AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PART 17—CLASSIFIED NATIONAL SECURITY INFORMATION AND ACCESS TO CLASSIFIED INFORMATION

AUTHORITY: 28 U.S.C. 501, 509, 510, 515–519; 5 U.S.C. 301; E.O. 12958, 60 FR 7977; 3 CFR, 1995 Comp., p. 333 19825; E.O. 12968, 60 FR 40245, 3 CFR, 1995 Comp., p. 391; 32 CFR part 2001.

SOURCE: Order No. 2091–97, 62 FR 36984, July 10, 1997, unless otherwise noted.

§17.1 Purpose.

The purpose of this part is to ensure that information within the Department of Justice (the ''Department'') relating to the national security is classified, protected, and declassified pursuant to the provisions of Executive Orders 12958 (3 CFR, 1995 Comp., p. 333) and 12968 (3 CFR, 1995 Comp., p. 391) and implementing directives from the Information Security Oversight Office of the National Archives and Records Administration (''ISOO''). Executive Orders 12958 and 12968 made numerous substantive changes in the system of classification, declassification, and downgrading of classified National Security Information and the criteria for access to this information. Accordingly, this part is a revision of the Department's classified information security rules.

(a) Subpart A of this part prescribes the implementation of Executive Orders 12958 and 12968 within the Department through the Assistant Attorney General for Administration, as the senior responsible agency official. Subpart A of this part also provides for certain relationships within the Department between the Assistant Attorney General for Administration, other component heads, and the Office of Intelligence Policy and Review.

(b) Subpart B of this part prescribes an orderly and progressive system for ensuring that every necessary safeguard and procedure is in place to assure that information is properly classified and that classified information is protected from unauthorized disclosure. Subpart B of this part requires original classification authorities to make classification decisions based on specific criteria; provides that most newly created classified information be considered for declassification after 10 years; provides that historically valuable information that is more than 25 years old (including information classified under prior Executive Orders) be automatically declassified, with appropriate exceptions; and establishes procedures for authorized holders of classified information to challenge the classification of information.

(c) Subpart C of this part establishes substantive standards and procedures for granting, denying, and revoking,

and for appealing decisions to deny access to classified information with an emphasis on ensuring the consistent, cost-effective, and efficient protection of classified information. Subpart C of this part provides a process that is fair and equitable to those with whom classified information is entrusted and, at the same time, assures the security of the classified information.

§ 17.2 Scope.

(a) All employees, contractors, grantees, and others granted access to classified information by the Department are governed by this part, and by the standards in Executive Order 12958, Executive Order 12968, and directives promulgated under those Executive Orders. If any portion of this part conflicts with any portion of Executive Order 12958, Executive Order 12968, or any successor Executive Order, the Executive Order shall apply. This part supersedes the former rule and any Department internal operating policy or directive that conflicts with any portion of this part.

(b) This part applies to non-contractor personnel outside of the Executive Branch and to contractor personnel or employees who are entrusted with classified national security information originated within or in the custody of the Department. This part does not affect the operation of the Department's participation in the National Industrial Security Program under Executive Order 12829 (3 CFR, 1993 Comp., p. 570).

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq*).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person. This part creates limited rights to administrative review of decisions pursuant to §§ 17.30, 17.31, and 17.47. This part does not, and is not intended to, create any right to judicial review of administrative action under §§ 17.14, 17.15, 17.18, 17.27, 17.30, 17.31 and 17.50.

§ 17.3 Definitions.

The terms defined or used in Executive Order 12958 and Executive Order 12968, and the implementing directives in 32 CFR 2001, are applicable to this part.

Subpart A—Administration

§ 17.11 Authority of the Assistant Attorney General for Administration.

(a) The Assistant Attorney General for Administration is designated as the senior agency official as required by § 5.6(c) of Executive Order 12958, and § 6.1(a) of Executive Order 12968 and, except as specifically provided elsewhere in this part, is authorized to administer the Department's national security information program pursuant to Executive Order 12958. The Assistant Attorney General for Administration shall appoint a Department Security Officer and may delegate to the Department Security Officer those functions under Executive Orders 12958 and 12968 that may be delegated by the senior agency official. The Department Security Officer may redelegate such functions when necessary to effectively implement this part.

(b) The Assistant Attorney General for Administration shall, among other actions:

(1) Oversee and administer the Department's program established under Executive Order No. 12958;

(2) Establish and maintain Department-wide security education and training programs;

(3) Establish and maintain an ongoing self-inspection program including the periodic review and assessment of the Department's classified product;

(4) Establish procedures to prevent unnecessary access to classified information, including procedures that:

(i) Require that a need for access to classified information is established before initiating administrative procedures to grant access; and

(ii) Ensure that the number of persons granted access to classified information is limited to the minimum necessary for operational and security requirements and needs;

(5) Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(6) Assure that the performance contract or other system used to rate personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(i) Original classification authorities;

(ii) Security managers or security specialists; and

(iii) All other personnel whose duties significantly involve the creation or handling of classified information;

(7) Account for the costs associated with implementing this part and report the cost to the Director of the ISOO;

(8) Assign in a prompt manner personnel to respond to any request, appeal, challenge, complaint, or suggestion concerning Executive Order 12958 that pertains to classified information that originated in a component of the Department that no longer exists and for which there is no clear successor in function;

(9) Cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines;

(10) Conduct periodic evaluations of the Department's implementation and administration of Executive Orders 12958 and 12968;

(11) Establish a plan for compliance with the automatic declassification provisions of Executive Order 12958 and oversee the implementation of that plan; and

(12) Maintain a list of specific files series of records exempted from automatic declassification by the Attorney General pursuant to section 3.4(c) of Executive Order 12958.

