

## § 15.4

Torts Branch, Civil Division, Department of Justice.

(b) The appropriate Federal agency shall submit a report to the United States Attorney for the district embracing the place where the civil action or proceeding is brought fully addressing whether the person was acting as a covered person at the time of the incident out of which the suit arose, and a copy of the report shall be sent by the appropriate Federal agency to the responsible Branch Director of the Torts Branch, Civil Division, Department of Justice.

(c) A report under this section shall be submitted at the earliest possible date, or within such time as shall be fixed upon request by the United States Attorney or the responsible Branch Director of the Torts Branch.

### § 15.4 Removal and defense of suits.

(a) The United States Attorney for the district where the civil action or proceeding is brought, or any Director of the Torts Branch, Civil Division, Department of Justice, is authorized to make the statutory certification that the Federal employee was acting within the scope of his office or employment with the Federal Government at the time of the incident out of which the suit arose.

(b) The United States Attorney for the district where the civil action or proceeding is brought, or any Director of the Torts Branch, Civil Division, Department of Justice, is authorized to make the statutory certification that the covered person was acting at the time of the incident out of which the suit arose under circumstances in which Congress has provided by statute that the remedy provided by the Federal Tort Claims Act is made the exclusive remedy.

(c) A certification under this section may be withdrawn if a further evaluation of the relevant facts or the consideration of new or additional evidence calls for such action. The making, withholding, or withdrawing of certifications, and the removal and defense of, or refusal to remove or defend, such civil actions or proceedings shall be subject to the instructions and supervision of the Assistant Attorney Gen-

## 28 CFR Ch. I (7-1-24 Edition)

eral in charge of the Civil Division or his or her designee.

## PART 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

### Subpart A—Procedures for Disclosure of Records Under the Freedom of Information Act

Sec.

- 16.1 General provisions.
- 16.2 Proactive disclosure of Department records.
- 16.3 Requirements for making requests.
- 16.4 Responsibility for responding to requests.
- 16.5 Timing of responses to requests.
- 16.6 Responses to requests.
- 16.7 Confidential commercial information.
- 16.8 Administrative appeals.
- 16.9 Preservation of records.
- 16.10 Fees.
- 16.11 Other rights and services.

### Subpart B—Production or Disclosure in Federal and State Proceedings

- 16.21 Purpose and scope.
- 16.22 General prohibition of production or disclosure in Federal and State proceedings in which the United States is not a party.
- 16.23 General disclosure authority in Federal and State proceedings in which the United States is a party.
- 16.24 Procedure in the event of a demand where disclosure is not otherwise authorized.
- 16.25 Final action by the Deputy or Associate Attorney General.
- 16.26 Considerations in determining whether production or disclosure should be made pursuant to a demand.
- 16.27 Procedure in the event a department decision concerning a demand is not made prior to the time a response to the demand is required.
- 16.28 Procedure in the event of an adverse ruling.
- 16.29 Delegation by Assistant Attorneys General.

APPENDIX TO SUBPART B OF PART 16—RE-DELEGATION OF AUTHORITY TO THE DEPUTY ASSISTANT ATTORNEY GENERAL FOR LITIGATION, ANTITRUST DIVISION, TO AUTHORIZE PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

### Subpart C—Production of FBI Identification Records in Response to Written Requests by Subjects Thereof

- 16.30 Purpose and scope.

- 16.31 Definition of identification record.
- 16.32 Procedure to obtain an identification record.
- 16.33 Fee for production of identification record.
- 16.34 Procedure to obtain change, correction or updating of identification records.

**Subpart D—Access to and Amendment of Individual Records Pursuant to the Privacy Act of 1974, and Other Privacy Protections**

- 16.40 General provisions.
- 16.41 Privacy Act requests for access to records.
- 16.42 Responsibility for responding to Privacy Act requests for access to records.
- 16.43 Responses to Privacy Act requests for access to records.
- 16.44 Classified information.
- 16.45 Privacy Act access appeals.
- 16.46 Privacy Act requests for amendment or correction.
- 16.47 Privacy Act requests for an accounting of record disclosures.
- 16.48 Preservation of records.
- 16.49 Fees.
- 16.50 Notice of compulsory legal process and emergency disclosures.
- 16.51 Security of systems of records.
- 16.52 Contracts for the operation of record systems.
- 16.53 Use and collection of Social Security account numbers.
- 16.54 Employee standards of conduct.
- 16.55 Other rights and services.

**Subpart E—Exemption of Records Systems Under the Privacy Act**

- 16.70 Exemption of the Office of the Attorney General System—limited access.
- 16.71 Exemption of the Office of the Deputy Attorney General System—limited access.
- 16.72 Exemption of Office of the Associate Attorney General System—limited access.
- 16.73 Exemption of Office of Legal Policy Systems.
- 16.74 Exemption of National Security Division Systems—limited access.
- 16.75 Exemption of the Office of the Inspector General Systems/Limited Access.
- 16.76 Exemption of Justice Management Division.
- 16.77 Exemption of U.S. Trustee Program System—limited access.
- 16.78 Exemption of the Special Counsel for Immigration-Related, Unfair Employment Practices Systems.
- 16.79 Exemption of Pardon Attorney System.
- 16.80 Exemption of Office of Professional Responsibility System—limited access.

- 16.81 Exemption of United States Attorneys Systems—limited access.
- 16.82 Exemption of the National Drug Intelligence Center Data Base—limited access.
- 16.83 Exemption of the Executive Office for Immigration Review System—limited access.
- 16.84 Exemption of Immigration Appeals System.
- 16.85 Exemption of U.S. Parole Commission—limited access.
- 16.88 Exemption of Antitrust Division Systems—limited access.
- 16.89 Exemption of Civil Division Systems—limited access.
- 16.90 Exemption of Civil Rights Division Systems.
- 16.91 Exemption of Criminal Division Systems—limited access, as indicated.
- 16.92 Exemption of Environment and Natural Resources Division Systems—limited access.
- 16.93 Exemption of Tax Division Systems—limited access.
- 16.96 Exemption of Federal Bureau of Investigation Systems—limited access.
- 16.97 Exemption of Bureau of Prisons Systems—limited access.
- 16.98 Exemption of the Drug Enforcement Administration (DEA) Systems—limited access.
- 16.99 Exemption of the Immigration and Naturalization Service Systems—limited access.
- 16.100 Exemption of Office of Justice Programs—limited access.
- 16.101 Exemption of U.S. Marshals Service Systems—limited access, as indicated.
- 16.102 Exemption of Drug Enforcement Administration and Immigration and Naturalization Service Joint System of Records.
- 16.103 Exemption of the INTERPOL-United States National Central Bureau (INTERPOL-USNCB) System.
- 16.104 Exemption of Office of Special Counsel—Waco System.
- 16.105 Exemption of Foreign Terrorist Tracking Task Force System.
- 16.106 Exemption of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—Limited Access.
- 16.130 Exemption of Department of Justice Systems: Correspondence Management Systems for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).
- 16.131 Exemption of Department of Justice (DOJ)/Nationwide Joint Automated Booking System (JABS), DOJ-005.

## § 16.1

## 28 CFR Ch. I (7-1-24 Edition)

- 16.132 Exemption of Department of Justice System—Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006.
- 16.133 Exemption of Department of Justice Regional Data Exchange System (RDEX), DOJ-012.
- 16.134 Exemption of Debt Collection Enforcement System, Justice/DOJ-016.
- 16.135 Exemptions of Executive Office for Organized Crime Drug Enforcement Task Forces Systems.
- 16.136 Exemptions of the Department of Justice, Giglio Information System, Justice/DOJ-017.
- 16.137 Exemption of the Department of Justice Insider Threat Program Records—limited access.
- 16.138 Exemption of the Department of Justice Information Technology, Information System, and Network Activity and Access Records, JUSTICE/DOJ-002.
- 16.139 Exemption of the Department of Justice Data Protection Review Court Records System, JUSTICE/OPCL-001.

### Subpart F—Public Observation of Parole Commission Meetings

- 16.200 Definitions.
- 16.201 Voting by the Commissioners without joint deliberation.
- 16.202 Open meetings.
- 16.203 Closed meetings—Formal procedure.
- 16.204 Public notice.
- 16.205 Closed meetings—Informal procedures.
- 16.206 Transcripts, minutes, and miscellaneous documents concerning Commission meetings.
- 16.207 Public access to nonexempt transcripts and minutes of closed Commission meetings—Documents used at meetings—Record retention.
- 16.208 Annual report.

### Subpart G—Access to Documents by Former Employees of the Department

- 16.300 Access to documents for the purpose of responding to an official inquiry.
- 16.301 Limitations.

APPENDIX I TO PART 16—COMPONENTS OF THE DEPARTMENT OF JUSTICE

AUTHORITY: 5 U.S.C. 301, 552, 552a, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717; 42 U.S.C. 405.

### Subpart A—Procedures for Disclosure of Records Under the Freedom of Information Act

SOURCE: AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, unless otherwise noted.

### § 16.1 General provisions.

(a) This subpart contains the rules that the Department of Justice follows in processing requests for records under the Freedom of Information Act (“FOIA”), 5 U.S.C. 552. The rules in this subpart should be read in conjunction with the text of the FOIA and the Uniform Freedom of Information Fee Schedule and Guidelines published by the Office of Management and Budget (“OMB Guidelines”). Additionally, the Department’s “FOIA Reference Guide” and its attachments contain information about the specific procedures particular to the Department with respect to making FOIA requests and descriptions of the types of records maintained by different Department components. This resource is available at [http://www.justice.gov/oip/04\\_3.html](http://www.justice.gov/oip/04_3.html). Requests made by individuals for records about themselves under the Privacy Act of 1974, 5 U.S.C. 552a, are processed under subpart D of part 16 as well as under this subpart.

(b) As referenced in this subpart, component means each separate bureau, office, division, commission, service, center, or administration that is designated by the Department as a primary organizational entity.

(c) The Department has a decentralized system for processing requests, with each component handling requests for its records.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 727, Jan. 4, 2017]

### § 16.2 Proactive disclosure of Department records.

Records that are required by the FOIA to be made available for public inspection in an electronic format may be accessed through the Department’s Web site at [http://justice.gov/oip/04\\_2.html](http://justice.gov/oip/04_2.html). Each component is responsible for determining which of its records are required to be made publicly available, as well as identifying additional records of interest to the public that are appropriate for public disclosure, and for posting and indexing such records. Each component shall ensure that its Web site of posted records and indices is reviewed and updated on an ongoing basis. Each component has a FOIA Public Liaison who

can assist individuals in locating records particular to a component. A list of the Department's FOIA Public Liaisons is available at <http://www.justice.gov/oip/foiacontact/index-list.html>.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 727, Jan. 4, 2017]

### § 16.3 Requirements for making requests.

(a) *General information.* (1) The Department has a decentralized system for responding to FOIA requests, with each component designating a FOIA office to process records from that component. All components have the capability to receive requests electronically either through email or a web portal. To make a request for records of the Department, a requester should write directly to the FOIA office of the component that maintains the records being sought. A request will receive the quickest possible response if it is addressed to the FOIA office of the component that maintains the records sought. The Department's FOIA Reference Guide, which may be accessed as described in § 16.1(a), contains descriptions of the functions of each component and provides other information that is helpful in determining where to make a request. Each component's FOIA office and any additional requirements for submitting a request to a given component are listed in Appendix I to this part. Part 0 of this chapter also summarizes the functions of each component. These references can all be used by requesters to determine where to send their requests within the Department.

(2) A requester may also send requests to the FOIA/PA Mail Referral Unit, Justice Management Division, Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001, or via email to [MRUFOIA.Requests@usdoj.gov](mailto:MRUFOIA.Requests@usdoj.gov), or via fax to (202) 616-6695. The Mail Referral Unit will forward the request to the component(s) that it determines to be most likely to maintain the records that are sought.

(3) A requester who is making a request for records about himself or herself must comply with the verification

of identity provision set forth in subpart D of this part.

(4) Where a request for records pertains to a third party, a requester may receive greater access by submitting either a notarized authorization signed by that individual or a declaration made in compliance with the requirements set forth in 28 U.S.C. 1746 by that individual authorizing disclosure of the records to the requester, or by submitting proof that the individual is deceased (e.g., a copy of a death certificate or an obituary). As an exercise of administrative discretion, each component can require a requester to supply additional information if necessary in order to verify that a particular individual has consented to disclosure.

(b) *Description of records sought.* Requesters must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. To the extent possible, requesters should include specific information that may assist a component in identifying the requested records, such as the date, title or name, author, recipient, subject matter of the record, case number, file designation, or reference number. Requesters should refer to Appendix I to this part for additional, component-specific requirements. In general, requesters should include as much detail as possible about the specific records or the types of records that they are seeking. Before submitting their requests, requesters may contact the component's FOIA contact or FOIA Public Liaison to discuss the records they are seeking and to receive assistance in describing the records. If after receiving a request a component determines that it does not reasonably describe the records sought, the component shall inform the requester what additional information is needed or why the request is otherwise insufficient. Requesters who are attempting to reformulate or modify such a request may discuss their request with the component's designated FOIA contact, its FOIA Public Liaison, or a representative of the Office of Information Policy ("OIP"), each of whom is available to assist the requester in reasonably describing the records sought. If a request does not reasonably describe the

## § 16.4

## 28 CFR Ch. I (7-1-24 Edition)

records sought, the agency's response to the request may be delayed.

### § 16.4 Responsibility for responding to requests.

(a) *In general.* Except in the instances described in paragraphs (c) and (d) of this section, the component that first receives a request for a record and maintains that record is the component responsible for responding to the request. In determining which records are responsive to a request, a component ordinarily will include only records in its possession as of the date that it begins its search. If any other date is used, the component shall inform the requester of that date. A record that is excluded from the requirements of the FOIA pursuant to 5 U.S.C. 552(c), is not considered responsive to a request.

(b) *Authority to grant or deny requests.* The head of a component, or designee, is authorized to grant or to deny any requests for records that are maintained by that component.

(c) *Re-routing of misdirected requests.* Where a component's FOIA office determines that a request was misdirected within the Department, the receiving component's FOIA office shall route the request to the FOIA office of the proper component(s).

(d) *Consultation, referral, and coordination.* When reviewing records located by a component in response to a request, the component shall determine whether another component or another agency of the Federal Government is better able to determine whether the record is exempt from disclosure under the FOIA. As to any such record, the component shall proceed in one of the following ways:

(1) *Consultation.* When records originated with the component processing the request, but contain within them information of interest to another component, agency, or other Federal Government office, the component processing the request should typically consult with that other component or agency prior to making a release determination.

(2) *Referral.* (i) When the component processing the request believes that a different component, agency, or other Federal Government office is best able

to determine whether to disclose the record, the component typically should refer the responsibility for responding to the request regarding that record, as long as the referral is to a component or agency that is subject to the FOIA. Ordinarily, the component or agency that originated the record will be presumed to be best able to make the disclosure determination. However, if the component processing the request and the originating component or agency jointly agree that the former is in the best position to respond regarding the record, then the record may be handled as a consultation.

(ii) Whenever a component refers any part of the responsibility for responding to a request to another component or agency, it shall document the referral, maintain a copy of the record that it refers, and notify the requester of the referral and inform the requester of the name(s) of the component or agency to which the record was referred, including that component's or agency's FOIA contact information.

(3) *Coordination.* The standard referral procedure is not appropriate where disclosure of the identity of the component or agency to which the referral would be made could harm an interest protected by an applicable exemption, such as the exemptions that protect personal privacy or national security interests. For example, if a non-law enforcement component responding to a request for records on a living third party locates within its files records originating with a law enforcement agency, and if the existence of that law enforcement interest in the third party was not publicly known, then to disclose that law enforcement interest could cause an unwarranted invasion of the personal privacy of the third party. Similarly, if a component locates within its files material originating with an Intelligence Community agency, and the involvement of that agency in the matter is classified and not publicly acknowledged, then to disclose or give attribution to the involvement of that Intelligence Community agency could cause national security harms. In such instances, in order to avoid harm to an interest protected by an applicable exemption, the component that received the request should coordinate with the

originating component or agency to seek its views on the disclosability of the record. The release determination for the record that is the subject of the coordination should then be conveyed to the requester by the component that originally received the request.

