Sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(e) A substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(f) Failure to report, when required, association with a foreign national;

(g) Unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

(h) Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;

(i) Conduct, especially while traveling outside the U.S., which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

8. *Conditions that could mitigate security concerns include:*

(a) The nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.;

(b) There is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;

(c) Contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation;

(d) The foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;

(e) The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country;

(f) The value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

GUIDELINE C: FOREIGN PREFERENCE

9. *The concern.* When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

10. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(1) Possession of a current foreign passport;

(2) Military service or a willingness to bear arms for a foreign country;

(3) Accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country;

(4) Residence in a foreign country to meet citizenship requirements;

(5) Using foreign citizenship to protect financial or business interests in another country;

(6) Seeking or holding political office in a foreign country;

(7) Voting in a foreign election;

(b) Action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(c) Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(d) Any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce United States citizenship; renunciation of United States citizenship.

11. *Conditions that could mitigate security concerns include:*

(a) Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(b) The individual has expressed a willingness to renounce dual citizenship;

(c) Exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor;

(d) Use of a foreign passport is approved by the cognizant security authority.

(e) The passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated;

(f) The vote in a foreign election was encouraged by the United States Government.

GUIDELINE D: SEXUAL BEHAVIOR

12. *The concern*. Sexual behavior that involves a criminal offense indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

13. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) A pattern of compulsive, self-destructive, or high risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

(c) Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

(d) Sexual behavior of a public nature and/or that reflects lack of discretion or judgment.

14. *Conditions that could mitigate security concerns include:*

(a) The behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) The sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(c) The behavior no longer serves as a basis for coercion, exploitation, or duress.

(d) The sexual behavior is strictly private, consensual, and discreet.

GUIDELINE E: PERSONAL CONDUCT

15. *The concern*. Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) Refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;

(b) Refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

16. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(b) Deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(c) Credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any

other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(d) Credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) Untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information:

(2) Disruptive, violent, or other inappropriate behavior in the workplace;

(3) A pattern of dishonesty or rule violations;

(4) Evidence of significant misuse of Government or other employer's time or resources;

(e) Personal conduct or concealment of information about one's conduct that creates a vulnerability to exploitation, manipulation, or duress, such as:

(1) Engaging in activities which, if known, may affect the person's personal, professional, or community standing, or

(2) While in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment;

(g) association with persons involved in criminal activity.

17. *Conditions that could mitigate security concerns include:*

(a) The individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) The refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully.

(c) The offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) The individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(e) The individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) The information was unsubstantiated or from a source of questionable reliability;

(g) Association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

GUIDELINE F: FINANCIAL CONSIDERATIONS

18. *The concern.* Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

19. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Inability or unwillingness to satisfy debts;

(b) Indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(c) A history of not meeting financial obligations;

(d) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

(e) Consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis;

(f) Financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern;

(g) Failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same;

(h) Unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income;

(i) Compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, ''chasing losses'' (i.e. increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

20. *Conditions that could mitigate security concerns include:*

(a) The behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) The conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances;

(c) The person has received or is receiving counseling for the problem and/or there are clear indications that the problem is being resolved or is under control;

(d) The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts;

(e) The individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue;

(f) The affluence resulted from a legal source of income.

GUIDELINE G: ALCOHOL CONSUMPTION

21. *The concern.* Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

22. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(b) Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(c) Habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent;

(d) Diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

(e) Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

(f) Relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program;

(g) Failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

23. *Conditions that could mitigate security concerns include:*

(a) So much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) The individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser);

(c) The individual is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress;

(d) The individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H: DRUG INVOLVEMENT

24. *The concern.* Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

(a) Drugs are defined as mood and behavior altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) Inhalants and other similar substances;

(b) Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

25. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Any drug abuse (see above definition);[1]

(b) Testing positive for illegal drug use;

(c) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) Diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

(e) Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(f) Failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(g) Any illegal drug use after being granted a security clearance;

(h) Expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

26. *Conditions that could mitigate security concerns include:*

(a) The behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) A demonstrated intent not to abuse any drugs in the future, such as:

(1) Disassociation from drug-using associates and contacts;

(2) Changing or avoiding the environment where drugs were used;

(3) An appropriate period of abstinence;

(4) A signed statement of intent with automatic revocation of clearance for any violation;

(c) Abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended;

(d) Satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

GUIDELINE I: PSYCHOLOGICAL CONDITIONS

27. *The concern.* Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (e.g., clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

28. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior;

(b) An opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness;[2]

(c) The individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition, e.g., failure to take prescribed medication.

29. *Conditions that could mitigate security concerns include:*

(a) The identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan;

(b) The individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional;

(c) Recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's previous condition is under control or in remission, and has a low probability of recurrence or exacerbation;

[1] Under the provisions of 10 U.S.C. 986 any person who is an unlawful user of, or is addicted to, a controlled substance as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802), may not be granted or have renewed their access to classified information.

[2] Under the provisions of 10 U.S.C. 986, any person who is mentally incompetent, as determined by a credentialed mental health professional approved by the Department of Defense, may not be granted or have renewed their access to classified information.

(d) The past emotional instability was a temporary condition (e.g., one caused by death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability;

(e) There is no indication of a current problem.

GUIDELINE J: CRIMINAL CONDUCT

30. *The concern.* Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

31. *Conditions that could raise a security concern and may be disqualifying include:*

(a) A single serious crime or multiple lesser offenses;

(b) Discharge or dismissal from the Armed Forces under dishonorable conditions;[3]

(c) Allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted;

(d) Individual is currently on parole or probation;

(e) Violation of parole or probation, or failure to complete a court-mandated rehabilitation program;

(f) Conviction in a Federal or State court, including a court-martial of a crime, sentenced to imprisonment for a term exceeding one year and incarcerated as a result of that sentence for not less than a year.[4]

32. *Conditions that could mitigate security concerns include:*

(a) So much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) The person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;

(c) Evidence that the person did not commit the offense;

(d) There is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement;

(e) Potentially disqualifying conditions 31. (b) and (f) may not be mitigated unless, where meritorious circumstances exist, the Secretaries of the Military Departments or designee; or the Directors of Washington Headquarters Services (WHS), Defense Intelligence Agency (DIA), National Security Agency (NSA), Defense Office of Hearings and Appeals (DOHA) or designee has granted a waiver.

GUIDELINE K: HANDLING PROTECTED INFORMATION

33. *The concern.* Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

34. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

(b) Collecting or storing classified or other protected information at home or in any other unauthorized location;

(c) Loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, ''palm'' or pocket device or other adjunct equipment;

(d) Inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

(e) Copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;

(f) Viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(g) Any failure to comply with rules for the protection of classified or other sensitive information;

(h) Negligence or lax security habits that persist despite counseling by management.

(i) Failure to comply with rules or regulations that results in damage to the National

[3] Under the provisions of 10 U.S.C. 986, a person who has received a dishonorable discharge or has been dismissed from the Armed Forces may not be granted or have renewed access to classified information. In a meritorious case, the Secretaries of the Military Departments or designee; or the Directors of WHS, DIA, NSA, DOHA or designee may authorize a waiver of this prohibition.

[4] Under the above mentioned statute, a person who has been convicted in a Federal or State court, including courts martial, sentenced to imprisonment for a term exceeding one year and incarcerated for not less than one year, may not be granted or have renewed access to classified information. The same waiver provision also applies.

Security, regardless of whether it was deliberate or negligent.

35. *Conditions that could mitigate security concerns include:*

(a) So much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) The individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) The security violations were due to improper or inadequate training.

GUIDELINE L: OUTSIDE ACTIVITIES

36. *The concern.* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

37. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Any employment or service, whether compensated or volunteer, with:

(1) The government of a foreign country;

(2) Any foreign national, organization, or other entity;

(3) A representative of any foreign interest;

(4) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(b) Failure to report or fully disclose an outside activity when this is required.