(c) The Department Security Officer may grant, deny, suspend, or revoke employee access to classified information pursuant to and in accordance with Executive Order 12968. The Department Security Officer may delegate the authority under this paragraph to qualified Security Programs Managers when the operational need justifies the delegation and when the Department Security Officer is assured that such officials will apply all access criteria in a uniform and correct manner in accord with the provisions of Executive Order 12968 and subpart C of this part. The fact that a delegation has been made pursuant to this section does not waive the Department Security Officer's authority to make any determinations that have been delegated.

(d) The Department Security Officer shall maintain a current list of all officials authorized pursuant to this part to originally classify or declassify documents.

(e) The Department Security Officer shall promulgate criteria and security requirements for the marking and safeguarding of information, transportation and transfer of information, preparation of classification guides, reporting of communications related to national security by persons granted access to classified information, reporting of information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security, and other matters necessary to the administration of the Executive Orders, the implementing regulations of the ISOO, and this part.

§ 17.12 Component head responsibilities.

The head of each component shall appoint and oversee a Security Programs Manager to implement this regulation. The Security Programs Managers shall:

(a) Observe, enforce, and implement security regulations or procedures pertaining to the classification, declassification, safeguarding, handling, and storage of classified national security information;

(b) Report violations of the provisions of this regulation to the Department Security Officer;

(c) Ensure that all employees acquire adequate security education and training as required by the provisions of the Department security regulations and procedures for classified information;

(d) Continuously review the requirements for personnel access to classified information as a part of the continuous need-to-know evaluation, and initiate action to administratively withdraw or

reduce the level of access authorized, as appropriate; and

(e) Cooperate fully with any request from the Department Security Officer for assistance in the implementation of this part.

§ 17.13 Office of Intelligence Policy and Review responsibilities; interpretation of Executive Orders.

(a) The Counsel for Intelligence Policy shall represent the Attorney General at interagency meetings on matters of general interest concerning national security information.

(b) The Counsel for Intelligence Policy shall provide advice and interpretation on any issues that arise under Executive Orders 12958 and 12968 and shall refer such questions to the Office of Legal Counsel, as appropriate.

(c) Any request for interpretation of Executive Order 12958 or Executive Order 12968, pursuant to section 6.1(b) of Executive Order 12958, and section 7.2(b) of Executive Order 12968, shall be referred to the Counsel for Intelligence Policy, who shall refer such questions to the Office of Legal Counsel, as appropriate.

§ 17.14 Department Review Committee.

(a) The Department Review Committee (DRC) is established to:

(1) Resolve all issues, except those related to the compromise of classified information, that concern the implementation and administration of Executive Order 12958, implementing directives from the ISOO, and subpart B of this part, including those issues concerning over-classification, failure to declassify, classification challenges, and delays in declassification not otherwise resolved;

(2) Review all appeals from denials of requests for records made under section 3.6 of Executive Order 12958 and the Freedom of Information Act (5 U.S.C. 552), when the proposed denial is based on their continued classification under Executive Order 12958;

(3) Recommend to the Attorney General appropriate administrative sanctions to correct the abuse or violation of any provision of Executive Order 12958, the implementing directives or subpart B of this part, except as it relates to the compromise of classified national security information; and

(4) Review, on appeal, challenges to classification actions and mandatory review requests.

(b)(1) The DRC shall consist of a senior representative designated by the:

(i) Deputy Attorney General;

(ii) Assistant Attorney General, Office of Legal Counsel;

(iii) Assistant Attorney General, Criminal Division;

(iv) Assistant Attorney General, Civil Division;

(v) Assistant Attorney General for Administration;

(vi) Director, Federal Bureau of Investigation; and

(vii) Counsel for Intelligence Policy.

(2) Each such official shall also designate in writing an alternate to serve in the absence of his or her representative. Four representatives shall constitute a quorum of the DRC. The Attorney General shall designate the Chairman of the DRC from among its members.

(c) The Office of Information and Privacy (OIP) shall provide the necessary administrative staff support for the DRC.

§ 17.15 Access Review Committee.

(a) The Access Review Committee (ARC) is hereby established to review all appeals from denials or revocations of eligibility for access to classified information under Executive Order 12968. Unless the Attorney General requests recommendations from the ARC and personally exercises appeal authority, the ARC's decisions shall be final.

(b) The ARC shall consist of the Deputy Attorney General or a designee, the Counsel for Intelligence Policy or a designee, and the Assistant Attorney General for Administration or a designee. Designations must be approved by the Attorney General.

(c) The Department Security Officer shall provide the necessary administrative staff support for the ARC.

§ 17.16 Violations of classified information requirements.

(a) Any person who suspects or has knowledge of a violation of this part, including the known or suspected loss

or compromise of national security information, shall promptly report and confirm in writing the circumstances to the Department Security Officer. Any person who makes such a report to the Department Security Officer shall promptly furnish a copy of such report:

(1) If the suspected violation involves a Department attorney (including an Assistant United States Attorney or Special Assistant United States Attorney) while engaged in litigation, grand jury proceedings, or giving legal advice, or a law enforcement officer assisting an attorney engaged in such activity, to the Office of Professional Responsibility;

(2) If the suspected violation involves an employee of the Federal Bureau of Investigation (FBI) or the Drug Enforcement Administration, other than a law enforcement officer in paragraph (a)(1) of this section, to the Office of Professional Responsibility in that component; or

(3) In any other circumstance, to the Office of the Inspector General.

(b) Department employees, contractors, grantees, or consultants may be reprimanded, suspended without pay, terminated from classification authority, suspended from or denied access to classified information, or subject to other sanctions in accordance with applicable law and Department regulation if they:

(1) Knowingly, willfully, or negligently disclose to unauthorized persons information classified under Executive Order 12958 or predecessor orders;

(2) Knowingly, willfully, or negligently classify or continue the classification of information in violation of Executive Order 12958 or its implementing directives; or

(3) Knowingly, willfully, or negligently violate any other provision of Executive Order 12958, or knowingly and wilfully grant eligibility for, or allow access to, classified information in violation of Executive Order 12968, or its implementing directives, this part, or security requirements promulgated by the Department Security Officer.

§ 17.17 Judicial proceedings.

(a)(1) Any Department official or organization receiving an order or subpoena from a federal or state court to produce classified information, required to submit classified information for official Department litigative purposes, or receiving classified information from another organization for production of such in litigation, shall immediately determine from the agency originating the classified information whether the information can be declassified. If declassification is not possible, the Department official or organization and the assigned Department attorney in the case shall take all appropriate action to protect such information pursuant to the provisions of this section.

(2) If a determination is made to produce classified information in a judicial proceeding in any manner, the assigned Department attorney shall take all steps necessary to ensure the cooperation of the court and, where appropriate, opposing counsel in safeguarding and retrieving the information pursuant to the provisions of this regulation.

(b) The Classified Information Procedures Act (CIPA), Pub. L. 96–456, 94 Stat. 2025, 18 U.S.C. App., and the ''Security Procedures Established Pursuant to Pub. L. 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information'' may be used in Federal criminal cases involving classified information. (Available from the Security and Emergency Planning Staff, Justice Management Division, Department of Justice, Washington, DC 20530.)

(c) In judicial proceedings other than Federal criminal cases where CIPA is used, the Department, through its attorneys, shall seek appropriate security safeguards to protect classified information from unauthorized disclosure, including, but not limited to, consideration of the following:

(1) A determination by the court of the relevance and materiality of the classified information in question;

(2) An order that classified information shall not be disclosed or introduced into evidence at a proceeding without the prior approval of either the originating agency, the Attorney General, or the President;

(3) A limitation on attendance at any proceeding where classified information is to be disclosed to those persons with appropriate authorization to access classified information whose duties require knowledge or possession of the classified information to be disclosed;

(4) A court facility that provides appropriate safeguarding for the classified information as determined by the Department Security Officer;

(5) Dissemination and accountability controls for all classified information offered for identification or introduced into evidence at such proceedings;

(6) Appropriate marking to indicate classified portions of any and any the maintenance of any classified under seal;

(7) Handling and storage of all classified information including classified portions of any transcript in a manner consistent with the provisions of this regulation and Department implementing directives;

(8) Return at the conclusion of the proceeding of all classified information to the Department or the originating agency, or placing the classified information under court seal;

(9) Retrieval by Department employees of appropriate notes, drafts, or any other documents generated during the course of the proceedings that contain classified information and immediate transfer to the Department for safeguarding and destruction as appropriate; and

(10) Full and complete advice to all persons to whom classified information is disclosed during such proceedings as to the classification level of such information, all pertinent safeguarding and storage requirements, and their liability in the event of unauthorized disclosure.

(d) Access to classified information by individuals involved in judicial proceedings other than employees of the Department is governed by § 17.46(c).

§ 17.18 Prepublication review.

(a) All individuals with authorized access to Sensitive Compartmented Information shall be required to sign nondisclosure agreements containing a provision for prepublication review to assure deletion of Sensitive Compartmented Information and other classified information. Sensitive Compartmented Information is information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods. The prepublication review provision will require Department of Justice employees and other individuals who are authorized to have access to Sensitive Compartmented Information to submit certain material, described further in the agreement, to the Department prior to its publication to provide an opportunity for determining whether an unauthorized disclosure of Sensitive Compartmented Information or other classified information would occur as a consequence of it publication.