(e) *Classified information.* On receipt of any request involving classified information, the component shall determine whether the information is currently and properly classified and take appropriate action to ensure compliance with part 17 of this title. Whenever a request involves a record containing information that has been classified or may be appropriate for classification by another component or agency under any applicable executive order concerning the classification of records, the receiving component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, or that should consider the information for classification. Whenever a component's record contains information that has been derivatively classified (for example, when it contains information classified by another component or agency), the component shall refer the responsibility for responding to that portion of the request to the component or agency that classified the underlying information.

(f) *Timing of responses to consultations and referrals.* All consultations and referrals received by the Department will be handled according to the date that the FOIA request initially was received by the first component or agency.

(g) *Agreements regarding consultations and referrals.* Components may establish agreements with other components or agencies to eliminate the need for consultations or referrals with respect to particular types of records.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 727, Jan. 4, 2017]

#### § 16.5 Timing of responses to requests.

(a) *In general.* Components ordinarily will respond to requests according to their order of receipt. Appendix I to this part contains the list of the Department components that are designated to accept requests. In instances

involving misdirected requests that are re-routed pursuant to § 16.4(c), the response time will commence on the date that the request is received by the proper component's office that is designated to receive requests, but in any event not later than 10 working days after the request is first received by any component's office that is designated by these regulations to receive requests.

(b) *Multitrack processing.* All components must designate a specific track for requests that are granted expedited processing, in accordance with the standards set forth in paragraph (e) of this section. A component may also designate additional processing tracks that distinguish between simple and more complex requests based on the estimated amount of work or time needed to process the request. Among the factors a component may consider are the number of pages involved in processing the request and the need for consultations or referrals. Components shall advise requesters of the track into which their request falls and, when appropriate, shall offer the requesters an opportunity to narrow their request so that it can be placed in a different processing track.

(c) *Unusual circumstances.* Whenever the statutory time limit for processing a request cannot be met because of "unusual circumstances," as defined in the FOIA, and the component extends the time limit on that basis, the component shall, before expiration of the 20-day period to respond, notify the requester in writing of the unusual circumstances involved and of the date by which processing of the request can be expected to be completed. Where the extension exceeds 10 working days, the component shall, as described by the FOIA, provide the requester with an opportunity to modify the request or arrange an alternative time period for processing. The component shall make available its designated FOIA contact and its FOIA Public Liaison for this purpose. The component must also alert requesters to the availability of the Office of Government Information Services to provide dispute resolution services.

## § 16.6

## 28 CFR Ch. I (7-1-24 Edition)

(d) *Aggregating requests.* For the purposes of satisfying unusual circumstances under the FOIA, components may aggregate requests in cases where it reasonably appears that multiple requests, submitted either by a requester or by a group of requesters acting in concert, constitute a single request that would otherwise involve unusual circumstances. Components shall not aggregate multiple requests that involve unrelated matters.

(e) *Expedited processing.* (1) Requests and appeals shall be processed on an expedited basis whenever it is determined that they involve:

(i) Circumstances in which the lack of expedited processing could reasonably be expected to pose an imminent threat to the life or physical safety of an individual;

(ii) An urgency to inform the public about an actual or alleged Federal Government activity, if made by a person who is primarily engaged in disseminating information;

(iii) The loss of substantial due process rights; or

(iv) A matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity that affect public confidence.

(2) A request for expedited processing may be made at any time. Requests based on paragraphs (e)(1)(i), (ii), and (iii) of this section must be submitted to the component that maintains the records requested. When making a request for expedited processing of an administrative appeal, the request should be submitted to OIP. Requests for expedited processing that are based on paragraph (e)(1)(iv) of this section must be submitted to the Director of Public Affairs at the Office of Public Affairs, Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001. A component that receives a misdirected request for expedited processing under the standard set forth in paragraph (e)(1)(iv) of this section shall forward it immediately to the Office of Public Affairs for its determination. The time period for making the determination on the request for expedited processing under paragraph (e)(1)(iv) of this section shall commence on the date that the Office

of Public Affairs receives the request, provided that it is routed within 10 working days.

(3) A requester who seeks expedited processing must submit a statement, certified to be true and correct, explaining in detail the basis for making the request for expedited processing. For example, under paragraph (e)(1)(ii) of this section, a requester who is not a full-time member of the news media must establish that the requester is a person whose primary professional activity or occupation is information dissemination, though it need not be the requester's sole occupation. Such a requester also must establish a particular urgency to inform the public about the government activity involved in the request—one that extends beyond the public's right to know about government activity generally. The existence of numerous articles published on a given subject can be helpful in establishing the requirement that there be an "urgency to inform" the public on the topic. As a matter of administrative discretion, a component may waive the formal certification requirement.

(4) A component shall notify the requester within 10 calendar days of the receipt of a request for expedited processing of its decision whether to grant or deny expedited processing. If expedited processing is granted, the request shall be given priority, placed in the processing track for expedited requests, and shall be processed as soon as practicable. If a request for expedited processing is denied, any appeal of that decision shall be acted on expeditiously.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 727, Jan. 4, 2017]

### § 16.6 Responses to requests.

(a) *In general.* Components should, to the extent practicable, communicate with requesters having access to the Internet using electronic means, such as email or web portal.

(b) *Acknowledgments of requests.* A component shall acknowledge the request and assign it an individualized tracking number if it will take longer

than 10 working days to process. Components shall include in the acknowledgment a brief description of the records sought to allow requesters to more easily keep track of their requests.

(c) *Grants of requests.* Once a component makes a determination to grant a request in full or in part, it shall notify the requester in writing. The component also shall inform the requester of any fees charged under § 16.10 and shall disclose the requested records to the requester promptly upon payment of any applicable fees. The component must inform the requester of the availability of the FOIA Public Liaison to offer assistance.

(d) *Adverse determinations of requests.* A component making an adverse determination denying a request in any respect shall notify the requester of that determination in writing. Adverse determinations, or denials of requests, include decisions that: the requested record is exempt, in whole or in part; the request does not reasonably describe the records sought; the information requested is not a record subject to the FOIA; the requested record does not exist, cannot be located, or has been destroyed; or the requested record is not readily reproducible in the form or format sought by the requester. Adverse determinations also include denials involving fees or fee waiver matters or denials of requests for expedited processing.

(e) *Content of denial.* The denial shall be signed by the head of the component, or designee, and shall include:

(1) The name and title or position of the person responsible for the denial;

(2) A brief statement of the reasons for the denial, including any FOIA exemption applied by the component in denying the request;

(3) An estimate of the volume of any records or information withheld, such as the number of pages or some other reasonable form of estimation, although such an estimate is not required if the volume is otherwise indicated by deletions marked on records that are disclosed in part or if providing an estimate would harm an interest protected by an applicable exemption; and

(4) A statement that the denial may be appealed under § 16.8(a), and a description of the requirements set forth therein.

(5) A statement notifying the requester of the assistance available from the component's FOIA Public Liaison and the dispute resolution services offered by the Office of Government Information Services.

(f) *Markings on released documents.* Markings on released documents must be clearly visible to the requester. Records disclosed in part shall be marked to show the amount of information deleted and the exemption under which the deletion was made unless doing so would harm an interest protected by an applicable exemption. The location of the information deleted shall also be indicated on the record, if technically feasible.

(g) *Use of record exclusions.* (1) In the event that a component identifies records that may be subject to exclusion from the requirements of the FOIA pursuant to 5 U.S.C. 552(c), the component must confer with OIP to obtain approval to apply the exclusion.

(2) Any component invoking an exclusion shall maintain an administrative record of the process of invocation and approval of the exclusion by OIP.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 727, Jan. 4, 2017]

#### **§ 16.7 Confidential commercial information.**

(a) *Definitions.* (1) *Confidential commercial information* means commercial or financial information obtained by the Department from a submitter that may be protected from disclosure under Exemption 4 of the FOIA, 5 U.S.C. 552(b)(4).

(2) *Submitter* means any person or entity, including a corporation, State, or foreign government, but not including another Federal Government entity, that provides information, either directly or indirectly to the Federal Government.

(b) *Designation of confidential commercial information.* A submitter of confidential commercial information must use good faith efforts to designate by appropriate markings, either at the

## § 16.7

## 28 CFR Ch. I (7-1-24 Edition)

time of submission or within a reasonable time thereafter, any portion of its submission that it considers to be protected from disclosure under Exemption 4. These designations shall expire 10 years after the date of the submission unless the submitter requests and provides justification for a longer designation period.

(c) *When notice to submitters is required.* (1) A component shall promptly provide written notice to a submitter of confidential commercial information whenever records containing such information are requested under the FOIA if, after reviewing the request, the responsive records, and any appeal by the requester, the component determines that it may be required to disclose the records, provided:

(i) The requested information has been designated in good faith by the submitter as information considered protected from disclosure under Exemption 4; or

(ii) The component has a reason to believe that the requested information may be protected from disclosure under Exemption 4, but has not yet determined whether the information is protected from disclosure under that exemption or any other applicable exemption.

(2) The notice shall either describe the commercial information requested or include a copy of the requested records or portions of records containing the information. In cases involving a voluminous number of submitters, notice may be made by posting or publishing the notice in a place or manner reasonably likely to accomplish it.

(d) *Exceptions to submitter notice requirements.* The notice requirements of this section shall not apply if:

(1) The component determines that the information is exempt under the FOIA;

(2) The information has been lawfully published or has been officially made available to the public;

(3) Disclosure of the information is required by a statute other than the FOIA or by a regulation issued in accordance with the requirements of Executive Order 12600 of June 23, 1987; or

(4) The designation made by the submitter under paragraph (b) of this sec-

tion appears obviously frivolous, except that, in such a case, the component shall give the submitter written notice of any final decision to disclose the information and must provide that notice within a reasonable number of days prior to a specified disclosure date.

(e) *Opportunity to object to disclosure.* (1) A component shall specify a reasonable time period within which the submitter must respond to the notice referenced above. If a submitter has any objections to disclosure, it should provide the component a detailed written statement that specifies all grounds for withholding the particular information under any exemption of the FOIA. In order to rely on Exemption 4 as basis for nondisclosure, the submitter must explain why the information constitutes a trade secret or commercial or financial information that is privileged or confidential.

(2) A submitter who fails to respond within the time period specified in the notice shall be considered to have no objection to disclosure of the information. Information received by the component after the date of any disclosure decision shall not be considered by the component. Any information provided by a submitter under this subpart may itself be subject to disclosure under the FOIA.

(f) *Analysis of objections.* A component shall consider a submitter's objections and specific grounds for nondisclosure in deciding whether to disclose the requested information.

(g) *Notice of intent to disclose.* Whenever a component decides to disclose information over the objection of a submitter, the component shall provide the submitter written notice, which shall include:

(1) A statement of the reasons why each of the submitter's disclosure objections was not sustained;

(2) A description of the information to be disclosed; and

(3) A specified disclosure date, which shall be a reasonable time subsequent to the notice.

(h) *Notice of FOIA lawsuit.* Whenever a requester files a lawsuit seeking to compel the disclosure of confidential

## Department of Justice

## § 16.10

commercial information, the component shall promptly notify the submitter.

(i) *Requester notification.* The component shall notify a requester whenever it provides the submitter with notice and an opportunity to object to disclosure; whenever it notifies the submitter of its intent to disclose the requested information; and whenever a submitter files a lawsuit to prevent the disclosure of the information.

### § 16.8 Administrative appeals.

(a) *Requirements for making an appeal.* A requester may appeal any adverse determinations to OIP. The contact information for OIP is contained in the FOIA Reference Guide, which is available at [http://www.justice.gov/oip/04\\_3.html](http://www.justice.gov/oip/04_3.html). Appeals can be submitted through the web portal accessible on OIP's Web site. Examples of adverse determinations are provided in §16.6(d). The requester must make the appeal in writing and to be considered timely it must be postmarked, or in the case of electronic submissions, transmitted, within 90 calendar days after the date of the response. The appeal should clearly identify the component's determination that is being appealed and the assigned request number. To facilitate handling, the requester should mark both the appeal letter and envelope, or subject line of the electronic transmission, "Freedom of Information Act Appeal."

(b) *Adjudication of appeals.* (1) The Director of OIP or designee will act on behalf of the Attorney General on all appeals under this section.

(2) An appeal ordinarily will not be adjudicated if the request becomes a matter of FOIA litigation.

(3) On receipt of any appeal involving classified information, OIP shall take appropriate action to ensure compliance with part 17 of this title.

(c) *Decisions on appeals.* A decision on an appeal must be made in writing. A decision that upholds a component's determination will contain a statement that identifies the reasons for the affirmance, including any FOIA exemptions applied. The decision will provide the requester with notification of the statutory right to file a lawsuit and will inform the requester of the medi-

ation services offered by the Office of Government Information Services of the National Archives and Records Administration as a non-exclusive alternative to litigation. If a component's decision is remanded or modified on appeal, the requester will be notified of that determination in writing. The component will thereafter further process the request in accordance with that appeal determination and respond directly to the requester.

(d) *Engaging in dispute resolution services provided by OGIS.* Mediation is a voluntary process. If a component agrees to participate in the mediation services provided by the Office of Government Information Services, it will actively engage as a partner to the process in an attempt to resolve the dispute.

(e) *When appeal is required.* Before seeking review by a court of a component's adverse determination, a requester generally must first submit a timely administrative appeal.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 728, Jan. 4, 2017]

### § 16.9 Preservation of records.

Each component shall preserve all correspondence pertaining to the requests that it receives under this subpart, as well as copies of all requested records, until disposition or destruction is authorized pursuant to title 44 of the United States Code or the General Records Schedule 14 of the National Archives and Records Administration. Records shall not be disposed of or destroyed while they are the subject of a pending request, appeal, or lawsuit under the FOIA.

### § 16.10 Fees.

(a) *In general.* Components shall charge for processing requests under the FOIA in accordance with the provisions of this section and with the OMB Guidelines. In order to resolve any fee issues that arise under this section, a component may contact a requester for additional information. Components shall ensure that searches, review, and duplication are conducted in the most efficient and the least expensive manner. A component ordinarily will collect all applicable fees before sending

## § 16.10

## 28 CFR Ch. I (7-1-24 Edition)

copies of records to a requester. Requesters must pay fees by check or money order made payable to the Treasury of the United States.

(b) *Definitions.* For purposes of this section:

(1) *Commercial use request* is a request that asks for information for a use or a purpose that furthers a commercial, trade, or profit interest, which can include furthering those interests through litigation. A component's decision to place a requester in the commercial use category will be made on a case-by-case basis based on the requester's intended use of the information.

(2) *Direct costs* are those expenses that an agency incurs in searching for and duplicating (and, in the case of commercial use requests, reviewing) records in order to respond to a FOIA request. For example, direct costs include the salary of the employee performing the work (*i.e.*, the basic rate of pay for the employee, plus 16 percent of that rate to cover benefits) and the cost of operating computers and other electronic equipment, such as photocopiers and scanners. Direct costs do not include overhead expenses such as the costs of space, and of heating or lighting a facility.

(3) *Duplication* is reproducing a copy of a record, or of the information contained in it, necessary to respond to a FOIA request. Copies can take the form of paper, audiovisual materials, or electronic records, among others.

(4) *Educational institution* is any school that operates a program of scholarly research. A requester in this fee category must show that the request is made in connection with the requester's role at the educational institution. Components may seek assurance from the requester that the request is in furtherance of scholarly research and will advise requesters of their placement in this category.

*Example 1.* A request from a professor of geology at a university for records relating to soil erosion, written on letterhead of the Department of Geology, would be presumed to be from an educational institution.

*Example 2.* A request from the same professor of geology seeking drug information from the Food and Drug Administration in furtherance of a murder mystery he is writing would not be presumed to be an institu-

tional request, regardless of whether it was written on institutional stationery.

*Example 3.* A student who makes a request in furtherance of the student's coursework or other school-sponsored activities and provides a copy of a course syllabus or other reasonable documentation to indicate the research purpose for the request, would qualify as part of this fee category.

(5) *Noncommercial scientific institution* is an institution that is not operated on a "commercial" basis, as defined in paragraph (b)(1) of this section and that is operated solely for the purpose of conducting scientific research the results of which are not intended to promote any particular product or industry. A requester in this category must show that the request is authorized by and is made under the auspices of a qualifying institution and that the records are sought to further scientific research and are not for a commercial use.

(6) *Representative of the news media* is any person or entity that actively gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. The term "news" means information that is about current events or that would be of current interest to the public. Examples of news media entities include television or radio stations that broadcast "news" to the public at large and publishers of periodicals that disseminate "news" and make their products available through a variety of means to the general public, including news organizations that disseminate solely on the Internet. A request for records supporting the news-dissemination function of the requester shall not be considered to be for a commercial use. "Freelance" journalists who demonstrate a solid basis for expecting publication through a news media entity shall be considered as a representative of the news media. A publishing contract would provide the clearest evidence that publication is expected; however, components shall also consider a requester's past publication record in making this determination.

(7) *Review* is the examination of a record located in response to a request in order to determine whether any portion of it is exempt from disclosure.

Review time includes processing any record for disclosure, such as doing all that is necessary to prepare the record for disclosure, including the process of redacting the record and marking the appropriate exemptions. Review costs are properly charged even if a record ultimately is not disclosed. Review time also includes time spent both obtaining and considering any formal objection to disclosure made by a confidential commercial information submitter under §16.7, but it does not include time spent resolving general legal or policy issues regarding the application of exemptions.

(8) *Search* is the process of looking for and retrieving records or information responsive to a request. Search time includes page-by-page or line-by-line identification of information within records and the reasonable efforts expended to locate and retrieve information from electronic records.

(c) *Charging fees*. In responding to FOIA requests, components shall charge the following fees unless a waiver or reduction of fees has been granted under paragraph (k) of this section. Because the fee amounts provided below already account for the direct costs associated with a given fee type, components should not add any additional costs to charges calculated under this section.

(1) *Search*. (i) Requests made by educational institutions, noncommercial scientific institutions, or representatives of the news media are not subject to search fees. Search fees shall be charged for all other requesters, subject to the restrictions of paragraph (d) of this section. Components may properly charge for time spent searching even if they do not locate any responsive records or if they determine that the records are entirely exempt from disclosure.

(ii) For each quarter hour spent by personnel searching for requested records, including electronic searches that do not require new programming, the fees shall be as follows: professional—\$10.00; and clerical/administrative—\$4.75.

(iii) Requesters shall be charged the direct costs associated with conducting any search that requires the creation of a new computer program to locate

the requested records. Requesters shall be notified of the costs associated with creating such a program and must agree to pay the associated costs before the costs may be incurred.

(iv) For requests that require the retrieval of records stored by an agency at a Federal records center operated by the National Archives and Records Administration (NARA), additional costs shall be charged in accordance with the Transactional Billing Rate Schedule established by NARA.

(2) *Duplication*. Duplication fees shall be charged to all requesters, subject to the restrictions of paragraph (d) of this section. A component shall honor a requester's preference for receiving a record in a particular form or format where it is readily reproducible by the component in the form or format requested. Where photocopies are supplied, the component shall provide one copy per request at a cost of five cents per page. For copies of records produced on tapes, disks, or other media, components shall charge the direct costs of producing the copy, including operator time. Where paper documents must be scanned in order to comply with a requester's preference to receive the records in an electronic format, the requester shall pay the direct costs associated with scanning those materials. For other forms of duplication, components shall charge the direct costs.

(3) *Review*. Review fees shall be charged to requesters who make commercial use requests. Review fees shall be assessed in connection with the initial review of the record, *i.e.*, the review conducted by a component to determine whether an exemption applies to a particular record or portion of a record. No charge will be made for review at the administrative appeal stage of exemptions applied at the initial review stage. However, if a particular exemption is deemed to no longer apply, any costs associated with a component's re-review of the records in order to consider the use of other exemptions may be assessed as review fees. Review fees shall be charged at the same rates as those charged for a search under paragraph (c)(1)(ii) of this section.

(d) *Restrictions on charging fees*. (1) No search fees will be charged for requests

## § 16.10

## 28 CFR Ch. I (7-1-24 Edition)

by educational institutions (unless the records are sought for a commercial use), noncommercial scientific institutions, or representatives of the news media.

(2) If a component fails to comply with the FOIA's time limits in which to respond to a request, it may not charge search fees, or, in the instances of requests from requesters described in paragraph (d)(1) of this section, may not charge duplication fees, except as described in paragraphs (d)(2)(i) through (iii) of this section.

(i) If a component has determined that unusual circumstances as defined by the FOIA apply and the agency provided timely written notice to the requester in accordance with the FOIA, a failure to comply with the time limit shall be excused for an additional 10 days.

(ii) If a component has determined that unusual circumstances as defined by the FOIA apply, and more than 5,000 pages are necessary to respond to the request, the component may charge search fees, or, in the case of requesters described in paragraph (d)(1) of this section, may charge duplication fees if the following steps are taken. The component must have provided timely written notice of unusual circumstances to the requester in accordance with the FOIA and the component must have discussed with the requester via written mail, email, or telephone (or made not less than three good-faith attempts to do so) how the requester could effectively limit the scope of the request in accordance with 5 U.S.C. 552(a)(6)(B)(ii). If this exception is satisfied, the component may charge all applicable fees incurred in the processing of the request.

(iii) If a court has determined that exceptional circumstances exist as defined by the FOIA, a failure to comply with the time limits shall be excused for the length of time provided by the court order.

(3) No search or review fees will be charged for a quarter-hour period unless more than half of that period is required for search or review.

(4) Except for requesters seeking records for a commercial use, components shall provide without charge:

(i) The first 100 pages of duplication (or the cost equivalent for other media); and

(ii) The first two hours of search.

(5) When, after first deducting the 100 free pages (or its cost equivalent) and the first two hours of search, a total fee calculated under paragraph (c) of this section is \$25.00 or less for any request, no fee will be charged.

(e) *Notice of anticipated fees in excess of \$25.00.* (1) When a component determines or estimates that the fees to be assessed in accordance with this section will exceed \$25.00, the component shall notify the requester of the actual or estimated amount of the fees, including a breakdown of the fees for search, review or duplication, unless the requester has indicated a willingness to pay fees as high as those anticipated. If only a portion of the fee can be estimated readily, the component shall advise the requester accordingly. If the requester is a noncommercial use requester, the notice shall specify that the requester is entitled to the statutory entitlements of 100 pages of duplication at no charge and, if the requester is charged search fees, two hours of search time at no charge, and shall advise the requester whether those entitlements have been provided.

(2) In cases in which a requester has been notified that the actual or estimated fees are in excess of \$25.00, the request shall not be considered received and further work will not be completed until the requester commits in writing to pay the actual or estimated total fee, or designates some amount of fees the requester is willing to pay, or in the case of a noncommercial use requester who has not yet been provided with the requester's statutory entitlements, designates that the requester seeks only that which can be provided by the statutory entitlements. The requester must provide the commitment or designation in writing, and must, when applicable, designate an exact dollar amount the requester is willing to pay. Components are not required to accept payments in installments.

(3) If the requester has indicated a willingness to pay some designated amount of fees, but the component estimates that the total fee will exceed

that amount, the component shall toll the processing of the request when it notifies the requester of the estimated fees in excess of the amount the requester has indicated a willingness to pay. The component shall inquire whether the requester wishes to revise the amount of fees the requester is willing to pay or modify the request. Once the requester responds, the time to respond will resume from where it was at the date of the notification.

(4) Components shall make available their FOIA Public Liaison or other FOIA professional to assist any requester in reformulating a request to meet the requester's needs at a lower cost.

(f) *Charges for other services.* Although not required to provide special services, if a component chooses to do so as a matter of administrative discretion, the direct costs of providing the service shall be charged. Examples of such services include certifying that records are true copies, providing multiple copies of the same document, or sending records by means other than first class mail.

(g) *Charging interest.* Components may charge interest on any unpaid bill starting on the 31st day following the date of billing the requester. Interest charges shall be assessed at the rate provided in 31 U.S.C. 3717 and will accrue from the billing date until payment is received by the component. Components shall follow the provisions of the Debt Collection Act of 1982 (Pub. L. 97-365, 96 Stat. 1749), as amended, and its administrative procedures, including the use of consumer reporting agencies, collection agencies, and offset.

(h) *Aggregating requests.* When a component reasonably believes that a requester or a group of requesters acting in concert is attempting to divide a single request into a series of requests for the purpose of avoiding fees, the component may aggregate those requests and charge accordingly. Components may presume that multiple requests of this type made within a 30-day period have been made in order to avoid fees. For requests separated by a longer period, components will aggregate them only where there is a reasonable basis for determining that aggre-

gation is warranted in view of all the circumstances involved. Multiple requests involving unrelated matters shall not be aggregated.

(i) *Advance payments.* (1) For requests other than those described in paragraphs (i)(2) or (i)(3) of this section, a component shall not require the requester to make an advance payment before work is commenced or continued on a request. Payment owed for work already completed (*i.e.*, payment before copies are sent to a requester) is not an advance payment.

(2) When a component determines or estimates that a total fee to be charged under this section will exceed \$250.00, it may require that the requester make an advance payment up to the amount of the entire anticipated fee before beginning to process the request. A component may elect to process the request prior to collecting fees when it receives a satisfactory assurance of full payment from a requester with a history of prompt payment.

(3) Where a requester has previously failed to pay a properly charged FOIA fee to any component or agency within 30 calendar days of the billing date, a component may require that the requester pay the full amount due, plus any applicable interest on that prior request, and the component may require that the requester make an advance payment of the full amount of any anticipated fee before the component begins to process a new request or continues to process a pending request or any pending appeal. Where a component has a reasonable basis to believe that a requester has misrepresented the requester's identity in order to avoid paying outstanding fees, it may require that the requester provide proof of identity.

(4) In cases in which a component requires advance payment, the request shall not be considered received and further work will not be completed until the required payment is received. If the requester does not pay the advance payment within 30 calendar days after the date of the component's fee determination, the request will be closed.

(j) *Other statutes specifically providing for fees.* The fee schedule of this section does not apply to fees charged under

## § 16.10

## 28 CFR Ch. I (7-1-24 Edition)

any statute that specifically requires an agency to set and collect fees for particular types of records. In instances where records responsive to a request are subject to a statutorily-based fee schedule program, the component shall inform the requester of the contact information for that program.

(k) *Requirements for waiver or reduction of fees.* (1) Requesters may seek a waiver of fees by submitting a written application demonstrating how disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(2) A component must furnish records responsive to a request without charge or at a reduced rate when it determines, based on all available information, that disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester. In deciding whether this standard is satisfied the component must consider the factors described in paragraphs (k)(2)(i) through (iii) of this section:

(i) Disclosure of the requested information would shed light on the operations or activities of the government. The subject of the request must concern identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated.

(ii) Disclosure of the requested information would be likely to contribute significantly to public understanding of those operations or activities. This factor is satisfied when the following criteria are met:

(A) Disclosure of the requested records must be meaningfully informative about government operations or activities. The disclosure of information that already is in the public domain, in either the same or a substantially identical form, would not be meaningfully informative if nothing new would be added to the public's understanding.

(B) The disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester. A requester's expertise in the subject area as well as the requester's ability and intention to effectively convey information to the public must be considered. Components will presume that a representative of the news media will satisfy this consideration.

(iii) The disclosure must not be primarily in the commercial interest of the requester. To determine whether disclosure of the requested information is primarily in the commercial interest of the requester, components will consider the following criteria:

(A) Components must identify whether the requester has any commercial interest that would be furthered by the requested disclosure. A commercial interest includes any commercial, trade, or profit interest. Requesters must be given an opportunity to provide explanatory information regarding this consideration.

(B) If there is an identified commercial interest, the component must determine whether that is the primary interest furthered by the request. A waiver or reduction of fees is justified when the requirements of paragraphs (k)(2)(i) and (ii) of this section are satisfied and any commercial interest is not the primary interest furthered by the request. Components ordinarily will presume that when a news media requester has satisfied the requirements of paragraphs (k)(2)(i) and (ii) of this section, the request is not primarily in the commercial interest of the requester. Disclosure to data brokers or others who merely compile and market government information for direct economic return will not be presumed to primarily serve the public interest.

(3) Where only some of the records to be released satisfy the requirements for a waiver of fees, a waiver shall be granted for those records.

(4) Requests for a waiver or reduction of fees should be made when the request is first submitted to the component and should address the criteria referenced above. A requester may submit a fee waiver request at a later time

**Department of Justice****§ 16.22**

so long as the underlying record request is pending or on administrative appeal. When a requester who has committed to pay fees subsequently asks for a waiver of those fees and that waiver is denied, the requester shall be required to pay any costs incurred up to the date the fee waiver request was received.

[AG Order No. 3517-2015, 80 FR 18106, Apr. 3, 2015, as amended by AG Order 3803-2016, 82 FR 728, Jan. 4, 2017]

**§ 16.11 Other rights and services.**

Nothing in this subpart shall be construed to entitle any person, as of right, to any service or to the disclosure of any record to which such person is not entitled under the FOIA.

**Subpart B—Production or Disclosure in Federal and State Proceedings**

SOURCE: Order No. 919-80, 45 FR 83210, Dec. 18, 1980, unless otherwise noted.

**§ 16.21 Purpose and scope.**

(a) This subpart sets forth procedures to be followed with respect to the production or disclosure of any material contained in the files of the Department, any information relating to material contained in the files of the Department, or any information acquired by any person while such person was an employee of the Department as a part of the performance of that person's official duties or because of that person's official status:

(1) In all federal and state proceedings in which the United States is a party; and

(2) In all federal and state proceedings in which the United States is not a party, including any proceedings in which the Department is representing a government employee solely in that employee's individual capacity, when a subpoena, order, or other demand (hereinafter collectively referred to as a "demand") of a court or other authority is issued for such material or information.

(b) For purposes of this subpart, the term *employee of the Department* includes all officers and employees of the United States appointed by, or subject

to the supervision, jurisdiction, or control of the Attorney General of the United States, including U.S. Attorneys, U.S. Marshals, U.S. Trustees and members of the staffs of those officials.

(c) Nothing in this subpart is intended to impede the appropriate disclosure, in the absence of a demand, of information by Department law enforcement agencies to federal, state, local and foreign law enforcement, prosecutive, or regulatory agencies.

(d) This subpart is intended only to provide guidance for the internal operations of the Department of Justice, and is not intended to, and does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States.

**§ 16.22 General prohibition of production or disclosure in Federal and State proceedings in which the United States is not a party.**

(a) In any federal or state case or matter in which the United States is not a party, no employee or former employee of the Department of Justice shall, in response to a demand, produce any material contained in the files of the Department, or disclose any information relating to or based upon material contained in the files of the Department, or disclose any information or produce any material acquired as part of the performance of that person's official duties or because of that person's official status without prior approval of the proper Department official in accordance with §§ 16.24 and 16.25 of this part.

(b) Whenever a demand is made upon an employee or former employee as described in paragraph (a) of this section, the employee shall immediately notify the U.S. Attorney for the district where the issuing authority is located. The responsible United States Attorney shall follow procedures set forth in § 16.24 of this part.

(c) If oral testimony is sought by a demand in any case or matter in which the United States is not a party, an affidavit, or, if that is not feasible, a statement by the party seeking the testimony or by his attorney, setting forth a summary of the testimony

## § 16.23

sought and its relevance to the proceeding, must be furnished to the responsible U.S. Attorney. Any authorization for testimony by a present or former employee of the Department shall be limited to the scope of the demand as summarized in such statement.

(d) When information other than oral testimony is sought by a demand, the responsible U.S. Attorney shall request a summary of the information sought and its relevance to the proceeding.

### § 16.23 General disclosure authority in Federal and State proceedings in which the United States is a party.

(a) Every attorney in the Department of Justice in charge of any case or matter in which the United States is a party is authorized, after consultation with the "originating component" as defined in § 16.24(a) of this part, to reveal and furnish to any person, including an actual or prospective witness, a grand jury, counsel, or a court, either during or preparatory to a proceeding, such testimony, and relevant unclassified material, documents, or information secured by any attorney, or investigator of the Department of Justice, as such attorney shall deem necessary or desirable to the discharge of the attorney's official duties: *Provided*, Such an attorney shall consider, with respect to any disclosure, the factors set forth in § 16.26(a) of this part: *And further provided*, An attorney shall not reveal or furnish any material, documents, testimony or information when, in the attorney's judgment, any of the factors specified in § 16.26(b) exists, without the express prior approval by the Assistant Attorney General in charge of the division responsible for the case or proceeding, the Director of the Executive Office for United States Trustees (hereinafter referred to as "the EOUST"), or such persons' designees.

(b) An attorney may seek higher level review at any stage of a proceeding, including prior to the issuance of a court order, when the attorney determines that a factor specified in § 16.26(b) exists or foresees that higher level approval will be required before disclosure of the information or testimony in question. Upon referral of a

## 28 CFR Ch. I (7-1-24 Edition)

matter under this subsection, the responsible Assistant Attorney General, the Director of EOUST, or their designees shall follow procedures set forth in § 16.24 of this part.

(c) If oral testimony is sought by a demand in a case or matter in which the United States is a party, an affidavit, or, if that is not feasible, a statement by the party seeking the testimony or by the party's attorney setting forth a summary of the testimony sought must be furnished to the Department attorney handling the case or matter.

### § 16.24 Procedure in the event of a demand where disclosure is not otherwise authorized.

(a) Whenever a matter is referred under § 16.22 of this part to a U.S. Attorney or, under § 16.23 of this part, to an Assistant Attorney General, the Director of the EOUST, or their designees (hereinafter collectively referred to as the "responsible official"), the responsible official shall immediately advise the official in charge of the bureau, division, office, or agency of the Department that was responsible for the collection, assembly, or other preparation of the material demanded or that, at the time the person whose testimony was demanded acquired the information in question, employed such person (hereinafter collectively referred to as the "originating component"), or that official's designee. In any instance in which the responsible official is also the official in charge of the originating component, the responsible official may perform all functions and make all determinations that this regulation vests in the originating component.

(b) The responsible official, subject to the terms of paragraph (c) of this section, may authorize the appearance and testimony of a present or former Department employee, or the production of material from Department files if:

(1) There is no objection after inquiry of the originating component;

(2) The demanded disclosure, in the judgment of the responsible official, is appropriate under the factors specified in § 16.26(a) of this part; and

**Department of Justice****§ 16.24**

(3) None of the factors specified in § 16.26(b) of this part exists with respect to the demanded disclosure.

(c) It is Department policy that the responsible official shall, following any necessary consultation with the originating component, authorize testimony by a present or former employee of the Department or the production of material from Department files without further authorization from Department officials whenever possible: *Provided*, That, when information is collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of the Department or by the EOUST, the Assistant Attorney General in charge of such a division or the Director of the EOUST may require that the originating component obtain the division's or the EOUST's approval before authorizing a responsible official to disclose such information. Prior to authorizing such testimony or production, however, the responsible official shall, through negotiation and, if necessary, appropriate motions, seek to limit the demand to information, the disclosure of which would not be inconsistent with the considerations specified in § 16.26 of this part.

(d)(1) In a case in which the United States is not a party, if the responsible U.S. attorney and the originating component disagree with respect to the appropriateness of demanded testimony or of a particular disclosure, or if they agree that such testimony or such a disclosure should not be made, they shall determine if the demand involves information that was collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of this Department or the EOUST. If so, the U.S. attorney shall notify the Director of the EOUST or the Assistant Attorney General in charge of the division responsible for such litigation or investigation, who may:

(i) Authorize personally or through a Deputy Assistant Attorney General, the demanded testimony or other disclosure of the information if such testimony or other disclosure, in the Assistant or Deputy Assistant Attorney General's judgment or in the judgment of the Director of the EOUST, is con-

sistent with the factors specified in § 16.26(a) of this part, and none of the factors specified in § 16.26(b) of this part exists with respect to the demanded disclosure;

(ii) Authorize, personally or by a designee, the responsible official, through negotiations and, if necessary, appropriate motions, to seek to limit the demand to matters, the disclosure of which, through testimony or documents, considerations specified in § 16.26 of this part, and otherwise to take all appropriate steps to limit the scope or obtain the withdrawal of a demand; or

(iii) If, after all appropriate steps have been taken to limit the scope or obtain the withdrawal of a demand, the Director of the EOUST or the Assistant or Deputy Assistant Attorney General does not authorize the demanded testimony or other disclosure, refer the matter, personally or through a Deputy Assistant Attorney General, for final resolution to the Deputy or Associate Attorney General, as indicated in § 16.25 of this part.

(2) If the demand for testimony or other disclosure in such a case does not involve information that was collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of this Department, the originating component shall decide whether disclosure is appropriate, except that, when especially significant issues are raised, the responsible official may refer the matter to the Deputy or Associate Attorney General, as indicated in § 16.25 of this part. If the originating component determines that disclosure would not be appropriate and the responsible official does not refer the matter for higher level review, the responsible official shall take all appropriate steps to limit the scope or obtain the withdrawal of a demand.

(e) In a case in which the United States is a party, the Assistant General or the Director of the EOUST responsible for the case or matter, or such persons' designees, are authorized, after consultation with the originating component, to exercise the authorities specified in paragraph (d)(1) (i) through (iii) of this section: *Provided*, That if a demand involves information that was

**§ 16.25****28 CFR Ch. I (7-1-24 Edition)**

collected, assembled, or prepared originally in connection with litigation or an investigation supervised by another unit of the Department, the responsible official shall notify the other division or the EOUST concerning the demand and the anticipated response. If two litigating units of the Department are unable to resolve a disagreement concerning disclosure, the Assistant Attorneys General in charge of the two divisions in disagreement, or the Director of the EOUST and the appropriate Assistant Attorney General, may refer the matter to the Deputy or Associate Attorney General, as indicated in § 16.25(b) of this part.

(f) In any case or matter in which the responsible official and the originating component agree that it would not be appropriate to authorize testimony or otherwise to disclose the information demanded, even if a court were so to require, no Department attorney responding to the demand should make any representation that implies that the Department would, in fact, comply with the demand if directed to do so by a court. After taking all appropriate steps in such cases to limit the scope or obtain the withdrawal of a demand, the responsible official shall refer the matter to the Deputy or Associate Attorney General, as indicated in § 16.25 of this part.

(g) In any case or matter in which the Attorney General is personally involved in the claim of privilege, the responsible official may consult with the Attorney General and proceed in accord with the Attorney General's instructions without subsequent review by the Deputy or Associate Attorney General.

**§ 16.25 Final action by the Deputy or Associate Attorney General.**

(a) Unless otherwise indicated, all matters to be referred under § 16.24 by an Assistant Attorney General, the Director of the EOUST, or such person's designees to the Deputy or Associate Attorney General shall be referred (1) to the Deputy Attorney General, if the matter is referred personally by or through the designee of an Assistant Attorney General who is within the general supervision of the Deputy At-

torney General, or (2) to the Associate Attorney General, in all other cases.

(b) All other matters to be referred under § 16.24 to the Deputy or Associate Attorney General shall be referred (1) to the Deputy Attorney General, if the originating component is within the supervision of the Deputy Attorney General or is an independent agency that, for administrative purposes, is within the Department of Justice, or (2) to the Associate Attorney General, if the originating component is within the supervision of the Associate Attorney General.

(c) Upon referral, the Deputy or Associate Attorney General shall make the final decision and give notice thereof to the responsible official and such other persons as circumstances may warrant.

**§ 16.26 Considerations in determining whether production or disclosure should be made pursuant to a demand.**

(a) In deciding whether to make disclosures pursuant to a demand, Department officials and attorneys should consider:

(1) Whether such disclosure is appropriate under the rules of procedure governing the case or matter in which the demand arose, and

(2) Whether disclosure is appropriate under the relevant substantive law concerning privilege.

(b) Among the demands in response to which disclosure will not be made by any Department official are those demands with respect to which any of the following factors exist:

(1) Disclosure would violate a statute, such as the income tax laws, 26 U.S.C. 6103 and 7213, or a rule of procedure, such as the grand jury secrecy rule, F.R.Cr.P., Rule 6(e),

(2) Disclosure would violate a specific regulation;

(3) Disclosure would reveal classified information, unless appropriately declassified by the originating agency,

(4) Disclosure would reveal a confidential source or informant, unless the investigative agency and the source or informant have no objection,

(5) Disclosure would reveal investigatory records compiled for law enforcement purposes, and would interfere

**Department of Justice****Pt. 16, Subpt. B, App.**

with enforcement proceedings or disclose investigative techniques and procedures the effectiveness of which would thereby be impaired,

(6) Disclosure would improperly reveal trade secrets without the owner's consent.

(c) In all cases not involving considerations specified in paragraphs (b)(1) through (b)(6) of this section, the Deputy or Associate Attorney General will authorize disclosure unless, in that person's judgment, after considering paragraph (a) of this section, disclosure is unwarranted. The Deputy or Associate Attorney General will not approve disclosure if the circumstances specified in paragraphs (b)(1) through (b)(3) of this section exist. The Deputy or Associate Attorney General will not approve disclosure if any of the conditions in paragraphs (b)(4) through (b)(6) of this section exist, unless the Deputy or Associate Attorney General determines that the administration of justice requires disclosure. In this regard, if disclosure is necessary to pursue a civil or criminal prosecution or affirmative relief, such as an injunction, consideration shall be given to:

(1) The seriousness of the violation or crime involved,

(2) The past history or criminal record of the violator or accused,

(3) The importance of the relief sought,

(4) The importance of the legal issues presented,

(5) Other matters brought to the attention of the Deputy or Associate Attorney General.

(d) Assistant Attorneys General, U.S. Attorneys, the Director of the EOUST, U.S. Trustees, and their designees, are authorized to issue instructions to attorneys and to adopt supervisory practices, consistent with this subpart, in order to help foster consistent application of the foregoing standards and the requirements of this subpart.

**§ 16.27 Procedure in the event a department decision concerning a demand is not made prior to the time a response to the demand is required.**

If response to a demand is required before the instructions from the appropriate Department official are received, the responsible official or other

Department attorney designated for the purpose shall appear and furnish the court or other authority with a copy of the regulations contained in this subpart and inform the court or other authority that the demand has been or is being, as the case may be, referred for the prompt consideration of the appropriate Department official and shall respectfully request the court or authority to stay the demand pending receipt of the requested instructions.

**§ 16.28 Procedure in the event of an adverse ruling.**

If the court or other authority declines to stay the effect of the demand in response to a request made in accordance with § 16.27 of this chapter pending receipt of instructions, or if the court or other authority rules that the demand must be complied with irrespective of instructions rendered in accordance with §§ 16.24 and 16.25 of this part not to produce the material or disclose the information sought, the employee or former employee upon whom the demand has been made shall, if so directed by the responsible Department official, respectfully decline to comply with the demand. See *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951).

**§ 16.29 Delegation by Assistant Attorneys General.**

With respect to any function that this subpart permits the designee of an Assistant Attorney General to perform, the Assistant Attorneys General are authorized to delegate their authority, in any case or matter or any category of cases or matters, to subordinate division officials or U.S. attorneys, as appropriate.

**APPENDIX TO SUBPART B OF PART 16—  
REDELEGATION OF AUTHORITY TO  
THE DEPUTY ASSISTANT ATTORNEY  
GENERAL FOR LITIGATION, ANTI-  
TRUST DIVISION, TO AUTHORIZE PRO-  
DUCTION OR DISCLOSURE OF MATE-  
RIAL OR INFORMATION**

1. By virtue of the authority vested in me by 28 CFR 16.23(b)(1) the authority delegated to me by that section to authorize the production of material and disclosure of information described in 28 CFR 16.21(a) is hereby

## § 16.30

redelegated to the Deputy Assistant Attorney General for Litigation, Antitrust Division.

2. This directive shall become effective on the date of its publication in the **FEDERAL REGISTER**.

[Order No. 960-81, 46 FR 52356, Oct. 27, 1981]

### **Subpart C—Production of FBI Identification Records in Response to Written Requests by Subjects Thereof**

SOURCE: Order No. 556-73, 38 FR 32806, Nov. 28, 1973, unless otherwise noted.

#### **§ 16.30 Purpose and scope.**

This subpart contains the regulations of the Federal Bureau of Investigation (FBI) concerning procedures to be followed when the subject of an identification record requests production of that record to review it or to obtain a change, correction, or updating of that record.

[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

#### **§ 16.31 Definition of identification record.**

An FBI identification record, often referred to as a "rap sheet," is a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, includes information taken from fingerprints submitted in connection with federal employment, naturalization, or military service. The identification record includes the name of the agency or institution that submitted the fingerprints to the FBI. If the fingerprints concern a criminal offense, the identification record includes the date of arrest or the date the individual was received by the agency submitting the fingerprints, the arrest charge, and the disposition of the arrest if known to the FBI. All arrest data included in an identification record are obtained from fingerprint submissions, disposition reports, and other reports submitted by agencies having criminal justice responsibilities. Therefore, the FBI Criminal Justice Information Services Division is not the source of the arrest data reflected on an identification record.

[Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

## **28 CFR Ch. I (7-1-24 Edition)**

#### **§ 16.32 Procedure to obtain an identification record.**

The subject of an identification record may obtain a copy thereof by submitting a written request via the U.S. mails directly to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. Such request must be accompanied by satisfactory proof of identity, which shall consist of name, date and place of birth and a set of rolled-inked fingerprint impressions placed upon fingerprint cards or forms commonly utilized for applicant or law enforcement purposes by law enforcement agencies.

[Order No. 1134-86, 51 FR 16677, May 6, 1986, as amended by Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

#### **§ 16.33 Fee for production of identification record.**

Each written request for production of an identification record must be accompanied by a fee of \$18 in the form of a certified check or money order, payable to the Treasury of the United States. This fee is established pursuant to the provisions of 31 U.S.C. 9701 and is based upon the clerical time beyond the first quarter hour to be spent in searching for, identifying, and reproducing each identification record requested as specified in § 16.10. Any request for waiver of the fee shall accompany the original request for the identification record and shall include a claim and proof of indigency. Subject to applicable laws, regulations, and directions of the Attorney General of the United States, the Director of the FBI may from time to time determine and establish a revised fee amount to be assessed under this authority. Notice relating to revised fee amounts shall be published in the **FEDERAL REGISTER**.

[Order No. 1943-94, 60 FR 38, Jan. 3, 1995, as amended by Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

#### **§ 16.34 Procedure to obtain change, correction or updating of identification records.**

If, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete

in any respect and wishes changes, corrections or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which contributed the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency.

[Order No. 1134-86, 51 FR 16677, May 6, 1986, as amended by Order No. 2258-99, 64 FR 52226, Sept. 28, 1999]

#### **Subpart D—Access to and Amendment of Individual Records Pursuant to the Privacy Act of 1974, and Other Privacy Protections**

SOURCE: AG Order No. 5851-2024, 89 FR 1450, Jan. 10, 2024, unless otherwise noted.

##### **§ 16.40 General provisions.**

(a) *Purpose and scope.* (1) This subpart contains the rules that the Department of Justice (“DOJ” or “the Department”) follows when handling records maintained by the Department in a system of records, in accordance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a (“Privacy Act” or “PA”). This subpart describes the procedures by which individuals can be notified if a Department system of records contains records about themselves, may request access to records about themselves maintained in a Department system of records, may request amendment or correction of records about themselves maintained in a Department system of records, and may request an accounting of disclosures of records about themselves maintained in a Department system of records. This subpart also establishes other pro-

cedures on the appropriate maintenance of records by the Department and when Privacy Act exemptions may apply. This subpart should be read together with the Privacy Act, which provides additional information about records maintained in agency systems of records, including those of the Department.

(2) This subpart contains the procedures that the Department follows when handling covered records maintained by the Department in a system of records, in accordance with the Judicial Redress Act of 2015, 5 U.S.C. 552a note (“Judicial Redress Act”). This subpart should be read together with the Privacy Act and the Judicial Redress Act, which provide additional information about covered records maintained in agency systems of records, including those of the Department.

(3) This subpart contains the procedures that the Department follows when collecting, using, maintaining, or disclosing Social Security account numbers, in accordance with the Privacy Act and the Social Security Number Fraud Prevention Act of 2017, 42 U.S.C. 405 note (“Social Security Number Fraud Prevention Act”). This subpart should be read together with the Privacy Act and the Social Security Number Fraud Prevention Act, which provide additional information about agencies’ maintenance of Social Security account numbers, including that of the Department.

(b) *Relationship to the Freedom of Information Act.* The Department also processes Privacy Act requests for access to records under the Freedom of Information Act (FOIA), 5 U.S.C. 552, following the rules contained in subpart A of this part, which gives requesters the benefits of both statutes.

(c) *Definitions.* In addition to the definitions found under 5 U.S.C. 552a(a), and section (2)(h) of the Judicial Redress Act, as used in this subpart:

*Component* means each separate bureau, office, board, division, commission, service, or administration of the Department.

*Privacy Act request for access* means a request made in accordance with 5 U.S.C. 552a(d)(1), and includes requests for a Privacy Act access appeal, in accordance with this subpart.

**§ 16.41****28 CFR Ch. I (7-1-24 Edition)**

*Privacy Act request for amendment or correction* means a request made in accordance with 5 U.S.C. 552a(d)(2)–(4), and includes requests for a Privacy Act amendment or correction appeal, in accordance with this subpart.

*Privacy Act request for an accounting* means a request made in accordance with 5 U.S.C. 552a(c)(3).

*Requester* means an individual who makes a Privacy Act request for access, a Privacy Act request for amendment or correction, a Privacy Act request for an accounting, or, as provided by the Judicial Redress Act, a covered person who makes either a Privacy Act request for access or a Privacy Act request for amendment or correction to covered records.

*System of Records Notice* means the notice(s) published by the Department in the FEDERAL REGISTER upon the establishment or modification of a system of records describing the existence and character of the system of records. A System of Records Notice (“SORN”) may be composed of a single FEDERAL REGISTER notice addressing all of the required elements that describe the current system of records, or it may be composed of multiple FEDERAL REGISTER notices that together address all of the required elements.

(d) *Authority to request records for a law enforcement purpose.* The head of a component or a United States Attorney, or either's designee, is authorized to make written requests under 5 U.S.C. 552a(b)(7), for records maintained by other agencies that are necessary to carry out an authorized law enforcement activity. The request must specify the particular portion desired and the law enforcement activity for which the record is sought.

(e) *Judicial Redress Act application.* (1) With respect to covered records, the Judicial Redress Act authorizes a covered person to bring a civil action against the Department and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring a civil action and obtain civil remedies with respect to records under 5 U.S.C. 552a(g)(1)(A), (B).

(2) To the extent consistent with the Judicial Redress Act, when making a

request for access, amendment, or correction to a covered record, a covered person must follow the procedures outlined in this subpart for making a Privacy Act request for access to a covered record, or a Privacy Act request for amendment or correction of a covered record. A covered person must exhaust the administrative remedies, as outlined in this subpart, before the covered person may bring a cause of action described in paragraph (e)(1) of this section.

(f) *Providing written consent to disclose records protected under the Privacy Act.* The Department may disclose any record contained in a system of records by any means of communication to any person, or to another agency, pursuant to a written request by, or with the prior written consent of, the individual about whom the record pertains. An individual must verify the individual's identity in the same manner as required by § 16.41(d) when providing written consent to disclose a record protected under the Privacy Act and pertaining to the individual.

**§ 16.41 Privacy Act requests for access to records.**

(a) *General information.* (1) The Department has a decentralized system for responding to Privacy Act requests for access to records, with each component designating an office to process Privacy Act requests for access to records maintained by that component. A requester may make a Privacy Act request for access to records about the requester by writing directly to the component that maintains the records. All components have the capability to receive requests electronically either through email or a web portal. The request should be sent or delivered to the component's office at the address listed in appendix I to this part, or in accordance with the access procedures outlined in the corresponding SORN. The functions of each component are summarized in part 0 of this title and in the description of the Department and its components in the United States Government Manual, which is updated on a year-round basis and is available free of charge at <https://www.usgovernmentmanual.gov/>.

**Department of Justice****§ 16.41**

(2) If a requester cannot determine where within the Department to send the Privacy Act request for access to records, the requester may send it by mail to the FOIA/PA Mail Referral Unit, Justice Management Division, Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001; by email to [MRUFOIA.Requests@usdoj.gov](mailto:MRUFOIA.Requests@usdoj.gov); or by fax to (202) 616-6695. The Mail Referral Unit will forward the request to the component(s) it believes most likely to have the requested records. For the quickest possible handling, the requester should mark both the request letter and the envelope "Privacy Act Access Request."

(b) *Description of records sought.* Requesters must describe the records sought in sufficient detail to enable Department personnel to locate the applicable system of records containing them with a reasonable amount of effort. To the extent possible, requesters should include specific information that may assist a component in identifying the requested records, such as the name or identifying number of each system of records in which the requester believes the records are maintained, or the date, title, name, author, recipient, case number, file designation, reference number, or subject matter of the record. The Department publishes SORNs in the **FEDERAL REGISTER** that describe the type and categories of records maintained in Department-wide and component-specific systems of records. Department SORNs may be found in published issues of the **FEDERAL REGISTER** and a list is available at <https://www.justice.gov/opcl/doj-systems-records>. Requesters may also request the record in a particular form or format.

(c) *Agreement to pay fees.* A Privacy Act request for access may specify the amount of fees that the requester is willing to pay in accordance with § 16.49. The component responsible for responding to the request shall confirm this agreement in an acknowledgement letter, in accordance with § 16.43.

(d) *Verification of identity.* (1) A requester must verify the requester's identity when making a Privacy Act request for access. The requester must state the requester's full name, current

address, and date and place of birth. The requester must:

(i) Sign the request, and the signature must either be notarized or submitted by the requester under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization; or

(ii) When available, use one of the Department's approved digital services, as indicated on the Department's Privacy Act Request web page, to verify the identity of the requester through identity proofing and authentication processes.

(2) While no specific form is required, the requester may obtain forms for this purpose from the FOIA/PA Mail Referral Unit, Justice Management Division, Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001, or obtain the form at <https://www.justice.gov/oip/doj-reference-guide-attachment-d-copies-forms>.

(3) To help identify and locate requested records, a requester may also include, at the requester's option, any additional identifying information which may be helpful in identifying and locating the requested records. Components shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information provided by the requester, and to protect against any anticipated threats, in accordance with § 16.51.

(e) *Verification of guardianship.* (1) The parent of a minor, or the legal guardian of an individual who has been declared incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, is permitted to act on behalf of the individual. In order for a parent of a minor or the legal guardian of an individual to make a Privacy Act request for access on behalf of the individual, the parent or legal guardian must establish:

(i) The identity of the individual who is the subject of the request, by stating the name, current address, date and place of birth, and, at the parent or legal guardian's option, any additional identifying information that may be helpful in identifying and locating the requested records;

## § 16.42

## 28 CFR Ch. I (7-1-24 Edition)

(ii) The parent or legal guardian's own identity, as required in paragraph (d) of this section;

(iii) Proof of parentage or legal guardianship, which may be proven by providing a copy of the individual's birth certificate or by providing a court order establishing legal guardianship; and

(iv) That the parent or legal guardian is acting on behalf of that individual in making the request.

(2) Components shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information provided by the parent or legal guardian, and to protect against any anticipated threats, in accordance with § 16.51.

### § 16.42 Responsibility for responding to Privacy Act requests for access to records.

(a) *In general.* Except as stated in paragraphs (c) through (f) of this section, the component that first receives a Privacy Act request for access is the component responsible for responding to the request. In determining which records are responsive to a request, a component ordinarily will include only those records it maintained as of the date the component begins its search. If any other date is used, the component shall inform the requester of that date.

(b) *Authority to grant or deny requests.* The head of a component, or the component head's designee, is authorized to grant or deny any Privacy Act request for access to records maintained by that component.

(c) *Re-routing of misdirected requests.* When a component's FOIA/Privacy Act office determines that a request was misdirected within the Department, the receiving component's FOIA/Privacy Act office shall route the request to the FOIA/Privacy Act office of the proper component(s).

(d) *Consultations, referrals, and coordination.* When a component receives a Privacy Act request for access to a record in its possession, it shall determine whether another component, or another agency of the Federal Government, is better able to determine whether the record is exempt from ac-

cess under the Privacy Act. If the receiving component determines that it is best able to process the record in response to the request, then it shall do so. If the receiving component determines that it is not best able to process the record, then it shall follow the consultation, referral, and coordination procedures under § 16.4, subject to the requirements in this section. Components may make agreements with other components or agencies to eliminate the need for consultations or referrals for particular types of records.

(e) *Consultations, referrals, and coordination concerning law enforcement information.* When a component receives a Privacy Act request for access to a record in its possession containing information that relates to an investigation of a possible violation of law and that originated with another component or agency of the Federal Government, the receiving component shall either refer the responsibility for responding to the request regarding that information to that other component or agency or shall consult with that other component or agency.

(f) *Consultations, referrals, and coordination concerning classified information.* (1) When a component receives a Privacy Act request for access to a record containing information that has been classified or may be appropriate for classification by another component or agency under any applicable Executive order concerning the classification of records, the receiving component shall consult with or refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, or that should consider the information for classification.

(2) When a component receives a Privacy Act request for access to a record containing information that has been derivatively classified, the receiving component shall consult with or refer the responsibility for responding to that portion of the request to the component or agency that classified the underlying information.

### § 16.43 Responses to a Privacy Act requests for access to records.

(a) *In general.* Components should, to the extent practicable, communicate

with requesters who have access to the internet using electronic means, such as through email or a web portal. A component shall honor a requester's preference for receiving a record in a particular form or format where it is readily reproducible by the component in the form or format requested.

(b) *Acknowledgement of requests.* The component responsible for responding to the request must acknowledge, in writing, receipt of a Privacy Act request for access. A component shall initially respond to the requester by acknowledging the Privacy Act request for access, assigning the request an individualized tracking number, and, if applicable, confirming, in writing, the requester's agreement to pay fees in accordance with §16.49.

(c) *Timing of responses to a Privacy Act request for access.* (1) Components ordinarily will respond to Privacy Act requests for access according to their order of receipt. The response time will commence on the date that the request is received by the proper component's office designated to receive requests, but in any event not later than ten (10) working days after the request is first received by any component's office designated by this subpart to receive requests.

(2) A component may designate multiple processing tracks that distinguish between simple and more complex Privacy Act requests for access, based on the estimated amount of work or time needed to process the request. Among the factors a component may consider are the number of pages involved in processing the request and the need for consultations or referrals. Components may advise requesters of the track into which their request falls and, when appropriate, may offer requesters an opportunity to narrow their request so that it can be placed in a different processing track.

(d) *Granting a Privacy Act request for access.* Once a component makes a determination to grant a Privacy Act request for access, in whole or in part, it shall notify the requester in writing. The component shall inform the requester in the notice of any fee charged under §16.49 and shall disclose records to the requester promptly on payment of any applicable fee.

(e) *Adverse determination to a Privacy Act request for access.* A component that makes an adverse determination to a Privacy Act request for access, in whole or in part, shall notify the requester of the adverse determination in writing. An adverse determination to a Privacy Act request for access includes a determination by the component that: the request did not reasonably describe the record sought; the information requested is not a record subject to the Privacy Act; the requested record is not maintained in a system of records; the requested record is exempt, in whole or in part, from a Privacy Act request for access under applicable exemption(s); the requested record does not exist, cannot be located, or has been destroyed; the record is not readily reproducible in a comprehensible form; or there is a matter regarding disputed fees.

(f) *Content of adverse determination response.* An adverse determination to a Privacy Act request for access, in whole or in part, shall be signed by the head of the component, or the component head's designee, and shall include:

(1) The name and title or position of the person responsible for the adverse determination to the Privacy Act request for access;

(2) A brief statement of the reason(s) for the adverse determination to the Privacy Act request for access, including any Privacy Act exemption(s) applied by the component;

(3) An estimate of the volume of any records or information withheld, if applicable, such as the number of pages or some other reasonable form of estimation, although such an estimate is not required if the volume is otherwise indicated or if providing an estimate would harm an interest protected by an applicable exemption; and

(4) A statement that the adverse determination to the Privacy Act request for access may be appealed under §16.45, and a description of the requirements set forth in §16.45.

#### **§ 16.44 Classified information.**

In processing a Privacy Act request for access, a Privacy Act request for amendment or correction, or a Privacy Act request for accounting, in which

## § 16.45

information is classified under any applicable Executive order concerning the classification of records, to the extent the requester lacks the appropriate security clearance and fails otherwise to meet all requirements to access the classified record or information, the originating component shall review the information in the record to determine whether it should remain classified. Information determined to no longer require classification shall be de-classified and the record evaluated for an appropriate release to the requester, subject to any applicable exemptions or exceptions. On receipt of any appeal involving classified information, the official responsible for adjudicating the appeal shall take appropriate action to ensure compliance with part 17 of this title.

### § 16.45 Privacy Act access appeals.

(a) *Requirement for making a Privacy Act access appeal.* A requester may appeal an adverse determination to a Privacy Act request for access to the Office of Information Policy (“OIP”). The contact information for OIP is contained in the FOIA Reference Guide, which is available at [https://www.justice.gov/oip/04\\_3.html](https://www.justice.gov/oip/04_3.html). Appeals may also be submitted through the web portal accessible on OIP’s website. Examples of an adverse determination to a Privacy Act request for access are provided in § 16.43. The requester must make the appeal in writing. To be considered timely, the requester must postmark, or in the case of electronic submissions, submit the request, within 90 calendar days after the date of the adverse determination. The appeal should indicate the assigned request number and clearly identify the component’s determination that is being appealed. To facilitate handling, the requester should mark both the appeal letter and envelope, or include in the subject line of any electronic communication, “Privacy Act Access Appeal.”

(b) *Adjudication of Privacy Act access appeals.* (1) The Director of OIP, or a designee of the Director of OIP, shall act on behalf of the Attorney General on all Privacy Act access appeals under this section, unless the Attorney General directs otherwise.

## 28 CFR Ch. I (7-1-24 Edition)

(2) Should the Attorney General exercise the right to respond to a Privacy Act request for access, the Attorney General’s decision shall serve as the final action of the Department and will not be subject to a Privacy Act access appeal.

(3) A Privacy Act access appeal ordinarily will not be adjudicated if the request becomes a matter of litigation.

(c) *Responses to Privacy Act access appeals.* (1) OIP shall make its decision on an appeal in writing.

(2) A decision that upholds a component’s adverse determination to the Privacy Act request for access, in whole or in part, shall include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, and shall provide the requester with notification of the statutory right to file a lawsuit.

(3) A decision that reverses or modifies, in whole or in part, a component’s adverse determination to the Privacy Act request for access shall include notice to the requester of the specific reversal or modification. The component(s) shall thereafter further process the request, in accordance with the appeal decision, and respond directly to the requester, as appropriate.

(d) *When a Privacy Act access appeal is required.* Before seeking review by a court of a component’s refusal to grant a Privacy Act request for access, a requester generally must first submit a timely appeal in accordance with this section.

### § 16.46 Privacy Act requests for amendment or correction.

(a) *Requirements for making a Privacy Act request for amendment or correction.* Unless the record is not subject to amendment or correction, as stated in paragraph (i) of this section, individuals may make a Privacy Act request for amendment or correction of a Department record about themselves. Requesters must write directly to the Department component that maintains the record. A Privacy Act request for amendment or correction shall identify each particular record in question, state the amendment or correction that the requester would like to make, and state why the requester believes the record is not accurate, relevant,

timely, or complete. Requesters may submit any documentation that would be helpful in determining the accuracy, relevance, timeliness, or completeness of the record. If the requester believes that the same record is in more than one Department system of records, the requester should address the request to each component that the requester believes maintains the record. For the quickest possible handling, requesters should mark both their request letter and envelope "Privacy Act Amendment Request." Components and requesters must otherwise follow the procedures and responsibilities set forth in §§16.41 and 16.42.

(b) *Timing of responses to a Privacy Act request for amendment or correction.* (1) Components responsible for responding to a Privacy Act request for amendment or correction must acknowledge, in writing, receipt of the request no later than ten (10) working days after receipt.

(2) Components must promptly respond to a Privacy Act request for amendment or correction. Components ordinarily will respond to Privacy Act requests for amendment or correction according to their order of receipt. The response time will commence on the date that the request is received by the proper component's office designated to receive requests, but in any event no later than ten (10) working days after the request is first received by any component's office designated by this subpart to receive requests.

(3) A component may designate multiple processing tracks that distinguish between simple and more complex Privacy Act requests for amendment or correction, based on the estimated amount of work or time needed to process the request. Among the factors a component may consider are the number of pages involved in processing the request and the need for consultations or referrals. Components may advise requesters of the track into which their request falls and, when appropriate, may offer requesters an opportunity to narrow their request so that it can be placed in a different processing track.

(c) *Granting a Privacy Act request for amendment or correction.* If a component grants a Privacy Act request for

amendment or correction, in whole or in part, it shall notify the requester in writing. The component shall describe the amendment or correction made and shall advise the requester of the requester's right to obtain a copy of the corrected or amended record, in accordance with the Privacy Act right of access procedures described in §§16.41 through 16.45.

(d) *Adverse determination to a Privacy Act request for amendment or correction.* A component that makes an adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall notify the requester of the determination in writing. An adverse determination to a Privacy Act request for amendment or correction includes a decision by the component that: the information at issue is not a record as defined by the Privacy Act; the requested record is not subject to amendment or correction as stated in paragraph (i) of this section; the request does not reasonably describe the records sought or the amendment or correction to that record; the record at issue does not exist, cannot be located, has been destroyed, or otherwise cannot be amended or corrected; or the record is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness in any determination about the individual about whom the record pertains.

(e) *Content of adverse determination response.* An adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall be signed by the head of the component, or the component head's designee, and shall include:

(1) The name and title or position of the person responsible for the adverse determination to the Privacy Act request for amendment or correction;

(2) A brief statement of the reason(s) for the adverse determination to the Privacy Act request for amendment or correction, including any Privacy Act exemption(s) applied by the component; and

(3) A statement that the adverse determination to the Privacy Act request for amendment or correction may be appealed under paragraph (f) of this

## § 16.46

## 28 CFR Ch. I (7-1-24 Edition)

section and a description of the requirements set forth in paragraph (f).

(f) *Privacy Act amendment appeals.* (1) A requester may appeal an adverse determination to a Privacy Act request for amendment or correction, in whole or in part, to the Office of Privacy and Civil Liberties (“OPCL”). The contact information for OPCL is available at <https://www.justice.gov/privacy>. The requester must make the appeal in writing. To be considered timely, the requester must postmark the appeal request, or in the case of electronic submissions, submit the appeal request, within 90 calendar days after the date of the component’s refusal to grant a Privacy Act request for amendment or correction. The appeal should indicate the assigned request number and clearly identify the component’s determination that is being appealed. To facilitate handling, the requester should mark both the appeal letter and envelope, or include in the subject line of the electronic transmission, “Privacy Act Amendment Appeal.”

(2) The Chief Privacy and Civil Liberties Officer (“CPCLO”), or a designee of the CPCLO, will act on behalf of the Attorney General on all Privacy Act amendment appeals under this section, unless otherwise directed by the Attorney General.

(3) A Privacy Act amendment appeal ordinarily will not be adjudicated if the request becomes a matter of litigation.

(4) A decision on a Privacy Act amendment appeal must be made in writing. A decision that upholds a component’s adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, whether the requester has a right to file a Statement of Disagreement, as described in paragraph (g) of this section, and the requester’s statutory right to file a lawsuit. A decision that reverses or modifies a component’s adverse determination to a Privacy Act request for amendment or correction, in whole or in part, shall notify the requester of the specific reversal or modification. The component shall thereafter further process the request, in accordance with

the appeal decision, and respond directly to the requester, as appropriate.

(g) *Statement of Disagreement.* If a request is subject to a Privacy Act request for amendment or correction, but the component’s adverse determination to a Privacy Act request for amendment or correction is upheld, in whole or in part, the requester has the right to file a Statement of Disagreement that states the requester’s reason(s) for disagreeing with the Department’s refusal to grant the requester’s Privacy Act request for amendment or correction. Statements of Disagreement must be concise, must clearly identify each part of any record that is disputed, and should be no longer than one typed page for each fact disputed. A Statement of Disagreement must be sent to the component involved, which shall place it in the system of records in which the disputed record is maintained so that the Statement of Disagreement supplements the disputed record. The component shall mark the disputed record to indicate that a Statement of Disagreement has been filed and where in the system of records it may be found.

(h) *Notification of amendment, correction, or Statement of Disagreement.* Within thirty (30) working days of the amendment or correction of a record, the component that maintains the record shall notify all persons, organizations, or agencies to which it previously disclosed the record, if an accounting of that disclosure was made, that the record has been amended or corrected. If an individual has filed a Statement of Disagreement, the component shall append a copy of it to the disputed record whenever the record is disclosed. The component may also append a concise statement of its reason(s) for denying the Privacy Act request for amendment or correction of the record.

(i) *Records not subject to amendment or correction.* The following records are not subject to amendment or correction:

- (1) Copies of court records;
- (2) Transcripts of testimony given under oath or written statements made under oath;
- (3) Transcripts of grand jury proceedings, judicial proceedings, or

**Department of Justice****§ 16.49**

quasi-judicial proceedings, which are the official record of those proceedings;

(4) Presentence reports, and other records pertaining directly to such reports originating with the courts;

(5) Records in a system of records that have been exempted from amendment and correction, pursuant to 5 U.S.C. 552a(j) or (k), through the applicable regulations in this subpart; and

(6) Records not maintained in a system of records.

**§ 16.47 Privacy Act requests for an accounting of record disclosures.**

(a) *Requirements for making a Privacy Act request for accounting of record disclosures.* Except where accountings of disclosures are not required to be kept as stated in paragraph (c) of this section, individuals may make a Privacy Act request for an accounting of record disclosures about themselves that have been made by the Department to another person, organization, or agency. This accounting contains the date, nature, and purpose of each disclosure, as well as the name and address of the person, organization, or agency to which the disclosure was made. If the requester believes that the same record is in more than one system of records, the requester should address their request to each component that the requester believes maintains the record. For the quickest possible handling, requesters should mark both their request letters and envelopes "Privacy Act Accounting Request." Requests must otherwise follow the procedures in § 16.41.

(b) *Processing Privacy Act requests for an accounting of record disclosures.* Unless otherwise specified in this section, components shall process Privacy Act requests for accountings of record disclosures following the procedures in §§ 16.42 and 16.43.

(c) *Where accountings of record disclosures are not required.* Components are not required to provide Privacy Act accountings of record disclosures to a requester in cases in which they relate to:

(1) Disclosures of information not subject to the Privacy Act;

(2) Disclosures of records not maintained in a system of records;

(3) Disclosures of records maintained in a system of records for which accountings are not required to be kept, including disclosures to those officers and employees of the Department who have a need for the record in the performance of their duties, 5 U.S.C. 552a(b)(1), or disclosures that are required under the FOIA, 5 U.S.C. 552a(b)(2);

(4) Disclosures made to law enforcement agencies for authorized law enforcement activities in response to written requests from those law enforcement agencies specifying the law enforcement activities for which the disclosures are sought; or

(5) Disclosures made from systems of records that have been exempted from the accounting of record disclosure requirements pursuant to the Privacy Act, 5 U.S.C. 552a(j) or (k), through the applicable regulations in this subpart.

(d) *Appeals.* A requester may appeal a component's refusal to grant a Privacy Act request for an accounting of record disclosures in the same manner, and under the same procedures, as a Privacy Act access appeal, as set forth in § 16.45.

**§ 16.48 Preservation of records.**

Each component shall preserve all correspondence pertaining to the requests that it receives under this subpart, as well as copies of all requested records, until disposition or destruction is authorized by title 44 of the United States Code or by the National Archives and Records Administration's General Records Schedule 4.2. Records shall not be disposed of while they are the subject of a pending request, appeal, or lawsuit under the Privacy Act.

**§ 16.49 Fees.**

Components shall charge fees for duplication of records under the Privacy Act in the same way in which they charge duplication fees for responding to FOIA requests under § 16.10. No search or review fee may be charged for any record unless the record has been exempted from access pursuant to exemptions enumerated in the Privacy Act, 5 U.S.C. 552a(j)(2) or (k)(2).

## § 16.50

### § 16.50 Notice of compulsory legal process and emergency disclosures.

(a) *Legal process disclosures.* Components shall make reasonable efforts to provide notice to an individual whose record is disclosed under compulsory legal process, such as an order by a court of competent jurisdiction, and such process becomes a matter of public record. Notice shall be given within a reasonable time after the component's receipt of process, except that in a case in which such process is not a matter of public record, the notice shall be given within a reasonable time only after such process becomes public. Where an individual, or the individual's legal counsel, has not otherwise received notice of the disclosure in the litigation process, notice shall be mailed to the individual's last known address and shall contain a copy of such process and a description of the information disclosed. Notice shall not be required if disclosure is made from a system of records that has been exempted from the notice requirement.

(b) *Emergency disclosures.* Upon disclosing a record pertaining to an individual made under compelling circumstances affecting health or safety, the component shall notify that individual of the disclosure. This notice shall be mailed to the individual's last known address and shall state the nature of the information disclosed; the person, organization, or agency to which it was disclosed; the date of disclosure; and the compelling circumstances justifying the disclosure.

### § 16.51 Security of systems of records.

(a) Each component shall establish and maintain administrative, technical, and physical controls consistent with applicable Department and Government-wide laws, regulations, policies, and standards, to ensure the security and confidentiality of records, and to protect against reasonably anticipated threats or hazards to their security or integrity, including against any reasonably anticipated unauthorized access, use, or disclosure, which could result in substantial harm, embarrassment, inconvenience, or unfairness to individuals about whom information is maintained. The stringency of these controls shall correspond to the sensi-

## 28 CFR Ch. I (7-1-24 Edition)

tivity of the records that the controls protect. At a minimum, each component shall maintain administrative, technical, or physical controls to ensure that:

(1) Records are protected from unauthorized access, including unauthorized public access;

(2) The physical area in which records are maintained is supervised or appropriately secured to prevent unauthorized persons from having access to them;

(3) Records are protected from damage, loss, or unauthorized alteration or destruction; and

(4) Records are not disclosed to unauthorized persons or to authorized persons for unauthorized purposes in either oral or written form.

(b) Each component shall establish procedures that restrict access to records to only those individuals within the Department who must have access to those records in order to perform their duties and that prevent inadvertent disclosure of records.

(c) The CPCLO, or a designee of the CPCLO, may impose additional administrative, technical, or physical controls to protect records in consultation with the Chief Information Officer and the Director of the Office of Records Management Policy.

### § 16.52 Contracts for the operation of record systems.

(a) Any approved contract for the operation of a system of records shall contain the standard contract terms and conditions in accordance with the Federal Acquisition Regulations in 48 CFR chapter 28 and may also contain additional privacy-related terms and conditions to ensure compliance with the requirements of the Privacy Act for that system of records. The contracting component will be responsible for ensuring that the contractor complies with these contract requirements.

(b) The CPCLO, a designee of the CPCLO, or contracting components may impose additional contract requirements to further protect records.

### § 16.53 Use and collection of Social Security account numbers.

(a) *Purpose and scope.* This section contains the rules that the Department

**Department of Justice****§ 16.54**

of Justice follows in handling Social Security account numbers in accordance with section 7 of the Privacy Act, and with the Social Security Fraud Prevention Act.

(b) *Definitions.* For the purposes of this section:

*Mail* means any physical package sent to entities or individuals outside the Department through the United States Postal Service or any other express mail carrier; and

*Necessary* includes only those circumstances in which a component would be unable to comply, in whole or in part, with a legal, regulatory, or policy requirement if prohibited from mailing the full Social Security account number. Including the full Social Security account number of an individual on a document sent by mail is not “necessary” if a legal, regulatory, or policy requirement could be satisfied by either partially redacting the Social Security account number in accordance with paragraph (d)(3) of this section, or entirely removing the Social Security account number.

(c) *Denial of rights, benefits, or privileges.* Components are prohibited from denying any right, benefit, or privilege provided by law to an individual because of such individual’s refusal to disclose the individual’s Social Security account number. This paragraph (c) shall not apply with respect to:

(1) Any disclosure that is required by Federal statute; or

(2) The disclosure of a Social Security account number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(d) *Restriction of Social Security account numbers on documents sent by mail.*

(1) A component shall not include the full Social Security account number of an individual on any document sent by mail, unless the inclusion of the Social Security account number on the document is necessary. Unless the Attorney General directs otherwise, the CPCLO is authorized to assist components in implementing this paragraph (d), including determining whether inclusion

of the Social Security account number on a document sent by mail is necessary.

(2) If the use of the full Social Security account number on a document sent by mail is necessary, the component sending the document shall implement appropriate administrative, technical, and physical safeguards to ensure a reasonable level of security against unauthorized access to, and use, disclosure, disruption, modification, or destruction of, the documents sent by mail.

(3) Where feasible, components should partially redact the Social Security account number on any document sent by mail by including no more than the last four digits of the Social Security account number. Components should prioritize technical methods to redact Social Security account numbers.

(4) Components are prohibited from placing a Social Security account number, whether full or partially redacted, on the outside of any mail.

(e) *Employee awareness.* Each component shall ensure that employees authorized to collect Social Security account numbers are made aware of the following:

(1) The requirements of paragraphs (c) and (d) of this section;

(2) That individuals requested to provide their Social Security account numbers must be informed of:

(i) Whether providing Social Security account numbers is mandatory or voluntary;

(ii) Any statutory or regulatory authority that authorizes the collection of Social Security account numbers; and

(iii) The uses that will be made of the Social Security account numbers; and

(3) That the Department may have other regulations or policies regulating the use, maintenance, or disclosure of Social Security account numbers by which employees must abide.

**§ 16.54 Employee standards of conduct.**

Each component shall inform its employees and any contractors involved in developing or maintaining a system of records of the provisions of the Privacy Act, including the Privacy Act’s

## § 16.55

civil liability and criminal penalty provisions. Unless otherwise permitted by law, employees and contractors of the Department shall:

(a) Collect from individuals only the information that is relevant and necessary to discharge the responsibilities of the Department;

(b) Collect information about an individual directly from that individual whenever practicable;

(c) Inform each individual asked to supply information for a record pertaining to that individual of:

(1) The legal authority to collect the information and whether providing it is mandatory or voluntary;

(2) The principal purpose for which the Department intends to use the information;

(3) The routine uses the Department may make of the information; and

(4) The effects on the individual, if any, of not providing the information;

(d) Ensure that the component maintains no system of records without public notice and that it notifies appropriate Department officials of the existence or development of any system of records that is not the subject of a current or planned public notice;

(e) Maintain all records that are used by the Department in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination;

(f) Except as to disclosures made to an agency or made under the FOIA, make reasonable efforts, prior to disseminating any record about an individual, to ensure that the record is accurate, relevant, timely, and complete;

(g) Maintain no record describing how an individual exercises the individual's First Amendment rights, unless maintaining the record is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity;

(h) When required by the Privacy Act, maintain an accounting in the specified form of all disclosures of records by the Department to persons, organizations, or agencies;

## 28 CFR Ch. I (7-1-24 Edition)

(i) Maintain and use records with care to prevent the loss or the unauthorized or inadvertent disclosure of a record to anyone;

(j) Notify the appropriate Department official of any record that contains information that the Privacy Act does not permit the Department to maintain; and

(k) Read, acknowledge, and agree to abide by the Department of Justice rules of behavior for accessing, collecting, using, and maintaining Department information.

### § 16.55 Other rights and services.

Nothing in this subpart shall be construed to entitle any person, as of right, to any service or to the disclosure of any record to which such person is not entitled under the Privacy Act, the Social Security Fraud Reduction Act, or the Judicial Redress Act.

## Subpart E—Exemption of Records Systems Under the Privacy Act

SOURCE: Order No. 645-76, 41 FR 12640, Mar. 26, 1976, unless otherwise noted.

