

§ 154.16

32 CFR Ch. I (7-1-10 Edition)

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 re-entry 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:

Office of the Secretary of Defense

§ 154.16

(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 clas-

sified 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 5230.11¹ 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 re-issued 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 5100.3¹ 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 adju-

icated 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.

§ 154.17

32 CFR Ch. I (7-1-10 Edition)

(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