

(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

contracting officers assure that actions required by the regulation are taken.

## PART 9—TESTIMONY OF EMPLOYEES OF THE DEPARTMENT AND PRODUCTION OF RECORDS IN LEGAL PROCEEDINGS

Sec.

- 9.1 Purpose.
- 9.2 Applicability.
- 9.3 Definitions.
- 9.5 General prohibition of production or disclosure in legal proceedings.
- 9.7 Testimony by employees before the Department or in other legal proceedings in which the United States is a party.
- 9.9 Legal proceedings between private litigants: General rules.
- 9.11 Legal proceedings between private litigants: Demands.
- 9.13 Legal proceedings between private litigants: Procedures to request records.
- 9.15 Legal proceedings between private litigants: Procedures to request testimony.
- 9.17 Legal proceedings between private litigants: Procedures for taking testimony.
- 9.19 Acceptance of service on behalf of Secretary.

AUTHORITY: 5 U.S.C. 301; 45 U.S.C. 41–42; 49 U.S.C. 322; 49 U.S.C. 504(f); 23 U.S.C. 409.

SOURCE: 58 FR 6724, Feb. 2, 1993, unless otherwise noted.

### § 9.1 Purpose.

(a) This part sets forth procedures governing the testimony of an employee in legal proceedings in which the United States is a party. It also sets forth procedures to be followed when an employee is issued a subpoena, order or other demand (collectively referred to in this part as a “demand”) by a court or other competent authority, or is requested by a private litigant, to provide testimony or produce records concerning information acquired in the course of performing official duties or because of the employee’s official status. It also prescribes the policies and procedures of the Department with respect to the acceptance of service of legal process and pleadings in legal proceedings involving the Department.

(b) The purposes of this part are to:

- (1) Conserve the time of employees for conducting official business;

- (2) Minimize the possibility of involving the Department in controversial issues not related to its mission;

- (3) Maintain the impartiality of the Department among private litigants;

- (4) Avoid spending the time and money of the United States for private purposes; and

- (5) To protect confidential, sensitive information and the deliberative processes of the Department.

(c) Agency counsel, in his or her discretion, may permit an exception from any requirement in this part. The exception may be granted only when the deviation will not interfere with matters of operational or military necessity, and when agency counsel determines that:

- (1) It is necessary to prevent a miscarriage of justice;

- (2) The Department has an interest in the decision that may be rendered in the legal proceeding; or

- (3) The exception is in the best interest of the Department or the United States.

For Office of Inspector General employees and documents, the Inspector General, in conjunction with the General Counsel of the Department, may permit an exception from any requirement of this part if the Inspector General determines, based on the Inspector General Act of 1978, as amended, that application of the requirement would be inappropriate.

### § 9.2 Applicability.

This part applies to the testimony of an employee in legal proceedings in which the United States is a party. It also applies in legal proceedings between private litigants to requests or demands for testimony or records concerning information acquired in the course of an employee performing official duties or because of the employee’s official status. This part does not apply to any legal proceeding in which an employee is to testify as to facts or events that are in no way related to the employee’s official duties or the functions of the Department. Nor does it apply to Congressional demands for testimony or documents.

### § 9.3 Definitions.

For purposes of this part: