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 Assistant Attorney General for National Security 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.

[Order No. 2091–97, 62 FR 36984, July 10, 1997, as amended by Order No. 2865–2007, 72 FR 10069, Mar. 7, 2007]

§ 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