38. *Conditions that could mitigate security concerns include:*

(a) Evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States;

(b) The individual terminated the employment or discontinued the activity upon being notified that it was in conflict with his or her security responsibilities.

GUIDELINE M: USE OF INFORMATION TECHNOLOGY SYSTEMS

39. *The concern.* Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

40. *Conditions that could raise a security concern and may be disqualifying include:*

(a) Illegal or unauthorized entry into any information technology system or component thereof;

(b) Illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

(c) Use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) Downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) Unauthorized use of a government or other information technology system;

(f) Introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations;

(g) Negligence or lax security habits in handling information technology that persist despite counseling by management;

(h) Any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

41. *Conditions that could mitigate security concerns include:*

(a) So much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) The misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;

(c) The conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

[71 FR 51475, Aug. 30, 2006]

APPENDIX I TO PART 154—OVERSEAS INVESTIGATIONS

1. Purpose

The purpose of this appendix is to establish, within the framework of this part, 32 CFR part 361 and Defense Investigative Service Manual 20–1, standardized procedures for the military investigative agencies to follow when they perform administrative and investigative functions on behalf of DIS at overseas locations.

2. Type Investigation

This part describes in detail Background Investigations (BI) which are conducted for Limited Access Authorizations and those Special Investigative Inquiries conducted for post-adjudicative purposes. Hereafter they are referred to as LAA and Post-adjudicative cases and are briefly described in paragraphs a and b below:

a. *Limited access authorization.* A level of access to classified defense information that may be granted to a non-U.S. citizen under certain conditions, one of which is that a BI must have been completed with satisfactory results. §154.16(d) further describes LAA cases.

b. *Post-adjudication investigation.* A Personnel Security Investigation (PSI) predicated on new, adverse or questionable security, suitability or hostage information that arises and requires the application of investigation procedures subsequent to adjudicative action on a DoD-affiliated person's eligibility for continued access to classified information, assignment to or retention in sensitive duties or other designated duties requiring such investigation. While these cases are normally predicated on the surfacing of unfavorable information subsequent to favorable adjudication, they may also be opened when favorable information is offered to counter a previous unfavorable adjudication. §154.9(c)(3) further describes these cases.

3. General

a. As a rule, investigative activity in most PSIs occurs in the U.S. even when the Subject is at an overseas location. Therefore, the submission of requests for investigation to the Personnel Investigation Center (PIC) at Baltimore is a required procedure as it ensures uniform application of DoD PSI policy and the efficient dispatch and coordination of leads.

b. When the purpose of the investigation is for an LAA or post-adjudication on a Subject overseas, much, if not all of the leads are at an overseas location. While these cases also may be submitted directly to PIC for action, there is an inherent delay in the mailing of the request, the exchange of leads and reports with PIC, and transmittal of the reports back to the requester. To avoid this delay, the military investigative agencies, when acting for DIS overseas in accordance with 32 CFR part 361 may, with their Headquarters approval, accept these requests for investigations, initiate them and disseminate the results from the same level as they open, close, and disseminate their own cases. Usually this will greatly improve response time to the requester.

c. Under the procedures in paragraph b., above, DIS will not often be in a position to directly exercise its responsibility for control and direction until the case or lead is in progress or even completed; therefore, adherence to the policy stated in referenced documents, and as modified herein, is mandatory. When the policy of the military investigative agency is at variance with the above, the matter will be referred to the respective headquarters for resolution.

d. Since DIS is ultimately responsible for the personnel security product, it must be kept informed of all such matters referred to in this appendix. For instance, when the investigative agency overseas receives a DD Form 1879, Request for Personnel Security Investigation, which sets forth an issue outside DIS jurisdiction, it will reject the request, inform the requester of the reason and furnish an information copy of the DD Form 1879 and rejection letter to PIC. When the issue/jurisdiction is unclear to the investigative agency, the DD Form 1879 and the perceived jurisdictional question should be promptly forwarded to DIS for action and, if appropriate, to the component's headquarters for information. Questions on the interpretation of DIS or DoD policy and Directives pertaining to individual PSI cases can usually be resolved through direct communications with PIC.

e. 32 CFR part 361 establishes the supporting relationship of the military investigative agencies to DIS in overseas areas, and DIS provides these agencies with copies of relevant policy and interpretive guidance. For these reasons, the investigative agency vice the requester, is responsible for evaluating the request, processing it, collecting and evaluating the results within their jurisdiction for sufficiency, and forwarding the completed product to the appropriate activity.

f. The magnitude of operations at PIC requires that methods of handling LAA and post-adjudicative cases be consistent to the maximum extent possible. For this reason, the procedures for LAA cases are nearly identical to those for post-adjudicative cases. Briefly, the main exceptions are:

(1) The notification to PIC that a post-adjudication case has been opened will be by message, since an issue is present at the outset, whereas notification of an LAA case should normally be by mail.

(2) The scope of the LAA investigation is 10 years or since the person's 18th birthday, whichever is shortest, whereas the leads in a post-djudication case are limited to resolving the issue.

4. Jurisdiction

a. As set-forth in 32 CFR part 361 DIS is responsible for conducting all DoD PSIs in the 50 States, District of Columbia, and Puerto Rico, and will request the military departments to accomplish investigative requirements elsewhere. The military investigative

agencies in overseas locations routinely respond to personnel security investigative leads for DIS.

b. DIS jurisdiction also includes investigation of subversive affiliations, suitability information, and hostage situations when such inquiries are required for personnel security purposes; however, jurisdiction will rest with the military investigative agencies, FBI and/or civil authorities as appropriate when the alleged subversion or suitability issue represents a violation of law or, in the case of a hostage situation, there is an indication that the person concerned is actually being pressured, coerced, or influenced by interests inimical to the United States, or that hostile intelligence is taking action specifically directed against that person. Specific policy guidance on the applicability of these procedures and the jurisdictional considerations are stated in §154.9.

5. Case Opening

a. A request for investigation must be submitted by using DD Form 1879 and accompanied by supporting documentation unless such documentation is not immediately available, or the obtaining of documentation would compromise a sensitive investigation. Upon receipt of the request, the military investigative component will identify the issue(s), scope the leads, and ensure that the proposed action is that which is authorized for DIS as delineated in this part, 32 CFR part 361 and Defense Investigative Service Manual 201–1.

b. Upon such determination, the Component will prepare an Action Lead Sheet (ALS) which fully identifies the Subject and the scope of the case, and specifies precisely the leads which each investigative component (including DIS/PIC when appropriate) is to conduct.

c. Case opening procedures described above are identical for LAA and post-adjudication cases except with respect to notification of case opening to PIC:

(1) Post-adjudication Cases. These cases, because they involve an issue, are potentially sensitive and must be examined as early as possible by PIC for conformity to the latest DoD policy. Accordingly, the initial notification to PIC of case openings will always be by message. The message will contain at a minimum:

(a) Full identification of the subject;

(b) A narrative describing the allegation/facts in sufficient detail to support opening of the case; and

(c) A brief listing of the leads that are planned.

The DD Form 1879 and supporting documents, along with the agency's ALS, should be subsequently mailed to PIC.

(2) LAA Cases. The notification to PIC of case opening will normally be accomplished by mailing the DD Form 1879, DD Form 398 (Personal History Statement), a copy of the ALS, and any other supporting documents to PIC. Message notification to PIC in LAA cases will only be required if there is a security or suitability issue apparent in the DD Form 1879 or supporting documents.

(d) Beyond initial actions necessary to test allegation for investigative merit and jurisdiction, no further investigative action should commence until the notification of case opening to PIC has been dispatched.

(e) PIC will promptly respond to the notification of case opening by mail or message specifying any qualifying remarks along with a summary of previously existing data. PIC will also provide a DIS case control number (CCN). This number must be used by all components on all case related paperwork/reports.

(The investigating agency may assign its unique service CCN for interim internal control; however, the case will be processed, referenced, and entered into the DCII by the DIS case control number.) The first five digits of the DIS CCN will be the Julian date of the case opening when received at DIS.

