

## Office of the Secretary of Transportation

## § 8.29

records management that will facilitate the public release of documents at the time such documents are declassified under the provisions of this part for automatic declassification. To the maximum extent possible without destroying the integrity of the Department's files, all such material will be segregated or set aside for public release upon request. The Department will cooperate with the Archivist in efforts to establish a Government-wide database of information that has been declassified.

### Subpart C—Access to Information

#### § 8.25 Personnel Security Review Board.

(a) There is hereby established a Department of Transportation Personnel Security Review Board, which will, on behalf of the Secretary of Transportation (except in any case in which the Secretary personally makes the decision), make the administratively final decision on an appeal arising in any part of the Department from:

(1) A decision not to grant access to classified information;

(2) A decision to revoke access to classified information; or

(3) A decision under § 8.29 to deny access to classified information.

(b) The Personnel Security Review Board will be composed of:

(1) Two persons appointed by the Assistant Secretary for Administration: one from the Office of Personnel and Training, and one, familiar with personnel security adjudication, from the Office of Security and Administrative Management, who will serve as Chair;

(2) One person appointed by the General Counsel, who, in addition to serving as a member of the Board, will provide to the Board whatever legal services it may require; and

(3) One person appointed by each of the Commandant of the Coast Guard and the Federal Aviation Administrator.

(4) Any member may designate a representative, meeting the same criteria as the member, with full power to serve in his/her place.

(c) In carrying out its responsibilities to review final decisions to revoke or deny access to classified information,

the Board will establish whatever procedures it deems fit.

#### § 8.27 Public availability of declassified information.

(a) It is a fundamental policy of the Department to make information available to the public to the maximum extent permitted by law. Information that is declassified for any reason loses its status as material protected in the interest of national security. Accordingly, declassified information will be handled in every respect on the same basis as all other unclassified information. Declassified information is subject to the Departmental public information policies and procedures, with particular reference to the Freedom of Information Act (5 U.S.C. 552) and implementing Departmental regulations (49 CFR part 7).

(b) In furtherance of this policy, all classified material produced after June 1, 1972 that is of sufficient historical or other value to warrant preservation as permanent records in accordance with appropriate records administrative standards, and that becomes declassified, will be systematically reviewed prior to the end of each calendar year for the purpose of making the material publicly available. To the maximum extent possible without destroying the integrity of the Department's files, all such material will be segregated or set aside for public release upon request.

#### § 8.29 Access by historical researchers and former Presidential appointees.

(a) *Historical researchers.* (1) Persons outside the executive branch who are engaged in historical research projects may have access to classified information provided that:

(i) Access to the information is clearly consistent with the interests of national security; and

(ii) The person to be granted access is trustworthy.

(2) The provisions of this paragraph apply only to persons who are conducting historical research as private individuals or under private sponsorship and do not apply to research conducted under Government contract or sponsorship. The provisions are applicable only to situations where the classified information concerned, or any

**§ 8.29**

**49 CFR Subtitle A (10-1-11 Edition)**

part of it, was originated by the Department or its contractors, or where the information, if originated elsewhere, is in the sole custody of the Department. Any person requesting access to material originated in another agency or to information under the exclusive jurisdiction of the National Archives and Records Administration (NARA) will be referred to the other agency or to NARA, as appropriate.

(3) When a request for access to classified information for historical research is received, it will be referred to the appropriate local security office. That office will obtain from the applicant completed Standard Form 86, Questionnaire for National Security Positions, in triplicate, and Standard Form 87, Fingerprint Chart; a statement in detail to justify access, including identification of the kind of information desired and the organization or organizations, if any, sponsoring the research; and a written statement (signed, dated, and witnessed) with respect to the following:

(i) That the applicant will abide by regulations of the Department:

(A) To safeguard classified information; and

(B) To protect information that has been determined to be proprietary or privileged and is therefore not eligible for public dissemination.

(ii) That the applicant understands that any classified information that the applicant receives affects the security of the United States.

(iii) That the applicant acknowledges an obligation to safeguard classified information or privileged information of which the applicant gains possession or knowledge as a result of the applicant's access to files of the Department.

(iv) That the applicant agrees not to reveal to any person or agency any classified information or privileged information obtained as a result of the applicant's access except as specifically authorized in writing by the Department, and further agrees that the applicant shall not use the information for purposes other than those set forth in the applicant's application.