(b) Persons subject to these requirements are invited to discuss their plans for public disclosures of information that may be subject to these obligations with authorized Department representatives at an early stage, or as soon as circumstances indicate these policies must be considered. Except as provided in paragraph (j) of this section for FBI personnel, all questions concerning these obligations should be addressed to the Counsel for Intelligence Policy, Department of Justice, 10th & Constitution Avenue, NW., Washington, DC 20530. The official views of the Department on whether specific materials require prepublication review may be expressed only by the Counsel for Intelligence Policy and persons should not act in reliance upon the views of other Department personnel.

(c) Prepublication review is required only as expressly provided for in a nondisclosure agreement. However, all persons who have had access to classified information have an obligation to avoid unauthorized disclosures of such information. Therefore, persons who have such access but are not otherwise required to submit to prepublication review under the terms of an employment or other nondisclosure agreement are encouraged to submit material for prepublication review voluntarily if

they believe that such material may contain classified information.

(d) The nature and extent of the material that is required to be submitted for prepublication review under nondisclosure agreements is expressly provided for in those agreements. It should be clear, however, that such requirements do not extend to any materials that exclusively contain information lawfully obtained at a time when the author has no employment, contract, or other relationship with the United States Government or that contain information exclusively acquired outside the scope of employment.

(e) A person's obligation to submit material for prepublication review remains identical whether such person prepares the materials or causes or assists another person (such as a ghost writer, spouse, friend, or editor) in preparing the material. Material covered by a nondisclosure agreement requiring prepublication review must be submitted prior to discussing it with or showing it to a publisher, co-author, or any other person who is not authorized to have access to it. In this regard, it should be noted that a failure to submit such material for prepublication review constitutes a breach of the obligation and exposes the author to remedial action even in cases where the published material does not actually contain Sensitive Compartmented Information or classified information. See *Snepp* v. *United States,* 444 U.S. 507 (1980).

(f) The requirement to submit material for prepublication review is not limited to any particular type of material or disclosure or methods of production. Written materials include not only book manuscripts but all other forms of written materials intended for public disclosure, such as (but not limited to) newspaper columns, magazine articles, letters to the editor, book reviews, pamphlets, scholarly papers, and fictional material.

(g) Oral statements are also within the scope of a prepublication review requirement when based upon written materials, such as an outline of the statements to be made. There is no requirement to prepare written materials for review, however, unless there is reason to believe in advance that oral statements may contain Sensitive Compartmented Information or other information required to be submitted for review under the terms of the nondisclosure agreement. Thus, a person may participate in an oral presentation where there is no opportunity for prior preparation (e.g., news interview, panel discussion) without violating the provisions of this paragraph.

(h) Material submitted for republication review will be reviewed solely for the purpose of identifying and preventing the disclosure of Sensitive Compartmented Information and other classified information. This review will be conducted in an impartial manner without regard to whether the material is critical of or favorable to the Department. No effort will be made to delete embarrassing or critical statements that are unclassified. Materials submitted for review will be disseminated to other persons or agencies only to the extent necessary to identify classified information.

(i) The Counsel for Intelligence Policy (or, in the case of FBI employees, the FBI's Office of Congressional and Public Affairs) will respond substantively to prepublication review requests within 30 working days of receipt of the submission. Priority shall be given to reviewing speeches, newspaper articles, and other materials that the author seeks to publish on an expedited basis. The Counsel's decisions may be appealed to the Deputy Attorney General, who will process appeals within 15 days of receipt of the appeal. The Deputy Attorney General's decision is final and not subject to further administrative appeal. Persons who are dissatisfied with the final administrative decision may obtain judicial review either by filing an action for declaratory relief or giving the Department notice of their intention to proceed despite the Department's request for deletions of classified information, and a reasonable opportunity (30 working days) to file a civil action seeking a court order prohibiting disclosure. Employees and other affected individuals remain obligated not to disclose or publish information determined by the Government to be classified until any civil action is resolved.

(j) The obligations of Department of Justice employees described in this subpart apply with equal force to employees of the FBI with following exceptions and provisos:

(1) Nothing in this subpart shall supersede or alter obligations assumed under the basic FBI employment agreement.

(2) FBI employees required to sign nondisclosure agreements containing a provision for prepublication review pursuant to this subpart shall submit materials for review to the Assistant Director, Office of Congressional and Public Affairs. Such individuals shall also submit questions as to whether specific materials require prepublication review under such agreements to that Office for resolution. Where such questions raise policy questions or concern significant issues of interpretation under such an agreement, the Assistant Director, Office of Congressional and Public Affairs, shall consult with the Counsel for Intelligence Policy prior to responding to the inquiry.

(3) Decisions of the Assistant Director, Office of Congressional and Public Affairs, concerning the deletion of classified information, may be appealed to the Director, FBI, who will process appeals within 15 working days of receipt. Persons who are dissatisfied with the Director's decision may, at their option, appeal further to the Deputy Attorney General as provided in paragraph (i) of this section. Judicial review, as set forth in that paragraph, is available following final agency action in the form of a decision by the Director or, if the appeal process in paragraph (i) of this section is pursued, the Deputy Attorney General.

Subpart B—Classified Information

§ 17.21 Classification and declassification authority.

(a) Top Secret original classification authority may only be exercised by the Attorney General, the Assistant Attorney General for Administration, and officials to whom such authority is delegated in writing by the Attorney General. No official who is delegated Top Secret classification authority pursuant to this paragraph may redelegate such authority.