6. Case Processing

a. The expected completion time for leads in LAA cases is 50 calendar days and for post-adjudication cases, 30 days, as computed from the date of receipt of the request. If conditions preclude completion in this time period, a pending report of the results to date, along with an estimated date of completion will be submitted to PIC.

b. Copies of all ALSs will be furnished to PIC. In addition, PIC will be promptly notified of any significant change in the scope of the case, or the development of an investigative issue.

c. The procedures for implementing the Privacy Act in PSI cases are set in DIS Manual 20–1–M 1. Any other restrictions on the release of information imposed by an overseas source or by regulations of the country where the inquiry takes place will be clearly stated in the report.

d. The report format for these cases will be that used by the military investigative agency.

e. Investigative action outside the jurisdictional area of an investigative component office may be directed elsewhere by ALS as needed in accordance with that agency's procedures and within the following geographical considerations:

(1) Leads will be sent to PIC if the investigative action is in the United States, District of Columbia, Puerto Rico, American Samoa, Bahama Islands, the U.S. Virgin Islands, and the following islands in the Pacific: Wake, Midway, Kwajalin, Johnston, Carolines, Marshalls, and Eniwetok.

(2) Leads to areas not listed above may be dispatched to other units of the investigative agency or even to another military agency's

field units if there is an agreement or memorandum of understanding that provides for such action. For case accountability purposes, copies of such ''lateral'' leads must be sent to the PIC.

(3) Leads that cannot be dispatched as described in paragraph (2) above, and those that must be sent to a non-DoD investigative agency should be sent to PIC for disposition.

f. The Defense Investigative Manual calls for obtaining PIC approval before conducting a Subject interview on a post-adjudicative investigation. To avoid the delay that compliance with this procedure would create, a military investigative component may conduct the interview provided:

(1) All other investigative leads have been completed and reviewed.

(2) The CCN has been received, signifying DIS concurrence with the appropriateness of the investigation.

(3) Contrary instructions have not been received from the PIC.

(4) The interview is limited to the resolution of the relevant issues disclosed by the investigation.

g. Notwithstanding the provisions of paragraphs f.(1) through (4) of this Appendix, if time is of the essence due to imminent transfer of the subject, a subject interview may be conducted at the discretion of the investigative agency.

7. Case Responsibility LAA and PA

Paragraph 3, above, describes the advantages of timely handling which accrue when the military investigative components act for DIS overseas. These actions for DIS may, however, be limited by the component's staffing and resource limitations, especially since some cases require more administration and management than others. Post-adjudication case leads, for instance, will normally be within the geographical jurisdiction of the component that accepted the request for investigation; therefore, relatively little case management is required. In contrast, LAA cases may require leads worldwide, and, therefore, create more complex case management and administration, especially in the tracking, monitoring and reviewing of leads outside the component's geographical area. Accordingly, an investigative component will accept the case from the requester, but only assign itself the appropriate leads within its own geographical jurisdiction and send the balance to PIC for appropriate disposition in accordance with the following:

a. The investigative agency will accept the request for investigation (thereby saving time otherwise lost in mailing to PIC) but limit its involvement in case management by extracting only those leads it will conduct or manage locally.

b. The agency should then prepare an ALS that shows clearly what leads it will cover and send PIC a copy of this ALS, along with the request for investigation and any other appropriate documentation. It must be clear in the ALS that PIC is to act on all those leads that the unit has not assigned to itself.

c. PIC, as case manager, will assume responsibility for the complete investigative package and, upon receipt of the last lead, will send the results to the appropriate activity.

d. The agency that accepted the case and assigned itself leads may send a copy of its report to the activity in the ''Results to'' block at the same time it sends the originals to PIC. If so, the letter of transmittal must inform the recipient that these reports are only a portion of the investigation, and that the balance will be forthcoming from PIC. Similarly, PIC must be informed of which investigative reports were disseminated. (This is normally done by sending PIC a copy of the letter of transmittal.)

8. Scope

a. *LAA.* The scope of investigation is 10 years or from age 18, whichever is the shortest period.

b. Post-Adjudication Cases. There is no standard scope. The inquiries conducted will be limited to those necessary to resolve the issue(s).

9. Case Closing: LAA and PA

a. Whether the investigative component or PIC closes out an investigation, there are three key elements to consider:

(1) The investigative results must be reviewed for quality and conformance to policy.

(2) The results must be sent to the activity listed in the ''Results to'' block of the DD Form 1879.

(3) PIC must be informed whether or not any dissemination was made by the investigative agency and, if so, what reports were furnished.

b. Investigative results may also be sent to a requester or higher level activity that makes a statement of need for the results. In such instances, a copy of the letter requesting the results and the corresponding letter of transmittal must be sent to PIC for retention.

c. When an investigative agency disseminates reports for PIC, it may use the transmittal documents, letters, or cover sheets it customarily uses for its own cases.

d. The material that is to be provided to PIC will consist of: The originals of all reports, and all other case documentation such as original statements, confidential source sheets, interview logs, requests for investigation, letters of transmittal to adjudicaters/requesters, or communications with the requester, such as those that modify the scope of the investigation.

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]

§ 155.3 Definitions.

(a) *Applicant.* Any U.S. citizen who holds or requires a security clearance or any immigrant alien who holds or requires a limited access authorization for access to classified information needed in connection with his or her employment in the private sector; any U.S. citizen who is a direct-hire employee or selectee for a position with the North Atlantic Treaty Organization (NATO) and who holds or requires NATO certificates of security clearance or security assurances for access to U.S. or foreign classified information; or any U.S. citizen nominated by the Red Cross or United Service Organizations for assignment with the Military Services overseas. The term ''applicant'' does not apply to those U.S. citizens who are seconded to NATO by U.S. Departments and Agencies or to U.S. citizens recruited through such Agencies in response to a request from NATO.

(b) *Clearance Decision.* A decision made in accordance with this part concerning whether it is clearly consistent with the national interest to grant an applicant a security clearance for access to Confidential, Secret, or Top Secret information. A favorable clearance decision establishes eligibility of the applicant to be granted a security clearance for access at the level governed by the documented need for such access, and the type of investigation specified for that level in 32 CFR part 154. An unfavorable clearance decision denies any application for a security clearance and revokes any existing security clearance, thereby preventing access to classified information at any level and the retention of any existing security clearance.

§ 155.4 Policy.

It is DoD policy that:

(a) All proceedings provided for by this part shall be conducted in a fair and impartial manner.

(b) A clearance decision reflects the basis for an ultimate finding as to whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant.

(c) Except as otherwise provided for by E.O. 10865, as amended, or this part, a final unfavorable clearance decision shall not be made without first providing the applicant with:

(1) Notice of specific reasons for the proposed action.

(2) An opportunity to respond to the reasons.

(3) Notice of the right to a hearing and the opportunity to cross-examine persons providing information adverse to the applicant.

(4) Opportunity to present evidence on his or her own behalf, or to be represented by counsel or personal representative.

(5) Written notice of final clearance decisions.

(6) Notice of appeal procedures.

(d) Actions pursuant to this part shall cease upon termination of the applicant's need for access to classified information except in those cases in which:

(1) A hearing has commenced;

(2) A clearance decision has been issued; or

(3) The applicant's security clearance was suspended and the applicant provided a written request that the case continue.

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

§ 155.5 Responsibilities.

(a) The Assistant Secretary of Defense of Command, Control, Communications and Intelligence shall:

(1) Establish investigative policy and adjudicative standards and oversee their application.

(2) Coordinate with the General Counsel of the Department of Defense (GC, DoD) on policy affecting clearance decisions.

(3) Issue clarifying guidance and instructions as needed.

(b) The General Counsel of the Department of Defense shall:

(1) Establish guidance and provide oversight as to legal sufficiency of procedures and standards established by this part.

(2) Establish the organization and composition of the DOHA.

(3) Designate a civilian attorney to be the Director, DOHA.

(4) Issue clarifying guidance and instructions as needed.

(5) Administer the program established by this part.

(6) Issue invitational travel orders in appropriate cases to persons to appear and testify who have provided oral or written statements adverse to the applicant relating to a controverted issue.