(v) That the applicant agrees to authorize a review of the applicant's notes and manuscript for the sole purpose of determining that no classified

information or material is contained therein.

(vi) That the applicant understands that failure to abide by conditions of this statement will constitute sufficient cause for canceling the applicant's access to classified information and for denying the applicant any future access, and may subject the applicant to criminal provisions of Federal law as referred to in this statement.

(vii) That the applicant is aware and fully understands that title 18, United States Code, Crimes and Criminal Procedures, and the Internal Security Act of 1950, as amended, title 50, United States Code, prescribe, under certain circumstances, criminal penalties for the unauthorized disclosure of information respecting the national security, and for loss, destruction, or compromise of such information.

(viii) That this statement is made to the U.S. Government to enable it to exercise its responsibilities for the protection of information affecting the national security.

(ix) That the applicant understands that any material false statement that the applicant makes knowingly and willfully will subject the applicant to the penalties of 18 U.S.C. 1001.

(4) The security office will process the forms in the same manner as specified for a preappointment national agency check for a critical-sensitive position. Upon receipt of the completed national agency check, the security office, if warranted, may determine that access by the applicant to the information will be clearly consistent with the interests of national security and the person to be granted access is trustworthy. If deemed necessary, before making its determination, the office may conduct or request further investigation. Before access is denied in any case, the matter will be referred through channels to the Director of Security and Administrative Management for review and submission to the Personnel Security Review Board for final review.

(5) If access to TOP SECRET or intelligence or communications security information is involved a special background investigation is required. However, this investigation will not be requested until the matter has been referred through channels to the Director of Security and Administrative Management for determination as to adequacy of the justification and the consent of other agencies as required.

(6) When it is indicated that an applicant's research may extend to material originating in the records of another agency, approval must be obtained from the other agency prior to the grant of access.

(7) Approvals for access will be valid for the duration of the current research project but no longer than 2 years from the date of issuance, unless renewed. If a subsequent request for similar access is made by the individual within one year from the date of completion of the current project, access may again be granted without obtaining a new National Agency Check. If more than one year has elapsed, a new National Agency Check must be obtained. The local security office will promptly advise its headquarters security staff of all approvals of access granted under the provisions of this section.

(8) An applicant may be given access only to that classified information that is directly pertinent to the applicant's approved project. The applicant may review files or records containing classified information only in offices under the control of the Department. Procedures must be established to identify classified material to which the applicant is given access. The applicant must be briefed on local procedures established to prevent unauthorized access to the classified material while in the applicant's custody, for the return of the material for secure storage at the end of the daily working period, and for the control of the applicant's notes until they have been reviewed. In addition to the security review of the applicant's manuscript, the manuscript must be reviewed by appropriate offices to assure that it is technically accurate insofar as material obtained from the Department is concerned, and is consistent with the Department's public release policies.

(b) *Former Presidential appointees.* Persons who previously occupied policy-making positions to which they were appointed by the President may be granted access to classified information or material that they originated, reviewed, signed, or received, while in public office, provided that:

(1) It is determined that such access is clearly consistent with the interests of national security; and

(2) The person agrees to safeguard the information, to authorize a review of the person's notes to assure that classified information is not contained therein, and that the classified information will not be further disseminated or published.

#### § 8.31 Industrial security.

(a) *Background.* The National Industrial Security Program was established by Executive Order 12829 of January 6, 1993 for the protection of information classified pursuant to Executive Order 12356 of April 2, 1982, National Security Information, or its predecessor or successor orders, and the Atomic Energy Act of 1954, as amended. The Secretary of Defense serves as the Executive Agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders that require or will require access to, or that store or will store, classified information, and for determining the eligibility for access to classified information of contractors, licensees, certificate holders, and grantees, and their respective employees.

(b) *Implementing regulations.* The Secretary of Transportation has entered into agreement for the Secretary of Defense to render industrial security services for the Department of Transportation. Regulations prescribed by the Secretary of Defense to fulfill the provisions of Executive Order 12829 have been extended to protect release of classified information for which the Secretary of Transportation is responsible. Specifically, this regulation is DOD 5220.22-M, National Industrial Security Program Operating Manual. This regulation is effective within the Department of Transportation, which functions as a User Agency as prescribed in the regulation. Appropriate security staffs, project personnel, and