(b) The Assistant Attorney General for Administration may delegate original Secret and Confidential classification authority to subordinate officials determined to have frequent need to exercise such authority. No official who is delegated original classification authority pursuant to this paragraph may redelegate such authority.

(c) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level. In the absence of an official authorized to exercise classification authority pursuant to this section, the person designated to act in lieu of such official may exercise the official's classification authority.

§ 17.22 Classification of information; limitations.

(a) Information may be originally classified only if all of the following standards are met:

(1) The information is owned by, produced by or for, or is under the control of the United States Government;

(2) The information falls within one or more of the categories of information specified in section 1.5 of Executive Order 12958; and

(3) The classifying official determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and such official is able to identify or describe the damage.

(b) Information may be classified as Top Secret, Secret, or Confidential according to the standards established in section 1.3 of Executive Order 12958. No other terms shall be used to identify United States classified national security information except as otherwise provided by statute.

(c) Information shall not be classified if there is significant doubt about the need to classify the information. If there is significant doubt about the appropriate level of classification with respect to information that is being classified, it shall be classified at the lower classification of the levels considered.

(d) Information shall not be classified in order to conceal inefficiency, violations of law, or administrative error; to

prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay release of information that does not require protection in the interest of national security. Information that has been declassified and released to the public under proper authority may not be reclassified.

(e) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after the Department has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of §17.31. When it is necessary to classify or reclassify such information, it shall be forwarded to the Department Security Officer and classified or reclassified only at the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for Administration.

(f) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that meets the standards for classification under Executive Order 12958 and that is not otherwise revealed in the individual items of information.

§17.23 Emergency classification requests.

(a) Whenever any employee, contractor, licensee, certificate holder, or grantee of the Department who does not have original classification authority originates or develops information that requires immediate classification and safeguarding, and no authorized classifier is available, that person shall:

(1) Safeguard the information in a manner appropriate for its classification level;

(2) Apply the appropriate overall classification markings; and

(3) Within five working days, securely transmit the information to the organization that has appropriate subject matter interest and classification authority.

(b) When it is not clear which Department organization would be the appropriate original classifier, the information shall be sent to the Department Security Officer to determine the appropriate organization.

(c) The organization with classification authority shall decide within 30 days whether to classify information.

§17.24 Duration of classification.

(a) At the time of original classification, original classification authorities shall attempt to establish a specific date or event for declassification not more than 10 years from the date of the original decision based on the duration of the national security sensitivity of the information. If the original classification authority cannot determine an earlier specific date or event for declassification, the information shall be marked for declassification 10 years from the date of the original decision.

(b) At the time of original classification, an original classification authority may exempt specific information from declassification within 10 years in accordance with section 1.6(d) of Executive Order 12958.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under, and subject to the limitations of, Executive Order 12958.

§17.25 Identification and markings.

(a) Classified information must be marked pursuant to the standards set forth in section 1.7 of Executive Order 12958; ISOO implementing directives in 32 CFR 2001, subpart B; and internal Department of Justice direction provided by the Department Security Officer.

(b) Foreign government information shall be marked or classified at a level equivalent to that level of classification assigned by the originating foreign government.

(c) Information assigned a level of classification under predecessor Executive Orders shall be considered as classified at that level of classification.

§17.26 Derivative classification.

(a) Persons need not possess original classification authority to derivatively

classify information based on source documents or classification guides.

(b) Persons who apply derivative classification markings shall observe original classification decisions and carry forward to any newly created documents the pertinent classification markings.

(c) Information classified derivatively from other classified information shall be classified and marked in accordance with the standards set forth in sections 2.1–2.3 of Executive Order 12958, the ISOO implementing directives in 32 CFR 2001.22, and internal Department directions provided by the Department Security Officer.

§ 17.27 Declassification and downgrading.

(a) Classified information shall be declassified as soon as it no longer meets the standards for classification. Declassification and downgrading is governed by § 3.1–3.3 of Executive Order 12958, implementing ISOO directives at 32 CFR 2001, subpart E, and applicable internal Department of Justice direction provided by the Department Security Officer.

(b) Information shall be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, the originator's successor, or a supervisory official of either, or by officials delegated such authority in writing by the Attorney General or the Assistant Attorney General for Administration.

(c) It is presumed that information that continues to meet the classification requirements under Executive Order 12958 requires continued protection. In some exceptional cases during declassification reviews, the need to protect classified information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. If it appears that the public interest in disclosure of the information may outweigh the need to protect the information, the declassification reviewing official shall refer the case with a recommendation for decision to the DRC. The DRC shall review the case and make a recommendation to the Attorney General on whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. The Attorney General shall decide whether to declassify the information. The decision of the Attorney General shall be final. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural rights subject to judicial review.

(d) Each component shall develop schedules for declassification of records in the National Archives. The Department shall cooperate with the National Archives and Records Administration and the Presidential Libraries to ensure that declassification is accomplished in a timely manner.

§ 17.28 Automatic declassification.