(7) Designate attorneys to be Department Counsels assigned to the DOHA to represent the Government's interest in cases and related matters within the applicability and scope of this part.

(8) Designate attorneys to be Administrative Judges assigned to the DOHA.

(9) Designate attorneys to be Administrative Judge members of the DOHA Appeal Board.

(10) Provide for supervision of attorneys and other personnel assigned or attached to the DOHA.

(11) Develop and implement policy established or coordinated with the GC, DoD, in accordance with this part.

(12) Establish and maintain qualitative and quantitative standards for all work by DOHA employees arising within the applicability and scope of this part.

(13) Ensure that the Administrative Judges and Appeal Board members have the requisite independence to render fair and impartial decisions consistent with DoD policy.

(14) Provide training, clarify policy, or initiate personnel actions, as appropriate, to ensure that all DOHA decisions are made in accordance with policy, procedures, and standards established by this part.

(15) Provide for maintenance and control of all DOHA records.

(16) Take actions as provided for in §155.6(b), and the additional procedural guidance in appendix A to this part.

(17) Establish and maintain procedures for timely assignment and completion of cases.

(18) Issue guidance and instructions, as needed, to fulfill the foregoing responsibilities.

(19) Designate the Director, DOHA, to implement paragraphs (b)(5) through (b)(18) of this section, under general guidance of the GC, DoD.

(c) The Heads of the DoD Components shall provide (from resources available to the designated DoD Component) financing, personnel, personnel spaces, office facilities, and related administrative support required by the DOHA.

(d) The ASD(C^3I) shall ensure that cases within the scope and applicability of this part are referred promptly to the DOHA, as required, and that clearance decisions by the DOHA are acted upon without delay.

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

§155.6 Procedures.

(a) Applicants shall be investigated in accordance with the standards in 32 CFR part 154.

(b) An applicant is required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed by the DOHA to reach a clearance decision and to otherwise comply with the procedures authorized by this part. The applicant may elect on constitutional or other grounds not to comply; but refusal or failure to furnish or authorize the providing of relevant and material information or otherwise cooperate at any stage in the investigation or adjudicative process may prevent the DOHA from making a clearance decision. If an applicant fails or refuses to:

(1) Provide relevant and material information or to authorize others to provide such information; or

(2) Proceed in a timely or orderly fashion in accordance with this part; or

(3) Follow directions of an Administrative Judge or the Appeal Board; then the Director, DOHA, or designee, may revoke any security clearance held by the applicant and discontinue case processing. Requests for resumption of case processing and reinstatement of a security clearance may be approved by the Director, DOHA, only upon a showing of good cause. If the request is denied, in whole or in part, the decision is final and bars reapplication for a security clearance for 1 year from the date of the revocation.

(c) Each clearance decision must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria in 32 CFR 154.7 and adjudication policy in appendix H to 32 CFR part 154, including as appropriate:

(1) Nature and seriousness of the conduct and surrounding circumstances.

(2) Frequency and recency of the conduct.

(3) Age of the applicant.

(4) Motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences involved.

(5) Absence or presence of rehabilitation.

(6) Probability that the circumstances or conduct will continue or recur in the future.

(d) Whenever there is a reasonable basis for concluding that an applicant's continued access to classified information poses an imminent threat to the national interest, any security clearance held by the applicant may be suspended by the ASD(C^3I), with the concurrence of the GC, DoD, pending a final clearance decision. This suspension may be rescinded by the same authorities upon presentation of additional information that conclusively demonstrates that an imminent threat to the national interest no longer exists. Procedures in appendix A to this part shall be expedited whenever an applicant's security clearance has been suspended pursuant to this section.

(e) Nothing contained in this part shall limit or affect the responsibility and powers of the Secretary of Defense or the head of another Department or Agency to deny or revoke a security clearance when the security of the nation so requires. Such authority may not be delegated and may be exercised only when the Secretary of Defense or the head of another Department or Agency determines that the hearing procedures and other provisions of this part cannot be invoked consistent with the national security. Such a determination shall be conclusive.

(f) Additional procedural guidance is in appendix A to this part.

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

APPENDIX A TO PART 155—ADDITIONAL PROCEDURAL GUIDANCE

1. When the DISCO cannot affirmatively find that it is clearly consistent with the national interest to grant or continue a security clearance for an applicant, the case will be promptly referred to the DOHA.

2. Upon referral, the DOHA shall make a prompt determination whether to grant or continue a security clearance, issue a statement of reasons (SOR) as to why it is not clearly consistent with the national interest to do so, or take interim actions, including but not limited to:

a. Direct further investigation.

b. Propound written interrogatories to the applicant or other persons with relevant information.

c. Requiring the applicant to undergo a medical evaluation by a DoD Psychiatric Consultant.

d. Interviewing the applicant.

3. An unfavorable clearance decision shall not be made unless the applicant has been provided with a written SOR that shall be as detailed and comprehensive as the national security permits. A letter of instruction with the SOR shall explain that the applicant or Department Counsel may request a hearing. It shall also explain the adverse consequences for failure to respond to the SOR within the prescribed time frame.

4. The applicant must submit a detailed written answer to the SOR under oath or affirmation that shall admit or deny each listed allegation. A general denial or other similar answer is insufficient. To be entitled to a hearing, the applicant must specifically request a hearing in his or her answer. The answer must be received by the DOHA within 20 days from receipt of the SOR. Requests for an extension of time to file an answer may be submitted to the Director, DOHA, or designee, who in turn may grant the extension only upon a showing of good cause.

5. If the applicant does not file a timely and responsive answer to the SOR, the Director, DOHA, or designee, may discontinue processing the case, deny issuance of the requested security clearance, and direct the DISCO to revoke any security clearance held by the applicant.

6. Should review of the applicant's answer to the SOR indicate that allegations are unfounded, or evidence is insufficient for further processing, Department Counsel shall take such action as appropriate under the circumstances, including but not limited to withdrawal of the SOR and transmittal to the Director for notification of the DISCO for appropriate action.

7. If the applicant has not requested a hearing with his or her answer to the SOR and Department Counsel has not requested a hearing within 20 days of receipt of the applicant's answer, the case shall be assigned to an Administrative Judge for a clearance decision based on the written record. Department Counsel shall provide the applicant with a copy of all relevant and material information that could be adduced at a hearing. The applicant shall have 30 days from

receipt of the information in which to submit a documentary response setting forth objections, rebuttal, extenuation, mitigation, or explanation, as appropriate.

8. If a hearing is requested by the applicant or Department Counsel, the case shall be assigned to an Administrative Judge for a clearance decision based on the hearing record. Following issuance of a notice of hearing by the Administrative Judge, or designee, the applicant shall appear in person with or without counsel or a personal representative at a time and place designated by the notice of hearing. The applicant shall have a reasonable time to prepare his or her case. The applicant shall be notified at least 15 days in advance of the time and place of the hearing, which generally shall be held at a location in the United States within a metropolitan area near the applicant's place of employment or residence. A continuance may be granted by the Administrative Judge only for good cause. Hearings may be held outside of the United States in NATO cases, or in other cases upon a finding of good cause by the Director, DOHA, or designee.

9. The Administrative Judge may require a prehearing conference.

10. The Administrative Judge may rule on questions of procedure, discovery, and evidence and shall conduct all proceedings in a fair, timely, and orderly manner.

11. Discovery by the applicant is limited to non-privileged documents and materials subject to control by the DOHA. Discovery by Department Counsel after issuance of an SOR may be granted by the Administrative Judge only upon a showing of good cause.

12. A hearing shall be open except when the applicant requests that it be closed, or when the Administrative Judge determines that there is a need to protect classified information or there is other good cause for keeping the proceeding closed. No inference shall be drawn as to the merits of a case on the basis of a request that the hearing be closed.

13. As far in advance as practical, Department Counsel and the applicant shall serve one another with a copy of any pleading, proposed documentary evidence, or other written communication to be submitted to the Administrative Judge.