### § 16.70 Exemption of the Office of the Attorney General System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e) (1), (2) and (3), (e)(4) (G) and (H), (e)(5); and (g):

(1) General Files System of the Office of the Attorney General (JUSTICE/OAG-001).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest on the part of the Department of Justice as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee

the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official Federal investigations. Individual access to these records might compromise ongoing investigations, reveal confidential informants or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e) (1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations of duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsections (e)(4) (G) and (H) because this system is exempt from the access provisions of subsection (d)

pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (g) because this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

[Order No. 31-85, 51 FR 751, Jan. 8, 1986]

**§ 16.71 Exemption of the Office of the Deputy Attorney General System—limited access.**

(a) The following systems of records and exempt from 5 U.S.C. 552a(d)(1) and (e)(1):

(1) Presidential Appointee Candidate Records System (JUSTICE/DAG-006).

(2) Presidential Appointee Records System (JUSTICE/DAG-007).

(3) Special Candidates for Presidential Appointments Records System (JUSTICE/DAG-008).

(4) Miscellaneous Attorney Personnel Records System (JUSTICE/DAG-011).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a Presidential appointee or Department attorney position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department of Justice. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate for a position which assists

## § 16.72

in determining whether that candidate should be nominated for appointment.

(c) The General Files System of the Office of the Deputy Attorney General (JUSTICE/DAG-013) is exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (2), (3) and (5); and (g).

(d) The exemptions for the General Files System apply only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(e) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her could reveal investigative interest on the part of the Department of Justice, as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel. Further, making available to a record subject the accounting of disclosures could reveal the identity of a confidential source. In addition, release of an accounting of disclosures from the General Files System may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security.

(2) From subsection (c)(4) because these systems are exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in these systems relate to official Federal investigations. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. In addition, release of records from the General Files System may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security. Amendment of the records in

## 28 CFR Ch. I (7-1-24 Edition)

either of these systems would interfere with ongoing law enforcement proceedings and impose an impossible administrative burden by requiring law enforcement investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede any investigative process, whether civil or criminal, if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and may therefore be able to avoid detection, apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsection (g) because these systems of records are exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

[Order No. 57-91, 56 FR 58305, Nov. 19, 1991, as amended by Order No. 006-2013, 78 FR 69754, Nov. 21, 2013]

### § 16.72 Exemption of Office of the Associate Attorney General System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e)(1), (2), (3) and (5); and (g):

(1) General Files System of the Office of the Associate Attorney General (JUSTICE/AAG-001).

**Department of Justice****§ 16.73**

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her could reveal investigative interest on the part of the Department of Justice, as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel. Further, making available to a record subject the accounting of disclosures could reveal the identity of a confidential source. In addition, release of an accounting of disclosures may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official Federal investigations. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. In addition, release of these records may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security. Amendment of the records in this system would interfere with ongoing law enforcement proceedings and impose an impossible administrative burden by requiring law enforcement investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or introduced

the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede any investigative process, whether civil or criminal, if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and may therefore be able to avoid detection, apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsection (g) because this system of records is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act.

[Order No. 57-91, 56 FR 58305, Nov. 19, 1991]

**§ 16.73 Exemption of Office of Legal Policy Systems.**

(a) The Judicial Nominations Files (JUSTICE/OLP-002) system of records is exempt from subsections (c)(3); (d); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), and (k)(6). The exemptions in this paragraph (a) apply only to the extent that information in this system of records is subject to an exemption, pursuant to 5 U.S.C. 552a(k). Where compliance would not appear to interfere with or adversely affect the Office of Legal Policy's (OLP's) processes, OLP may waive the applicable exemption.

(b) Exemptions from the particular subsections in paragraph (a) of this section are justified for the following reasons:

**§ 16.73****28 CFR Ch. I (7-1-24 Edition)**

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because release of disclosure accountings could alert the subject of an investigation and/or evaluation to the extent of an investigation and/or evaluation. Such a disclosure could also reveal investigative interests by not only OLP, but also other recipient agencies or components. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation and/or evaluation, release could result in the destruction of documentary evidence, improper influencing of witnesses, endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel, the fabrication of testimony, and other activities that could impede or compromise the investigation and/or evaluation. In addition, providing the individual an accounting for each disclosure could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy.

(2) From subsection (d), the access and amendment provisions, because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning the subject of an investigation and/or evaluation. Access could reveal the identity of the source of the information and constitute a breach of the promised confidentiality on the part of the Department. Such breaches ultimately would restrict the free flow of information vital to the determination of a candidate's qualifications and suitability, among other determinations. The Department also relies on certain examination materials to assess and evaluate an individual's qualifications for an applicable position. Access and/or amendment to such material could reveal information about the examination and vetting process and could compromise its objectivity and/or fairness. Access and/or amendment to such material could also inappropriately advantage future candidates with knowledge of the examination materials. Finally, providing the individual access or amendment rights could result in

the release of properly classified information which would compromise the national defense or disrupt foreign policy.

(3) From subsection (e)(1), because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of the subject of an investigation and/or evaluation. Information which may seem irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate which assists in determining whether that candidate should be nominated for appointment. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In interviewing individuals or obtaining other forms of information during OLP processes, information may be supplied to OLP which relates to matters incidental to the primary purpose of OLP's processes, but also relate to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(4) From subsections (e)(4)(G) and (H), and subsection (f), because this system is exempt from the access and amendment provisions of subsection (d).

(c) The General Files System of the Office of Legal Policy (JUSTICE/OLP-003) system of records is exempt from subsections 552a(c)(3) and (4); (d); (e)(1), (2) and (3), (e)(4)(G) and (H), and (e)(5); and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5). The exemptions in this paragraph (c) apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552(j), (k). Where compliance would not appear to interfere with or adversely affect OLP's processes, the applicable exemption may be waived by OLP.

(d) Exemptions from the particular subsections in paragraph (c) of this section are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject

**Department of Justice****§ 16.74**

the accounting of disclosures from records concerning him/her would reveal investigative interest on the part of the Department as well as the recipient agency. This would permit record subjects to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official Federal investigations. Individual access to these records might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information since it may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigation process if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsections (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations and duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information gathering process, thus hampering the investigation.

(7) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (g) because this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

[Order No. 009-2021, 86 FR 54369, Oct. 1, 2021]

**§ 16.74 Exemption of National Security Division Systems—limited access.**

(a) The following system of records is exempted from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2) and (5): Foreign Intelligence and Counterintelligence Records System (JUSTICE/NSD-001). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) *Subsection (c)(3).* To provide the target of a surveillance or collection activity with the disclosure accounting records concerning him or her would hinder authorized United States intelligence activities by informing that individual of the existence, nature, or scope of information that is properly classified pursuant to Executive Order 12958, as amended, and thereby cause damage to the national security.

(2) *Subsection (c)(4).* This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d)(1).* Disclosure of foreign intelligence and counterintelligence information would interfere with collection activities, reveal the identity of confidential sources, and cause damage to the national security

## § 16.75

## 28 CFR Ch. I (7-1-24 Edition)

of the United States. To ensure unhampered and effective collection and analysis of foreign intelligence and counterintelligence information, disclosure must be precluded.

(4) *Subsection (d)(2).* Amendment of the records would interfere with ongoing intelligence activities thereby causing damage to the national security.

(5) *Subsections (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsection (e)(1).* It is often impossible to determine in advance if intelligence records contained in this system are relevant and necessary, but, in the interests of national security, it is necessary to retain this information to aid in establishing patterns of activity and provide intelligence leads.

(7) *Subsection (e)(2).* Although this office does not conduct investigations, the collection efforts of agencies that supply information to this office would be thwarted if the agencies were required to collect information with the subject's knowledge.

(8) *Subsection (e)(3).* To inform individuals as required by this subsection could reveal the existence of collection activity and compromise national security. For example, a target could, once made aware that collection activity exists, alter his or her manner of engaging in intelligence or terrorist activities in order to avoid detection.

(9) *Subsections (e)(4)(G), (H) and (I), and (f).* These subsections are inapplicable to the extent that this system is exempt from the access provisions of subsection (d).

(10) *Subsection (e)(5).* It is often impossible to determine in advance if intelligence records contained in this system are accurate, relevant, timely and complete, but, in the interests of national security, it is necessary to retain this information to aid in establishing patterns of activity and providing intelligence leads.

(11) *Subsection (e)(8).* Serving notice could give persons sufficient warning to evade intelligence collection and anti-terrorism efforts.

(12) *Subsections (g) and (h).* These subsections are inapplicable to the extent

that this system is exempt from other specific subsections of the Privacy Act.

[Order No. 023-2007, 72 FR 44382, Aug. 8, 2007]

### § 16.75 Exemption of the Office of the Inspector General Systems/Limited Access.

(a) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2), (3), (5), and (8), and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) of 5 U.S.C. 552a:

(1) Office of the Inspector General Investigative Records (JUSTICE/OIG-001).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the Office of the Inspector General (OIG).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation, and reveal investigative interest by not only the OIG, but also by the recipient agency. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation, release could result in the destruction of documentary evidence, improper influencing of witnesses, endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel, the fabrication of testimony, flight of the subject from the area, and other

activities that could impede or compromise the investigation. In addition, accounting for each disclosure could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel, and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIG for the following reasons:

(i) It is not possible to detect relevance or necessity of specific informa-

tion in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIG may obtain information concerning actual or potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIG should retain this information, as it may aid in establishing patterns of criminal activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation, information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may relate also to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(5) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts, violations of rules of conduct, or any other misconduct must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

## § 16.75

## 28 CFR Ch. I (7-1-24 Edition)

(6) From subsection (e)(3) because the application of this provision would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5) because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Material which may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance as an investigation progresses. The restrictions of this provision could interfere with the preparation of a complete investigative report, and thereby impede effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2) and (k)(1) and (k)(2) of the Privacy Act.

(c) The Data Analytics Program Records System (JUSTICE/OIG-006) system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act. These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, *e.g.*, public source materials, the applicable exemption

may be waived, either partially or totally, by OIG.

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because release of disclosure accounting could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of an investigation and the fact that the individual is the subject of the investigation. Such a disclosure could also reveal investigative interests by not only OIG, but also by the recipient agency or component. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation, release could result in the destruction of documentary evidence, improper influencing of witnesses, endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel, the fabrication of testimony, flight of the subject from the area, and other activities that could impede or compromise the investigation. In addition, providing the individual an accounting for each disclosure could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy.

(2) From subsection (c)(4) notification requirements, for the same reasons that justify exempting this system from the access and amendment provisions of subsection (d), and similarly, from the accounting of disclosures provision of subsection (c)(3). The DOJ takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of DOJ records, it will share that information in appropriate cases.

(3) From subsection (d), the access and amendment provisions, because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, of the existence of the investigation; of the nature and scope of the

information and evidence obtained as to the subject's activities; of the identity of confidential sources, witnesses, and law enforcement personnel, and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information that would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1), because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIG for the following reasons:

(i) It is not possible to determine the relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIG may obtain information concerning actual or potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIG should retain this information in accordance with applicable record retention procedures, as it may aid in es-

tablishing patterns of criminal activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation, information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may also relate to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(5) From subsection (e)(2), because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts, violations of rules of conduct, or any other misconduct must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

(6) From subsection (e)(3), because the application of this provision would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5), because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In the collection of information

## § 16.76

## 28 CFR Ch. I (7-1-24 Edition)

for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Material that may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance as an investigation progresses. The restrictions of this provision could interfere with the preparation of a complete investigative report, and thereby impede effective law enforcement.

(8) From subsection (e)(8), because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on OIG and may alert the subjects of law enforcement investigations, who might be otherwise unaware, to the fact of those investigations. Such notice could also reveal investigative techniques, procedures, or evidence.

(9) From subsection (g), to the extent that this system is exempt from the access and amendment provisions of subsection (d), pursuant to subsections (j)(2), (k)(1), and (k)(2) of the Privacy Act.

[Order No. 63-92, 57 FR 8263, Mar. 9, 1992, as amended by Order No. 64-92, 57 FR 8263, Mar. 9, 1992; AG Order No. 006-2018, 83 FR 66126, Dec. 26, 2018]

### § 16.76 Exemption of Justice Management Division.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) Controlled Substances Act Non-public Records (JUSTICE/JMD-002).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemption from subsection (d) is justified for the following reasons:

(1) Access to and use of the nonpublic records maintained in this system are restricted by law. Section 3607(b) of Title 18 U.S.C. (enacted as part of the Sentencing Reform Act of 1984, Pub. L. 98-473, Chapter II) provides that the sole purpose of these records shall be for use by the courts in determining whether a person found guilty of violating section 404 of the Controlled Substances Act qualifies:

(i) For the disposition available under 18 U.S.C. 3607(a) to persons with

no prior conviction under a Federal or State law relating to controlled substances, or

(ii) For an order, under 18 U.S.C. 3607(c), expunging all official records (except the nonpublic records to be retained by the Department of Justice) of the arrest and any subsequent criminal proceedings relating to the offense.

(2) Information in this system consists of arrest records, including those of co-defendants. The records include reports of informants and investigations. Therefore, access could disclose investigative techniques, reveal the identity of confidential sources, and invade the privacy of third parties.

(c) The following system of records is exempted from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g): Federal Bureau of Investigation Whistleblower Case Files (Justice/JMD-023). These exemptions apply only to the extent that information in a record contained within this system is subject to exemptions pursuant to 5 U.S.C. 552a(j)(2) and (k).

(d) Exemption from the particular subsections is justified for the following reasons:

(1) *Subsection (c)(3).* To provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) *Subsection (c)(4).* This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d)(1).* Information within this record system could relate to official federal investigations and matters of law enforcement. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal

privacy of third parties who are involved in a certain investigation. Disclosure may also reveal information relating to actual or potential law enforcement investigations. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) *Subsection (d)(2).* Amendment of these records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) *Subsections (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsection (e)(1).* It is often impossible to determine in advance if investigatory information contained in this system is accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2).* To collect information from the subject individual could serve to notify the subject individual that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) *Subsection (e)(3).* To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) *Subsection (e)(5).* It is often impossible to determine in advance if investigatory information contained in this system is accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8).* To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g).* This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(e) The following system of records is exempted from 5 U.S.C. 552a(c)(3); (d)(1)–(4); (e)(1), (e)(4)(G), (H), and (I); and (f): Department of Justice Security Monitoring and Analytics Service Records (JUSTICE/JMD-026). The exemptions in this paragraph (e) apply only to the extent that information in this system of records is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Where DOJ determines compliance would not appear to interfere with or adversely affect the purpose of this system of records to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems, the applicable exemption may be waived by the DOJ in its sole discretion.

(f) Exemptions from the particular subsections listed in paragraph (e) of this section are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system of records is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning the subject would specifically reveal investigative interests in the records by the DOJ, external Federal agency subscribers, or other entities that are recipients of the disclosures. Revealing this information could compromise sensitive information or interfere with the overall law enforcement process by revealing a pending sensitive cybersecurity investigation. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to impede the investigation, *e.g.*, destroy evidence or alter techniques to evade discovery.

(2) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), and (f) because these provisions concern individual access to and amendment of certain law enforcement and sensitive records,

## § 16.77

## 28 CFR Ch. I (7-1-24 Edition)

compliance of which could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the DOJ, external Federal agency subscribers, and/or other entities that are recipients of the disclosure. Providing access could compromise sensitive information or reveal sensitive cybersecurity investigative techniques; provide information that would allow a subject to avoid detection; or constitute a potential danger to the health or safety of law enforcement personnel or confidential sources.

(3) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes. The relevance and utility of certain information that may have a nexus to cybersecurity threats may not always be fully evident until and unless it is vetted and matched with other information lawfully maintained by the DOJ, external Federal agency subscribers, or other entities.

(4) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system of records than has been published in the *FEDERAL REGISTER*. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement information.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 688-77, 42 FR 9999, Feb. 18, 1977; Order No. 899-80, 45 FR 43703, June 30, 1980; Order No. 6-86, 51 FR 15476, Apr. 24, 1986; Order No. 246-2001, 66 FR 54663, Oct. 30, 2001; Order No. 297-2002, 67 FR 70163, Nov. 21, 2002; Order No. 019-2005, 71 FR 17, Jan. 3, 2006; CPCLO Order No. 011-2021, 86 FR 61691, Nov. 8, 2021]

### § 16.77 Exemption of U.S. Trustee Program System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4); (d); (e) (1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8); (f) and (g):

(1) U.S. Trustee Program Case Referral System, JUSTICE/UST-004.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the nature of that investigation. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) since an exemption being claimed for subsection (d) makes this subsection inapplicable.