(a) Subject to paragraph (b) of this section, all classified information contained in records that are more than 25 years old that have been determined to have permanent historical value shall be declassified automatically on April 17, 2000. Subsequently, all classified information in such records shall be automatically declassified not later than 25 years after the date of its original classification with the exception of specific information exempt from automatic declassification pursuant to section 3.4 (b) and (d) of Executive Order 12958.

(b) At least 220 days before information is declassified automatically under this section, the respective component head shall notify the Assistant Attorney General for Administration through the Department Security Officer of any specific information they propose to exempt from automatic declassification. The notification shall include:

(1) A description of the information;

(2) An explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) A specific date or event for declassification of the information whenever the information exempted does not identify a confidential human source or human intelligence source.

(c) Proposed exemptions under this section shall be forwarded to the DRC,

which shall recommend a disposition of the exemption request to the Assistant Attorney General for Administration. When the Assistant Attorney General for Administration determines the exemption request is consistent with this section, he or she will submit it to the Executive Secretary of the Interagency Security Classification Appeals Panel.

(d) Declassification guides that narrowly and precisely define exempted information may be used to exempt information from automatic declassification. Declassification guides must include the exemption notification information detailed in paragraph (b) of this section, and be approved pursuant to paragraph (c) of this section.

§ 17.29 Documents of permanent historical value.

The original classification authority, to the greatest extent possible, shall declassify classified information contained in records determined to have permanent historical value under title 44 of the United States Code before they are accessioned into the National Archives. The Department shall cooperate with the National Archives and Records Administration in carrying out an automatic declassification program involving accessioned Department records, presidential papers, and historical materials under the control of the Archivist of the United States.

§ 17.30 Classification challenges.

(a) Authorized holders of information classified by the Department who, in good faith, believe that specific information is improperly classified or unclassified are encouraged and expected to challenge the classification status of that information pursuant to section 1.9 of Executive Order 12958. Authorized holders may submit classification challenges in writing to the DRC, through the Office of Information and Privacy, United States Department of Justice, Washington, DC 20530. The challenge need not be more specific than a question as to why the information is or is not classified, or is classified at a certain level.

(b) The DRC shall redact the identity of an individual challenging a classification under paragraph (a) of this section and forward the classification challenge to the original classification authority for review and response.

(c) The original classification authority shall promptly, and in no case later than 30 days, provide a written response to the DRC. The original classification authority may classify or declassify the information subject to challenge or state specific reasons why the original classification determination was proper. If the original classification authority is not able to response within 30 days, the DRC shall inform the individual who filed the challenge in writing of that fact, and the anticipated determination date.

(d) The DRC shall inform the individual challenging the classification of the determination made by the original classification authority and that individual may appeal this determination to the DRC. Upon appeal, the DRC may declassify, or direct the classification of, the information. If the DRC is not able to act on any appeal within 45 days of receipt, the DRC shall inform the individual who filed the challenge in writing of that fact, and the anticipated determination date.

(e) The DRC shall provide the individual who appeals a classification challenge determination with a written explanation of the basis for the DRC decision and a statement of his or her right to appeal that determination to the Interagency Security Classification Appeals Panel (ISCAP) pursuant to section 5.4 of Executive Order 12958 and the rules issued by the ISCAP pursuant to section 5.4 of Executive Order 12958.

(f) Any individual who challenges a classification and believes that any action has been taken against him or her in retribution because of that challenge shall report the facts to the Office of the Inspector General or the Office of Professional Responsibility, as appropriate.

(g) Requests for review of classified material for declassification by persons other than authorized holders are governed by § 17.31.

§ 17.31 Mandatory review for declassification requests.

(a) Any person may request classified information be reviewed for declassification pursuant to the mandatory declassification review provisions of

section 3.6 of Executive Order 12958. After such a review, the information or any reasonably segregable portion thereof that no longer requires protection under this part shall be declassified and released to the requester unless withholding is otherwise warranted under applicable law. If the information, although declassified, is withheld, the requester shall be given a brief statement as to the reasons for denial and a notice of the right to appeal the determination to the Director, Office of Information and Privacy (OIP), United States Department of Justice, Washington, DC 20530. If the mandatory review for declassification request relates to the classification of information that has been reviewed for declassification within the past two years or that is the subject of pending litigation, the requester shall be informed of that fact and the administrative appeal rights.

(b) Request for mandatory review for declassification and any subsequent appeal to the DRC shall be submitted to the Director, Office of Information and Privacy, United States Department of Justice, Washington, DC 20530, describing the document or material containing the information with sufficient specificity to enable the Department to locate that information with a reasonable amount of effort. The OIP shall promptly forward the request to the component that originally classified the information, or the DRC in the case of an appeal, and provide the requester with an acknowledgement of receipt of the request.

(c) When the description of the information in a request is deficient, the component shall solicit as much additional identifying information as possible from the requestor. Before denying a request on the basis that the information or material is not obtainable with a reasonable amount of effort, the component shall ask the requestor to limit the request to information or material that is reasonably obtainable. If the information or material requested cannot be described in sufficient particularity, or if it cannot be obtained with a reasonable amount of effort, the component shall provide the requestor with written notification of the reasons why no action will be taken and the right to appeal the decision to the DRC.

(d) The component that originally classified the information shall provide a written response to requests for mandatory review within 60 days whenever possible, or shall inform the requester in writing why additional time is needed. Unless there are unusual circumstances, the additional time needed by the component originally classifying the information shall not extend beyond 180 days from the receipt of the request. If no determination has been made at the end of the 180 day period, the requester may apply to the DRC for a determination.

(e) If the component that originally classified the information determines that continued classification is warranted, it shall notify the requester in writing of the decision and the right to appeal the decision to the DRC no later that 60 days after receipt of the notification of the decision.

(f) The DRC shall determine the appeals of the components' mandatory declassification review decisions within 60 days after receipt of the appeal, or notify the requester why additional time is needed. In making its determinations concerning requests for declassification of classified information, the DRC, for administrative purposes, shall impose the burden of proof on the originating component to show that continued classification is warranted. The DRC shall provide the requester with a written statement of reasons for its decisions.

(g) If the individual requesting review of a classification is not satisfied with the DRC's decision, he or she may appeal to the ISCAP pursuant to section 5.4 of Executive Order 12958 and rules issued by the ISCAP pursuant to that section.

§ 17.32 Notification of classification changes.

All known holders of information affected by unscheduled classification changes actions shall be notified promptly of such changes by the original classifier or the authority making the change in classification.

Supart C—Access to Classified Information

§ 17.41 Access to classified information.

(a) No person may be given access to classified information or material originated by, in the custody, or under the control of the Department, unless the person—

(1) Has been determined to be eligible for access in accordance with sections 3.1–3.3 of Executive Order 12968;

(2) Has a demonstrated need-to-know; and

(3) Has signed an approved nondisclosure agreement.

(b) Eligibility for access to classified information is limited to United States citizens for whom an appropriate investigation of their personal and professional history affirmatively indicated loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of the national security. Sections 2.6 and 3.3 of Executive Order 12968 provide only limited exceptions to these requirements.

(c) The Department of Justice does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information. However, the Department may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No negative inferences concerning the standards for access may be raised solely on the basis of the sexual orientation of the employee or mental health counseling.

(d) An employee granted access to classified information may be investigated at any time to ascertain whether he or she continues to meet the requirements for access.

(e) An employee granted access to classified information shall provide to the Department written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of three years thereafter, to:

(1) Financial records maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in 12 U.S.C. 3401;

(2) Consumer reports under the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*); and

(3) Records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(f) Information may be requested pursuant to the employee consent obtained under paragraph (e) of this section only where:

(1) There are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(2) Information the Department deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or

(3) Circumstances indicate that the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

§ 17.42 Positions requiring financial disclosure.

(a) The Assistant Attorney General for Administration, in consultation with the Counsel for Intelligence Policy, shall designate each employee, by position or category where possible, who has a regular need for access to

any of the categories of classified information described in section 1.3(a) of Executive Order 12968.

(b) An employee may not hold a position designated as requiring a regular need for access to categories of classified information described in section 1.3(a) of Executive Order 12968 unless, as a condition of access to such information, the employee files with the Department Security Officer:

(1) A financial disclosure form developed pursuant to section 1.3(c) of Executive Order 12968 as part of all background investigations or reinvestigations;

(2) The same financial disclosure form, if selected by the Department Security Officer on a random basis; and

(3) Relevant information concerning foreign travel, as determined by the Department Security Officer.

§ 17.43 Reinvestigation requirements.

Employees who are eligible for access to classified information shall be subject to periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access.

§ 17.44 Access eligibility.

(a) Determinations of eligibility for access to classified information are separate from suitability determinations with respect to the hiring or retention of persons for employment by the Department or any other personnel actions.

(b) The number of employees eligible for access to classified information shall be kept to the minimum required for the conduct of Department functions.

(c) Eligibility for access to classified information shall be limited to classification levels for which there is a need for access. No person shall be granted eligibility higher than his or her need.

§ 17.45 Need-to-know.

No person shall be granted access to specific classified information unless that person has an actual need-to-know that classified information, pursuant to section 2.5 of Executive Order 12968.

§ 17.46 Access by persons outside the Executive Branch.

(a) Classified information shall not be disseminated outside the Executive Branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the Executive Branch.

(b) Classified information originated by or in the custody of the Department may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Federal Government will derive a benefit or advantage and that the release is not prohibited by the originating department or agency (or foreign government in the case of Foreign Government Information). Before such a release is made, the head of the Office, Board, Division, or Bureau making the release shall determine the propriety of such action, in the interest of the national security, and must approve the release. Prior to the release, the Department Security Officer must confirm that the recipient is eligible for access to the classified information involved and agrees to safeguard the information in accordance with the provisions of this part.

(c) Members of Congress, Justices of the United States Supreme Court, and Judges of the United States Courts of Appeal and District Courts do not require a determination of their eligibility for access to classified information by the Department. Federal Magistrate Judges must be determined eligible for access to classified information by the Department Security Officer pursuant to procedures approved by the Assistant Attorney General for Administration in consultation with the Judicial Conference of the United States. All other Legislative and Judicial personnel including, but not limited to, congressional staff, court reporters, typists, secretaries, law clerks, and translators who require access to classified information must be determined eligible by the Department Security Officer consistent with standards established in this regulation.