14. Department Counsel is responsible for presenting witnesses and other evidence to establish facts alleged in the SOR that have been controverted.

15. The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision.

16. Witnesses shall be subject to cross-examination.

17. The SOR may be amended at the hearing by the Administrative Judge on his or her own motion, or upon motion by Department Counsel or the applicant, so as to render it in conformity with the evidence admitted or for other good cause. When such amendments are made, the Administrative Judge may grant either party's request for such additional time as the Administrative Judge may deem appropriate for further preparation or other good cause.

18. The Administrative Judge hearing the case shall notify the applicant and all witnesses testifying that 18 U.S.C. 1001 is applicable.

19. The Federal Rules of Evidence (28 U.S.C. 101 *et seq.*) shall serve as a guide. Relevant and material evidence may be received subject to rebuttal, and technical rules of evidence may be relaxed, except as otherwise provided herein, to permit the development of a full and complete record.

20. Official records or evidence compiled or created in the regular course of business, other than DoD personnel background reports of investigation (ROI), may be received and considered by the Administrative Judge without authenticating witnesses, provided that such information has been furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense, or the Department or Agency head concerned, to safeguard classified information within industry under to E.O. 10865, as amended. An ROI may be received with an authenticating witness provided it is otherwise admissible under the Federal Rules of Evidence (28 U.S.C. 101 *et seq.*).

21. Records that cannot be inspected by the applicant because they are classified may be received and considered by the Administrative Judge, provided the GC, DoD, has:

a. Made a preliminary determination that such evidence appears to be relevant and material.

b. Determined that failure to receive and consider such evidence would be substantially harmful to the national security.

22. A written or oral statement adverse to the applicant on a controverted issue may be received and considered by the Administrative Judge without affording an opportunity to cross-examine the person making the statement orally, or in writing when justified by the circumstances, only in either of the following circumstances:

a. If the head of the Department or Agency supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his or her identity would be substantially harmful to the national interest; or

b. If the GC, DoD, has determined the statement concerned appears to be relevant, material, and reliable; failure to receive and

consider the statement would be substantially harmful to the national security; and the person who furnished the information cannot appear to testify due to the following:

(1) Death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant; or

(2) Some other cause determined by the Secretary of Defense, or when appropriate by the Department or Agency head, to be good and sufficient.

23. Whenever evidence is received under item 21. or 22., the applicant shall be furnished with as comprehensive and detailed a summary of the information as the national security permits. The Administrative Judge and Appeal Board may make a clearance decision either favorable or unfavorable to the applicant based on such evidence after giving appropriate consideration to the fact that the applicant did not have an opportunity to confront such evidence, but any final determination adverse to the applicant shall be made only by the Secretary of Defense, or the Department or Agency head, based on a personal review of the case record.

24. A verbatim transcript shall be made of the hearing. The applicant shall be furnished one copy of the transcript, less the exhibits, without cost.

25. The Administrative Judge shall make a written clearance decision in a timely manner setting forth pertinent findings of fact, policies, and conclusions as to the allegations in the SOR, and whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant. The applicant and Department Counsel shall each be provided a copy of the clearance decision. In cases in which evidence is received under items 21. and 22., the Administrative Judge's written clearance decision may require deletions in the interest of national security.

26. If the Administrative Judge decides that it is clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the DISCO shall be so notified by the Director, DOHA, or designee, when the clearance decision becomes final in accordance with item 36., below.

27. If the Administrative Judge decides that it is not clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the Director, DOHA, or designee, shall expeditiously notify the DISCO, which shall in turn notify the applicant's employer of the denial or revocation of the applicant's security clearance. The letter forwarding the Administrative Judge's clearance decision to the applicant shall advise the applicant that these actions are being taken, and that the applicant may appeal the Administrative Judge's clearance decision.

28. The applicant or Department Counsel may appeal the Administrative Judge's clearance decision by filing a written notice of appeal with the Appeal Board within 15 days after the date of the Administrative Judge's clearance decision. A notice of appeal received after 15 days from the date of the clearance decision shall not be accepted by the Appeal Board, or designated Board Member, except for good cause. A notice of cross appeal may be filed with the Appeal Board within 10 days of receipt of the notice of appeal. An untimely cross appeal shall not be accepted by the Appeal Board, or designated Board Member, except for good cause.

29. Upon receipt of a notice of appeal, the Appeal Board shall be provided the case record. No new evidence shall be received or considered by the Appeal Board.

30. After filing a timely notice of appeal, a written appeal brief must be received by the Appeal Board within 45 days from the date of the Administrative Judge's clearance decision. The appeal brief must state the specific issue or issues being raised, and cite specific portions of the case record supporting any alleged error. A written reply brief, if any, must be filed within 20 days from receipt of the appeal brief. A copy of any brief filed must be served upon the applicant or Department Counsel, as appropriate.

31. Requests for extension of time for submission of briefs may be submitted to the Appeal Board or designated Board Member.

A copy of any request for extension of time must be served on the opposing party at the time of submission. The Appeal Board, or designated Board Member, shall be responsible for controlling the Appeal Board's docket, and may enter an order dismissing an appeal in an appropriate case or vacate such an order upon a showing of good cause.

32. The Appeal Board shall address the material issues raised by the parties to determine whether harmful error occurred. Its scope of review shall be to determine whether or not:

a. The Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record. In making this review, the Appeal Board shall give deference to the credibility determinations of the Administrative Judge;

b. The Administrative Judge adhered to the procedures required by E.O. 10865, as amended and this part; or

c. The Administrative Judge's rulings or conclusions are arbitrary, capricious, or contrary to law.

33. The Appeal Board shall issue a written clearance decision addressing the material

issues raised on appeal. The Appeal Board shall have authority to:

a. Affirm the decision of the Administrative Judge;

b. Remand the case to an Administrative Judge to correct identified error. If the case is remanded, the Appeal Board shall specify the action to be taken on remand; or

c. Reverse the decision of the Administrative Judge if correction of identified error mandates such action.

34. A copy of the Appeal Board's written clearance decision shall be provided to the parties. In cases in which evidence was received under items 21. and 22., the Appeal Board's clearance decision may require deletions in the interest of national security.

35. Upon remand, the case file shall be assigned to an Administrative Judge for correction of error(s) in accordance with the Appeal Board's clearance decision. The assigned Administrative Judge shall make a new clearance decision in the case after correcting the error(s) identified by the Appeal Board. The Administrative Judge's clearance decision after remand shall be provided to the parties. The clearance decision after remand may be appealed pursuant to items 28. to 35.

36. A clearance decision shall be considered final when:

a. A security clearance is granted or continued pursuant to item 2.;

b. No timely notice of appeal is filed;

c. No timely appeal brief is filed after a notice of appeal has been filed;

d. The appeal has been withdrawn;

e. When the Appeal Board affirms or reverses an Administrative Judge's clearance decision; or

f. When a decision has been made by the Secretary of Defense, or the Department or Agency head, under item 23.

The Director, DOHA, or designee, shall notify the DISCO of all final clearance decisions.

37. An applicant whose security clearance has been finally denied or revoked by the DOHA is barred from reapplication for 1 year from the date of the initial unfavorable clearance decision.

38. A reapplication for a security clearance must be made initially by the applicant's employer to the DISCO and is subject to the same processing requirements as those for a new security clearance application. The applicant shall thereafter be advised he is responsible for providing the Director, DOHA, with a copy of any adverse clearance decision together with evidence that circumstances or conditions previously found against the applicant have been rectified or sufficiently mitigated to warrant reconsideration.

39. If the Director, DOHA, determines that reconsideration is warranted, the case shall be subject to this part for making a clearance decision.

40. If the Director, DOHA, determines that reconsideration is not warranted, the DOHA shall notify the applicant of this decision. Such a decision is final and bars further reapplication for an additional one year period from the date of the decision rejecting the application.

41. Nothing in this part is intended to give an applicant reapplying for a security clearance any greater rights than those applicable to any other applicant under this part.

42. An applicant may file a written petition, under oath or affirmation, for reimbursement of loss of earnings resulting from the suspension, revocation, or denial of his or her security clearance. The petition for reimbursement must include as an attachment the favorable clearance decision and documentation supporting the reimbursement claim. The Director, DOHA, or designee, may in his or her discretion require additional information from the petitioner.

43. Claims for reimbursement must be filed with the Director, DOHA, or designee, within 1 year after the date the security clearance is granted. Department Counsel generally shall file a response within 60 days after receipt of applicant's petition for reimbursement and provide a copy thereof to the applicant.

44. Reimbursement is authorized only if the applicant demonstrates by clear and convincing evidence to the Director, DOHA, that all of the following conditions are met:

a. The suspension, denial, or revocation was the primary cause of the claimed pecuniary loss; and

b. The suspension, denial, or revocation was due to gross negligence of the Department of Defense at the time the action was taken, and not in any way by the applicant's failure or refusal to cooperate.

45. The amount of reimbursement shall not exceed the difference between the earnings of the applicant at the time of the suspension, revocation, or denial and the applicant's interim earnings, and further shall be subject to reasonable efforts on the part of the applicant to mitigate any loss of earnings. No reimbursement shall be allowed for any period of undue delay resulting from the applicant's acts or failure to act. Reimbursement is not authorized for loss of merit raises and general increases, loss of employment opportunities, counsel's fees, or other costs relating to proceedings under this part.

46. Claims approved by the Director, DOHA, shall be forwarded to the Department or Agency concerned for payment. Any payment made in response to a claim for reimbursement shall be in full satisfaction of any further claim against the United States or any Federal Department or Agency, or any of its officers or employees.

47. Clearance decisions issued by Administrative Judges and the Appeal Board shall be indexed and made available in redacted form to the public.

[57 FR 5383, Feb. 14, 1992, as amended at 59 FR 35464, July 12, 1994; 59 FR 48565, Sept. 22, 1994]

PART 156—DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM (DoDPSP)

Sec.
156.1 Purpose.
156.2 Applicability and scope.
156.3 Policy
156.4 Responsibilities.

AUTHORITY: 50 U.S.C. 781.

SOURCE: 58 FR 42855, Aug. 12, 1993, unless otherwise noted.

§ 156.1 Purpose.

This part:

(a) Updates the policy and responsibilities for the DoDPSP under Pub. L. 81–832; E.O. 10450, 18 FR 2489, 3 CFR, 1949–1953 Comp., p. 936; E.O. 10865, 25 FR 1583, 3 CFR, 1959–1963 Comp., p. 398; E.O. 12333, 46 FR 59941, 3 CFR, 1981 Comp., p.200; and E.O. 12356, 47 FR 14874 and 15557, 3 CFR 1982 Comp., p. 166.

(b) Continues to authorize the publication of DoD 5200.2–R[1] in accordance with DoD 5025.1–M.[2]

§ 156.2 Applicability and scope.

This part applies to:

(a) The Office of the Secretary of Defense, the Military Departments (including the Coast Guard when it is operating as a Military Service in the Navy), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, and the Defense Agencies, except as provided for the National Security Agency (NSA) in paragraph (b) of this section (hereafter referred to collectively as ''the DoD Components'').

(b) The NSA is exempt from the provisions of this Directive. The personnel security program for the NSA is implemented pursuant to DoD Directive 5210.45,[3] and internal regulations of the NSA.

(c) DoD military and civilian personnel, consultants to the Department of Defense, contractors cleared under the Defense Industrial Security Program (DISP) Regulations DoD 5220.22[4] and others affiliated with the Department of Defense.

§ 156.3 Policy.

It is DoD policy that:

(a) No person shall be appointed as a civilian employee of the Department of Defense, accepted for entrance into the Armed Forces of the United States, authorized access to classified information, or assigned to duties that are subject to investigation under this part unless such appointment, acceptance, clearance, or assignment is clearly consistent with the interests of national security.

(b) A personnel security clearance shall be granted and assignment to sensitive duties shall be authorized only to U.S. citizens. As an exception, a non-U.S. citizen may, by an authorized official (as specified in 32 CFR part 154) be assigned to sensitive duties or granted a Limited Access Authorization for access to classified information if there is a need for access in support of a specific DoD program, project, or contract.

(c) The personnel security standard that shall be applied in determining a person's eligibility for a security clearance or assignment to sensitive duties is whether, based on all available information, the person's allegiance, trustworthiness, reliability, and judgment are such that the person can reasonably to expected to comply with Government policy and procedures for safeguarding classified information and performing sensitive duties.

(d) 32 CFR part 154 shall identify those positions and duties that require a personnel security investigation (PSI). A PSI is required for:

(1) Appointment to a sensitive civilian position.

(2) Entry into military service.

[1] Copies may be obtained at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

[2] See footnote 1 to 156.1(b).

[3] See footnote 1 to 156.1(b).

[4] See footnote 1 to 156.1(b).

(3) The granting of a security clearance or approval for access to classified information.

(4) Assignment to other duties that require a personnel security or trustworthiness determination.

(5) Continuing eligibility for retention of a security clearance and approval for access to classified information or for assignment to other sensitive duties.

(e) 32 CFR part 154 shall contain personnel security criteria and adjudicative guidance to assist in determining whether an individual meets the clearance and sensitive position standards referred to in paragraphs (a) and (c) of this section.

(f) No unfavorable personnel security determination shall be made except in accordance with procedures set forth in 32 CFR part 154 or 32 CFR part 155 or as otherwise authorized by law.

§ 156.4 Responsibilities.

(a) The *Assistant Secretary of Defense for Command, Control, Communications, and Intelligence* shall:

(1) Be responsible for overall policy, guidance, and control of the DoDPSP.

(2) Develop and implement plans, policies, and procedures for the DoDPSP.

(3) Issue and maintain DoD 5200.2–R consistent with DoD 5025.1–M.

(4) Conduct an active oversight program to ensure compliance with DoDPSP requirements.

(5) Ensure that research is conducted to assess and improve the effectiveness of the DoDPSP (DoD Directive 5210.79[5]).

(6) Ensure that the Defense Investigative Service is operated pursuant to 32 CFR part 361.

(7) Ensure that the DoD Security Institute provides the education, training, and awareness support to the DoDPSP under DoD Directive 5200.32.[6]

(8) Be authorized to make exceptions to the requirements of this part on a case-by-case basis when it is determined that doing so furthers the mission of the Department of Defense and is consistent with the protection of classified information from unauthorized disclosure.

(b) The *General Counsel of the Department of Defense* shall:

(1) Be responsible for providing advice and guidance as to the legal sufficiency of procedures and standards implementing the DoDPSP and the DISP.

(2) Exercise oversight of PSP appeals procedures to verify that the rights of individuals are being protected consistent with the constitution, laws of the United States, Executive Orders, Directives, or Regulations that implement the DoDPSP and DISP, and with the interests of national security.

(c) The *Heads of the DoD Components* shall:

(1) Designate a senior official who shall be responsible for implementing the DoDPSP within their components.

(2) Ensure that the DoDPSP is properly administered under this Directive within their components.

(3) Ensure that information and recommendations are provided to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence on any aspect of the program.

PART 159—PRIVATE SECURITY CONTRACTORS OPERATING IN CONTINGENCY OPERATIONS

Sec.
159.1 Purpose.
159.2 Applicability and scope.
159.3 Definitions.
159.4 Policy.
159.5 Responsibilities.
159.6 Procedures.

AUTHORITY: Public Law 110–181; Pub. L. 110–417.

SOURCE: 74 FR 34691, July 17, 2009, unless otherwise noted.

§ 159.1 Purpose.

This part establishes policy, assigns responsibilities and provides procedures for the regulation of the selection, accountability, training, equipping, and conduct of personnel performing private security functions under a covered contract. It also assigns responsibilities and establishes procedures for incident reporting, use of and accountability for equipment, rules for the use of force, and a process

[5] See footnote 1 to 156.1(b).
[6] See footnote 1 to 156.1(b).

for administrative action or the removal, as appropriate, of PSCs and PSC personnel.