(d) When other persons outside the Executive Branch who are not subject to the National Industrial Security

Program require access to classified information originated by or in the custody of the Department, but do not otherwise possess a proper access authorization, an appropriate background investigation must be completed to allow the Department Security Officer to determine their eligibility for access to classified information. The length of time it generally takes to complete an expedited background investigation is 90 days. Therefore, all persons requiring access to classified information to participate in congressional or judicial proceedings should be identified and the background investigation initiated far enough in advance to ensure a minimum impact on such proceedings.

(e) Personnel who are subject to a Department contract or grant or who are rendering consultant services to the Department and require access to classified information originated by or in the custody of the Department shall be processed for such access pursuant to procedures approved by the Assistant Attorney General for Administration.

(f)(1) The requirement that access to classified information may be granted only as is necessary for the performance of official duties may be waived, pursuant to section 4.5(a) of Executive Order 12958, for persons who:

(i) Are engaged in historical research projects; or

(ii) Have previously occupied policy-making positions to which they were appointed by the President.

(2) All persons receiving access pursuant to this paragraph (f) must have been determined to be trustworthy by the Department Security Officer as a precondition before receiving access. Such determinations shall be based on such investigation as the Department Security Officer deems appropriate. Historical researchers and former presidential appointees shall not have access to Foreign Government Information without the written permission from an appropriate authority of the foreign government concerned.

(3) Waivers of the ''need-to-know'' requirement under this paragraph (f) may be granted by the Department Security Officer provided that the Security Programs Manager of the Office, Board, Division, or Bureau with classification jurisdiction over the information being sought:

(i) Makes a written determination that such access is consistent with the interest of national security;

(ii) Limits such access to specific categories of information over which the Department has classification jurisdiction;

(iii) Maintains custody of the classified information at a Department facility;

(iv) Obtains the recipient's written and signed agreement to safeguard the information in accordance with the provisions of this regulation and to authorize a review of any notes and manuscript for determination that no classified information is contained therein; and

(v) In the case of former presidential appointees, limits their access to items that such former appointees originated, reviewed, signed, or received while serving as a presidential appointee and ensures that such appointee does not remove or cause to be removed any classified information reviewed.

(4) If access requested by historical researchers and former presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to 31 U.S.C. 9701, the requester shall be so notified and fees may be imposed.

§ 17.47 Denial or revocation of eligibility for access to classified information.

(a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of Executive order 12968 shall be:

(1) Provided with a comprehensive and detailed written explanation of the basis for that decision as the national security interests of the United States and other applicable law permit and informed of their right to be represented by counsel or other representative at their own expense;

(2) Permitted 30 days from the date of the written explanation to request any documents, records, or reports including the entire investigative file upon which a denial or revocation is based; and

(3) Provided copies of documents requested pursuant to this paragraph (a) within 30 days of the request to the extent such documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), and as the national security interests and other applicable law permit.

(b) An applicant or employee may file a written reply and request for review of the determination within 30 days after written notification of the determination or receipt of the copies of the documents requested pursuant to this subpart, whichever is later.

(c) An applicant or employee shall be provided with a written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal.

(d) Within 30 days of receipt of a determination under paragraph (c) of this section, the applicant or employee may appeal that determination in writing to the ARC, established under §17.15. The applicant or employee may request an opportunity to appear personally before the ARC and to present relevant documents, materials, and information.

(e) An applicant or employee may be represented in any such appeal by an attorney or other representative of his or her choice, at his or her expense. Nothing in this section shall be construed as requiring the Department to grant such attorney or other representative eligibility for access to classified information, or to disclose to such attorney or representative, or permit the applicant or employee to disclose to such attorney or representative, classified information.

(f) A determination of eligibility for access to classified information by the ARC is a discretionary security decision. Decisions of the ARC shall be in writing and shall be made as expeditiously as possible. Access shall be granted only where facts and circumstances indicate that access to classified information is clearly consistent with the national security interest of the United States, and any doubt shall be resolved in favor of the national security.

(g) The Department Security Officer shall have an opportunity to present relevant information in writing or, if the applicant or employee appears personally, in person. Any such written submissions shall be made part of the applicant's or employee's security record and, as the national security interests of the United States and other applicable law permit, shall also be provided to the applicant or employee. Any personal presentations shall be, to the extent consistent with the national security and other applicable law, in the presence of the applicant or employee.

(h) When the Attorney General or Deputy Attorney General personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This is a discretionary and final decision not subject to further review.

(i) This section does not limit the authority of the Attorney General pursuant to any other law or Executive Order to deny or terminate access to classified information if the national security so requires and the Attorney General determines that the appeal procedures set forth in this section cannot be invoked in a manner that is consistent with the national security. Nothing in this section requires that the Department provide any procedures under this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any reason other than denial of eligibility for access to classified information. Suitability determinations shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

PART 18—OFFICE OF JUSTICE PROGRAMS HEARING AND APPEAL PROCEDURES

Sec.