§ 159.2 Applicability and scope.

This part:

(a) Applies to:

(1) The Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to as the ''DoD Components'').

(2) The Department of State and other U.S. Federal agencies insofar as it implements the requirements of section 862 of Public Law 110–181. Specifically, in areas of operations which require enhanced coordination of PSC and PSC personnel working for U.S. Government (U.S.G.) agencies, the Secretary of Defense may designate such areas as areas of combat operations for the limited purposes of this part. In such an instance, the standards established in accordance with this part would, in coordination with the Secretary of State, expand from covering only DoD PSCs and PSC personnel to cover all U.S.G.-funded PSCs and PSC personnel operating in the designated area.

(b) Prescribes policies applicable to all:

(1) DoD PSCs and PSC personnel performing private security functions during contingency operations outside the United States.

(2) USG-funded PSCs and PSC personnel performing private security functions in an area of combat operations, as designated by the Secretary of Defense.

§ 159.3 Definitions.

Unless otherwise noted, these terms and their definitions are for the purpose of this part.

Area of combat operations. An area of operations designated as such by the Secretary of Defense for the purpose of this part, when enhanced coordination of PSCs working for U.S.G. agencies is required.

Contingency operation. A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (10 U.S.C. 101(a)(13)). It is a military operation that: a. Is designated by the Secretary of Defense as an operation in which members of the Armed Forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing force; or b. Is created by definition of law. Under 10 U.S.C. 101(a)(13)(B), a contingency operation exists if a military operation results in the (1) call-up to (or retention on) active duty of members of the uniformed Services under certain enumerated statutes (10 U.S.C. 688, 12301(a), 12302, 12304, 12305, 12406, or 331–335); and (2) the call-up to (or retention on) active duty of members of the uniformed Services under any other (non-enumerated) provision of law during war or national emergency declared by the President or Congress. These may include humanitarian or peacekeeping operations or other military operations or exercises.

Contractor. The contractor, subcontractor, grantee, or other party carrying out the covered contract.

Covered contract. A DoD contract for performance of services in an area of contingency operations or a contract of a non-DoD Federal agency for performance of services in an area of combat operations, as designated by the Secretary of Defense;

A subcontract at any tier under such a contract; or

A task order or delivery order issued under such a contract or subcontract.

Also includes contracts or subcontracts funded under grants and subgrants by a Federal agency for performance in an area of combat operations as designated by the Secretary of Defense. Excludes temporary arrangements entered into by non-DoD contractors or grantees for the performance of private security functions by individual indigenous personnel not affiliated with a local or expatriate security company. Such arrangements must still be in compliance with local law.

Private security functions. Activities engaged in by a contractor under a covered contract as follows:

(1) Guarding of personnel, facilities, designated sites, or property of a Federal agency, the contractor or subcontractor, or a third party.[1]

(2) Any other activity for which personnel are required to carry weapons in the performance of their duties. For the DoD, DoDI Instruction 3020.41, ''Contractor Personnel Authorized to Accompany the U.S. Armed Forces,''[2] prescribes policies related to personnel allowed to carry weapons for self defense.

PSC. During contingency operations ''PSC'' means a company employed by the DoD performing private security functions under a covered contract. In a designated area of combat operations, the term ''PSC'' expands to include all companies employed by U.S.G. agencies performing private security functions under a covered contract.

PSC personnel. Any individual performing private security functions under a covered contract.

§ 159.4 Policy.

(a) Consistent with the requirements of paragraph (a)(2) of section 862 of Public Law 110–181, the selection, training, equipping, and conduct of PSC personnel including the establishment of appropriate processes shall be coordinated between the DoD and the Department of State.

(b) Geographic Combatant Commanders will provide tailored PSC guidance and procedures for the operational environment in their Area of Responsibility (AOR) in accordance with this part, the Federal Acquisition Regulation (FAR)[3] and the Defense Federal Acquisition Regulation Supplement (DFARS).[4]

(c) In a designated area of combat operations, the relevant Chief of Mission will be responsible for developing and issuing implementing instructions for non-DoD PSCs and their personnel consistent with the standards set forth by the geographic Combatant Commander in accordance with paragraph (b) of this section. The Chief of Mission has the option to instruct non DoD PSCs and their personnel to follow the guidance and procedures developed by the Geographic Combatant Commander and/or Subordinate Commander.

(d) The requirements of this part shall not apply to contracts entered into by elements of the intelligence community in support of intelligence activities.

§ 159.5 Responsibilities.

(a) The Assistant Deputy Under Secretary of Defense for Program Support, under the authority, direction, and control of the Deputy Under Secretary of Defense for Logistics and Materiel Readiness, shall monitor the registering, processing, and accounting of PSC personnel in an area of contingency operations.

(b) The Director, Defense Procurement and Acquisition Policy, under the authority, direction, and control of the Deputy Under Secretary of Defense for Acquisition and Technology (DUSD(AT)), shall ensure that the DFARS and (in consultation with the other members of the FAR Council) the FAR provide appropriate guidance and contract clauses consistent with this part and paragraph (b) of section 862 of Public Law 110–181.

(c) The Director, Defense Business Transformation Agency, under the authority, direction, and control of the Deputy Chief Management Officer of the Department of Defense, through the DUSD(AT), shall ensure that information systems effectively support the accountability and visibility of contracts, contractors, and specified equipment associated with private security functions.

[1] Contractors performing private security functions are not authorized to perform inherently governmental functions. In this regard, they are limited to a defensive response to hostile acts or demonstrated hostile intent.

[2] Available at *http://www.dtic.mil/whs/directives/corres/pdf/302041p.pdf*.

[3] Published in Title 48 of the Code of Federal Regulations.

[4] Published in Title 48 of the Code of Federal Regulations.

(d) The Chairman of the Joint Chiefs of Staff shall ensure that joint doctrine is consistent with the principles established by DoD Directive 3020.49 ''Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution,''[5] DoD Instruction 3020.41, ''Contractor Personnel Authorized to Accompany the U.S. Armed Forces,'' and this part.

(e) The geographic Combatant Commanders in whose AOR a contingency operation is occurring, and within which PSCs and PSC personnel perform under covered contracts, shall:

(1) Provide guidance and procedures, as necessary and consistent with the principles established by DoD Directive 3020.49, ''Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution,'' DoD Instruction 3020.41, ''Contractor Personnel Authorized to Accompany the U.S. Armed Forces,''[6] and this part, for the selection, training, accountability and equipping of such PSC personnel and the conduct of PSCs and PSC personnel within their AOR. Individual training and qualification standards shall meet, at a minimum, one of the Military Departments' established standards.

Within a geographic Combatant Command, Subordinate Commanders shall be responsible for developing and issuing implementing procedures as warranted by the situation, operation, and environment, in consultation with the relevant Chief of Mission in designated areas of combat operations.

(2) Through the Contracting Officer, ensure that PSC personnel acknowledge, through their PSC, their understanding and obligation to comply with the terms and conditions of their covered contracts.

(3) Issue written authorization to the PSC identifying individual PSC personnel who are authorized to be armed. Rules for the use of force, developed in accordance with Chairman of the Joint Chief of Staff Instruction 3121.01B, ''Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces,''[7] shall be included with the written authorization.

(4) Ensure that the procedures, orders, directives and instructions prescribed §159.6(a) of this part are available through a single location (to include an Internet Web site, consistent with security considerations and requirements).

(f) The Heads of the DoD Components shall:

(1) Ensure that all private security-related requirement documents are in compliance with the procedures listed in §159.6 of this part and the guidance and procedures issued by the geographic Combatant Command,

(2) Ensure private security-related contracts contain the appropriate clauses in accordance with the applicable FAR clause and include additional mission-specific requirements as appropriate.

§159.6 Procedures.

(a) *Standing Combatant Command Guidance and Procedures.* Each geographic Combatant Commander shall develop and publish guidance and procedures for PSCs and PSC personnel operating during a contingency operation within their AOR, consistent with applicable law; this part; applicable Military Department publications; and other applicable DoD issuances to include DoD Directive 3020.49, ''Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution,'' DFARS, DoD Directive 2311.01E, ''DoD Law of War Program,''[8] DoD 5200.8–R, ''Physical Security Program,''[9] CJCSI 3121.01B,

[5] Available from *http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf*.

[6] Available from *http://www.dtic.mil/whs/directives/corres/html/302041.htm*.

[7] CJCSI 3121.01B provides guidance on the standing rules of engagement (SROE) and establishes standing rules for the use of force (SRUF) for DOD operations worldwide. This document is classified secret. CJCSI 3121.01B is available via Secure Internet Protocol Router Network at *http://js.smil.mil* If the requester is not an authorized user of the classified network, the requester should contact Joint Staff J–3 at 703–614–0425.

[8] Available at *http://www.dtic.mil/whs/directives/corres/html/231101.htm*.

[9] Available at *http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf*.

''Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces,'' and DoD Directive 5210.56, ''Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties.''[10] The guidance and procedures shall:

(1) Contain, at a minimum, procedures to implement the following processes, and identify the organization responsible for managing these processes:

(i) Registering, processing, accounting for and keeping appropriate records of PSCs and PSC personnel in accordance with DoD Instruction 3020.41, ''Contractor Personnel Authorized to Accompany the U.S. Armed Forces.''

(ii) PSC verification that PSC personnel meet all the legal, training, and qualification requirements for authorization to carry a weapon in accordance with the terms and conditions of their contract and host country law. Weapons accountability procedures will be established and approved prior to the weapons authorization.

(iii) Arming of PSC personnel. Requests for permission to arm PSC personnel shall be reviewed on a case-by-case basis by the appropriate Staff Judge Advocate to the geographic Combatant Commander (or a designee) to ensure there is a legal basis for approval. The request will then be approved or denied by the geographic Combatant Commander or a specifically identified designee, no lower than the flag officer level. Requests to arm non-DOD PSC personnel shall be reviewed and approved in accordance with §159.4(c) of this part. Requests for permission to arm PSC personnel shall include:

(A) A description of where PSC personnel will operate, the anticipated threat, and what property or personnel such personnel are intended to protect, if any.

(B) A description of how the movement of PSC personnel will be coordinated through areas of increased risk or planned or ongoing military operations, including how PSC personnel will be rapidly identified by members of the U.S. Armed Forces.

(C) A communication plan, to include a description of how relevant threat information will be shared between PSC personnel and U.S. military forces and how appropriate assistance will be provided to PSC personnel who become engaged in hostile situations. DoD contractors performing private security functions are only to be used in accordance with DoD Instruction 1100.22, ''Guidance for Determining Workforce Mix,''[11] that is, they are limited to a defensive response to hostile acts or demonstrated hostile intent.

(D) Documentation of individual training covering weapons familiarization and qualification, rules for the use of force, limits on the use of force including whether defense of others is consistent with host nation Status of Forces Agreements or local law, the distinction between the rules of engagement applicable to military forces and the prescribed rules for the use of force that control the use of weapons by civilians, and the Law of Armed Conflict.

(E) Written acknowledgment by the PSC and its individual PSC personnel, after investigation of background of PSC personnel by the contractor, verifying such personnel are not prohibited under U.S. law to possess firearms.

(F) Written acknowledgment by the PSC and individual PSC personnel that:

(1) Potential civil and criminal liability exists under U.S. and local law or host nation Status of Forces Agreements for the use of weapons.[12]

(2) Proof of authorization to be armed must be carried by each PSC personnel.

(3) PSC personnel may possess only U.S.G.-issued and/or -approved weapons and ammunition for which they have been qualified according to paragraph (a)(1)(iii)(E) of this section.

[10] Available at *http://www.dtic.mil/whs/directives/corres/html/521056.htm*.

[11] Available at *http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf*.

[12] This requirement is specific to arming procedures. Such written acknowledgement should not be construed to limit civil and criminal liability to conduct arising from ''the use of weapons.'' PSC personnel could be held criminally liable for any conduct that would constitute a federal offense (see MEJA, 18 USC 3261(a)).

(4) PSC personnel were briefed and understand limitations on the use of force.

(5) Authorization to possess weapons and ammunition may be revoked for non-compliance with established rules for the use of force.

(*6*) PSC personnel are prohibited from consuming alcoholic beverages or being under the influence of alcohol while armed.

(iv) Registration and identification in the Synchronized Predeployment and Operational Tracker (or its successor database) of armored vehicles, helicopters, and other vehicles operated by PSC personnel.

(v) Reporting alleged criminal activity or other incidents involving PSCs or PSC personnel by another company or any other person. All incidents involving the following shall be reported and documented:

(A) A weapon is discharged by an individual performing private security functions;

(B) An individual performing private security functions is killed or injured in the performance of their duties;

(C) A person other than an individual performing private security functions is killed or injured as a result of conduct by PSC personnel;

(D) Property is destroyed as a result of conduct by a PSC or PSC personnel;

(E) An individual performing private security functions has come under attack including in cases where a weapon is discharged against an individual performing private security functions or personnel performing such functions believe a weapon was so discharged; or

(F) Active, non-lethal counter-measures (other than the discharge of a weapon) are employed by PSC personnel in response to a perceived immediate threat in an incident that could significantly affect U.S. objectives with regard to the military mission or international relations.

(vi) The independent review and, if practicable, investigation of incidents reported pursuant to paragraphs (a)(1)(v)(A) through (a)(1)(v)(F) of this section and incidents of alleged misconduct by PSC personnel.

(vii) Identification of ultimate criminal jurisdiction and investigative responsibilities, where conduct of U.S.G.-funded PSCs or PSC personnel are in question, in accordance with applicable laws to include a recognition of investigative jurisdiction and coordination for joint investigations (i.e., other U.S.G. agencies, host nation, or third country agencies), where the conduct of PSCs and PSC personnel is in question.

(viii) A mechanism by which a commander of a combatant command may request an action by which PSC personnel who are non-compliant with contract requirements are removed from the designated operational area.

(ix) Interagency coordination of administrative penalties or removal, as appropriate, of non-DoD PSC personnel who fail to comply with the terms and conditions of their contract, as is applicable to this part.

(x) Implementation of the training requirements contained below in paragraph (a)(2)(ii) of this section.

(2) Specifically cover:

(i) Matters relating to authorized equipment, force protection, security, health, safety, and relations and interaction with locals in accordance with DoD Instruction 3020.41, ''Contractor Personnel Authorized to Accompany the U.S. Armed Forces.''

(ii) Predeployment training requirements addressing, at a minimum, the identification of resources and assistance available to PSC personnel as well as country information and cultural training, and guidance on working with host country nationals and military personnel.

(iii) Rules for the use of force and graduated force procedures.

(iv) Requirements and procedures for direction, control and the maintenance of communications with regard to the movement and coordination of PSCs and PSC personnel, including specifying interoperability requirements. These include coordinating with the Chief of Mission, as necessary, private security operations outside secure bases and U.S. diplomatic properties to include movement control procedures for all contractors, including PSC personnel.

(b) *Availability of Guidance and Procedures.* The geographic Combatant Commander shall ensure the guidance and procedures prescribed in paragraph (a)

of this section are readily available and accessible by PSCs and their personnel (e.g., on a Web page and/or through contract terms), consistent with security considerations and requirements.

(c) *Subordinate Guidance and Procedures.* The Subordinate Commander, in consultation with the Chief of Mission, will issue guidance and procedures implementing the standing combatant command publications specified in paragraph (a) of this section, consistent with the situation and operating environment.

(d) *Consultation and Coordination.* The Chief of Mission and the geographic Combatant Commander/Subordinate Commander shall make every effort to consult and coordinate responses to common threats and common concerns related to oversight of the conduct of U.S.G.-funded PSC and their personnel. The Memorandum of Agreement between the Department of Defense and Department of State on U.S.G. Private Security Contractors[13] shall provide the framework for the development of guidance and procedures without regard to the specific locations identified therein.

[13] Available at *http://www.acq.osd.mil/log/PS/p__vault.html.*