(3) From subsection (d) because access to the records contained in this system might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously re-investigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interest of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness, and completeness of all information obtained.

(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement because the subject of the investigation would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses

**Department of Justice****§ 16.79**

improperly, to destroy evidence, or to fabricate testimony.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it would compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7) From subsections (e)(4) (G) and (H) because this system of records is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k).

(8) From subsection (e)(8) because the individual notice requirement of this subsection could present a serious impediment to law enforcement in that this could interfere with the U.S. Attorney's ability to issue subpoenas.

(9) From subsections (f) and (g) because this system has been exempted from the access provisions of subsection (d).

[Order No. 1-87, 52 FR 3631, Feb. 5, 1987]

**§ 16.78 Exemption of the Special Counsel for Immigration-Related, Unfair Employment Practices Systems.**

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (d).

(1) Central Index File and Associated Records, JUSTICE/OSC-001.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the nature of that investigation. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries.

(2) From subsection (d) because access to the records might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal

privacy of third parties who are involved in a certain investigation.

[Order No. 10-88, 53 FR 7735, Mar. 10, 1988]

**§ 16.79 Exemption of Pardon Attorney System.**

(a) The following system of records is exempt from 5 U.S.C. 552a, subsections (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), and (e)(5): Executive Clemency Case Files/Executive Clemency Tracking System (JUSTICE/OPA-001). These exemptions apply only to the extent that information in this system of records is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because:

(i) The purpose of the creation and maintenance of the Executive Clemency Case Files/Executive Clemency Tracking System (JUSTICE/OPA-001) is to enable the Justice Department to prepare reports and recommendations to the President for his ultimate decisions on clemency matters, which are committed to exclusive discretion of the President pursuant to Article II, Section 2, Clause 1 of the Constitution.

(ii) Release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the requester to obtain valuable information concerning the nature and scope of a clemency investigation, invade the right of candid and confidential communications among officials concerned with making recommendations to the President in clemency matters, and disclose the identity of persons who furnished information to the Government under an express or implied promise that their identities would be held in confidence.

(2) From subsection (c)(4) because the exemption from subsections (d)(1), (d)(2), (d)(3), and (d)(4) will make notification of disputes inapplicable.

(3) From subsections (d)(1), (d)(2), (d)(3), and (d)(4) is justified for the reasons stated in paragraph (b)(1) of this section.

(4) From subsection (e)(5) is justified for the reasons stated in paragraph (b)(1) of this section.

[Order No. 005-2003, 68 FR 4929, Jan. 31, 2003]

## § 16.80

## 28 CFR Ch. I (7-1-24 Edition)

### § 16.80 Exemption of Office of Professional Responsibility System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f) and (g):

(1) Office of Professional Responsibility Record Index (JUSTICE/OPR-001).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of the disclosure accounting would enable the subject of an investigation to gain information concerning the existence, nature and scope of the investigation and seriously hamper law enforcement efforts.

(2) From subsections (c)(4), (d), (e)(4)(G) and (H), (f) and (g) because these provisions concern individual access to records and such access might compromise ongoing investigations, reveal confidential informants and constitute unwarranted invasions of the personal privacy of third persons who provide information in connection with a particular investigation.

(3) From subsections (e)(1) and (5) because the collection of information during an investigation necessarily involves material pertaining to other persons or events which is appropriate in a thorough investigation, even though portions thereof are not ultimately connected to the person or event subject to the final action or recommendation of the Office of Professional Responsibility.

(4) From subsection (e)(2) because collecting the information from the subject would thwart the investigation by placing the subject on notice of the investigation.

(5) From subsections (e)(3) and (e)(8) because disclosure and notice would provide the subject with substantial information which could impede or compromise the investigation. For example, an investigatory subject occupying a supervisory position could, once made aware that a misconduct inves-

tigation was ongoing, put undue pressure on subordinates so as to preclude their cooperation with investigators.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).

(1) Freedom of Information/Privacy Act (FOI/PA) Records (JUSTICE/OPR-002).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigations and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by OPR.

(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment

**Department of Justice****§ 16.81**

of the records would interfere with ongoing investigations and law enforcement activities and impose an enormous administrative burden by requiring investigations to be continuously reinvestigated.

[Order No. 58-81, 46 FR 3509, Jan. 15, 1981, as amended by Order No. 159-99, 64 FR 17977, Apr. 13, 1999]

**§ 16.81 Exemption of United States Attorneys Systems—limited access.**

(a) The following systems of records are exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Citizen Complaint Files (JUSTICE/USA-003).

(2) Civil Case Files (JUSTICE/USA-005).

(3) Consumer Complaints (JUSTICE/USA-006).

(4) Criminal Case Files (JUSTICE/USA-007).

(5) Kline-District of Columbia and Maryland-Stock and Land Fraud Interrelationship Filing System (JUSTICE/USA-009).

(6) Major Crimes Division Investigative Files (JUSTICE/USA-010).

(7) Prosecutor's Management Information System (PROMIS) (JUSTICE/USA-011).

(8) United States Attorney, District of Columbia Superior Court Division, Criminal Files (JUSTICE/USA-013).

(9) Pre-trial Diversion Program Files (JUSTICE/USA-014).

These exemptions apply to the extent that information in these systems is subject to exemption pursuant to U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for these systems, would permit the subject of a criminal investigation and/or civil case or matter under investigation, litigation, regulatory or administrative review or action, to obtain valuable information concerning the nature of that investigation, case or matter and present a serious impediment to law enforcement or civil legal activities.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in these systems would inform the subject of criminal investigation and/or civil investigation, matter or case of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection, apprehension or legal obligations, and present a serious impediment to law enforcement and other civil remedies.

(4) From subsection (e)(1) because in the course of criminal investigations and/or civil investigations, cases or matters, the U.S. Attorneys often obtain information concerning the violation of laws or civil obligations other than those relating to an active case or matter. In the interests of effective law enforcement and civil litigation, it is necessary that the U.S. Attorneys retain this information since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought within the U.S. Attorneys' offices.

(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection, apprehension or legal obligations and duties.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because these systems of records

## § 16.81

## 28 CFR Ch. I (7-1-24 Edition)

are exempt from individual access pursuant to subsections (j) and (k) of the Privacy Act of 1974.

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the United States Attorneys' ability to issue subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (f) because these systems of records have been exempted from the access provisions of subsection (d).

(11) From subsection (g) because these systems of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(c) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Freedom of Information Act/Privacy Act Files (JUSTICE/USA-008)

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(d) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit the subject of a criminal investigation and/or civil case or mat-

ter under investigation, in litigation, or under regulatory or administrative review or action to obtain valuable information concerning the nature of that investigation, case or matter, and present a serious impediment to law enforcement or civil legal activities.

(2) From subsection (c)(4) because an exemption is being claimed for subsection (d) of the Act (Access to Records), rendering this subsection inapplicable to the extent that this system of records is exempted from subsection (d).

(3) From subsection (d) because access to the records contained in these systems would inform the subject of a criminal or civil investigation, matter or case of the existence of such, and provide the subject with information that might enable him to avoid detection, apprehension or legal obligations, and present a serious impediment to law enforcement and other civil remedies. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because in the course of criminal investigations and/or civil investigations, cases or matters, the U.S. Attorneys often obtain information concerning the violation of laws or civil obligations other than those relating to an active case or matter. In the interests of effective law enforcement and civil litigation, it is necessary that the U.S. Attorneys retain this information since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought within the U.S. Attorneys' offices.

(5) From subsection (e)(2) because to collect information to the greatest extent possible from the subject individual of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations and duties.

(6) From subsection (e)(3) because to provide individuals supplying information with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information, and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because this system of records is exempt from the individual access provisions of subsection (d) and the rules provisions of subsection (f).

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would inhibit the ability of trained investigator and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the U.S. Attorneys' ability to issue subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (f) because this system has been exempted from the individual access provisions of subsection (d).

(11) From subsection (g) because the records in this system are generally compiled for law enforcement purposes and are exempt from the access provisions of subsections (d) and (f), rendering subsection (g) inapplicable.

(e) The following systems of records are exempt from 5 U.S.C. 552a(d)(1) and (e)(1):

(1) Assistant U.S. Attorneys Applicant Records System (JUSTICE/USA-016).

(2) Appointed Assistant U.S. Attorneys Personnel System (JUSTICE/USA-017).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for an Assistant U.S. Attorney position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department of Justice. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate for a position which assists in determining whether that candidate should be nominated for appointment.

(g)–(h) [Reserved]

(i) Consistent with the legislative purpose of the Privacy Act of 1974, the Executive Office for United States Attorneys will grant access to nonexempt material in records which are maintained by the U.S. Attorneys. Disclosure will be governed by the Department's Privacy regulations, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal, civil or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever

## § 16.82

## 28 CFR Ch. I (7-1-24 Edition)

possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 716-77, 42 FR 23506, May 9, 1977; Order No. 738-77, 42 FR 38177, July 27, 1977; Order No. 6-86, 51 FR 15476, Apr. 24, 1986; Order No. 57-91, 56 FR 58306, Nov. 19, 1991; Order No. 224-2001, 66 FR 17809, Apr. 4, 2001; Order No. 008-2015, 80 FR 34051, June 15, 2015]

### § 16.82 Exemption of the National Drug Intelligence Center Data Base—limited access.

(a) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4); (d); (e) (1), (2), and (3); (e)(4)(I); (e) (5) and (8); and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) and (e)(4)(I) of 5 U.S.C. 552a:

(1) National Drug Intelligence Center Data Base (JUSTICE/NDIC-001).

(2) [Reserved]

(b) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the National Drug Intelligence Center (NDIC). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) for the same reasons that the system is exempted from the provisions of subsection (d).

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsection (j)(2) of the Privacy Act.

(3) From subsection (d) because disclosure to the subject could alert the

subject of an investigation pertaining to narcotic trafficking or related activity of the fact and nature of the investigation, and/or of the investigative interest of NDIC and other intelligence or law enforcement agencies (including those responsible for civil proceedings related to laws against drug trafficking); lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life and safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Finally, access to records could result in the release of properly classified information that could compromise the national defense or foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because, in the course of its acquisition, collation, and analysis of information, NDIC will need to retain information not immediately shown to be relevant to counterdrug law enforcement to establish patterns of activity and to assist other agencies charged with the enforcement of laws and regulations regarding drug trafficking and charged with the acquisition of intelligence related to international aspects of drug trafficking. This consideration applies equally to information acquired from, or collated or analyzed for, both law enforcement agencies and agencies of the U.S. foreign intelligence community.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to law enforcement in that it would put the subject of an investigation, study or analysis on notice of the fact of such

investigation, study, or analysis, thereby permitting the subject to engage in conduct intended to frustrate the activity; because, in some circumstances, the subject of an investigation may not be required to provide to investigators certain information; and because thorough analysis and investigation may require seeking information from a number of different sources.

(6) From subsection (e)(3) (to the extent applicable) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation and reveal the identity of confidential informants and endanger their lives and safety.

(7) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than have been published in the *FEDERAL REGISTER*. Should the subsection be so interpreted, exemption from this provision is necessary to protect the confidentiality of the sources of criminal and other law enforcement information and to protect the privacy and physical safety of witnesses and informants. Furthermore, greater specificity concerning the sources of properly classified records could compromise national defense or foreign policy.

(8) From subsection (e)(5) because the acquisition, collation, and analysis of information for law enforcement purposes does not permit advance determination whether such information is accurate or relevant, nor can such information be limited to that which is complete or apparently timely. Information of this type often requires further analysis and investigation to develop into a comprehensive whole that which is otherwise incomplete or even fragmentary. Moreover, its accuracy is continually subject to analysis and review, and, upon careful examination, seemingly irrelevant or untimely information may acquire added significance as additional information brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exer-

cise their judgment in collating and analyzing information and would impede the development of criminal intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement by revealing investigative techniques, procedures, or evidence.

(10) From subsection (g) to the extent that the system is exempt from subsection (d).

[Order No. 78-93, 58 FR 41038, Aug. 2, 1993]

**§ 16.83 Exemption of the Executive Office for Immigration Review System—limited access.**

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) The Executive Office for Immigration Review's Records and Management Information System (JUSTICE/EOIR-001).

This exemption applies only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1) and (2).

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsection (d) because access to information which has been properly classified pursuant to an Executive Order could have an adverse effect on the national security. In addition, from subsection (d) because unauthorized access to certain investigatory material could compromise ongoing or potential investigations; reveal the identity of confidential informants; or constitute unwarranted invasions of the personal privacy of third parties.

(2) From subsection (d) (2), (3), and (4) because the record of proceeding constitutes an official record which includes transcripts of quasi-judicial administrative proceedings, investigatory materials, evidentiary materials such as exhibits, decisional memoranda, and other case-related papers. Administrative due process could not be achieved by the *ex parte* "correction" of such materials by the individual who is the subject thereof.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).

## § 16.83

## 28 CFR Ch. I (7-1-24 Edition)

(1) Practitioner Compliant/Disciplinary Files (JUSTICE/EOIR 003). This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigations and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law or regulatory enforcement process, the applicable exemption may be waived by the Executive Office for Immigration Review.

(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of the investigation of an actual or potential criminal, civil, or regulatory violation or the existence of that investigation; of the nature and scope of the information and evidence obtained as to the subject's activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law and regulatory enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an enormous administra-

tive burden by requiring investigations to be continuously reinvestigated.

(e) The following system of records is exempt from 5 U.S.C. 552a(d): Office of the Chief Administrative Hearing Officer (OCAHO) Case Management System (CMS) (JUSTICE/EOIR-002). This exemption applies only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1) and (2).

(f) Exemption from 5 U.S.C. 552a(d) is justified for the system of records in paragraph (e) of this section for the following reasons:

(1) In limited circumstances, from subsection (d) when access to the records contained in the system of records in paragraph (e) of this section could inform the subject of an ongoing investigation of an actual or potential criminal, civil, or regulatory violation or the existence of that investigation; of the nature and scope of the information and evidence obtained as to the subject's activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law and regulatory enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel; and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties.

(2) From subsections (d)(2), (3), and (4) because the administrative case files constitute an official record which includes transcripts of administrative proceedings, investigatory materials, evidentiary materials such as exhibits, decisional memoranda, and other case-related papers. Administrative due process could not be achieved by the ex parte "correction" of such materials

**Department of Justice****§ 16.85**

by the individual who is the subject thereof.

[Order No. 18-86, 51 FR 32305, Sept. 11, 1986, as amended by Order No. 180-99, 64 FR 61787, Nov. 15, 1999; Order No. 11-2019; 84 FR 64200, Nov. 21, 2019]

**§ 16.84 Exemption of Immigration Appeals System.**

(a) The following system of records is exempt from 5 U.S.C. 552a(d) (2), (3) and (4):

(1) Decisions of the Board of Immigration Appeals (JUSTICE/BIA-001).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (d) (2), (3) and (4) because the decisions reflected constitute official records of opinions rendered in quasi-judicial proceedings. Administrative due process could not be achieved by the ex parte "correction" of such opinions by the subject of the opinion.

**§ 16.85 Exemption of U.S. Parole Commission—limited access.**

(a) The following systems of records are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e)(8), (f) and (g):

(1) Docket Scheduling and Control System (JUSTICE/PRC-001).

(2) Inmate and Supervision Files System (JUSTICE/PRC-003).

(3) Labor and Pension Case, Legal File, and General Correspondence System (JUSTICE/PRC-004).

(4) Statistical, Educational and Developmental System (JUSTICE/PRC-006).

(5) Workload Record, Decision Result, and Annual Report System (JUSTICE/PRC-007).

These exemptions apply only to the extent that information in these systems is subject to exemptions pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because revealing disclosure of accountings to in-

mates and persons on supervision could compromise legitimate law enforcement activities and U.S. Parole Commission responsibilities.

(2) From subsection (c)(4) because the exemption from subsection (d) will make notification of disputes inapplicable.

(3) From subsection (d) because this is essential to protect internal processes by which Commission personnel are able to formulate decisions and policies with regard to federal prisoners and persons under supervision, to prevent disclosures of information to federal inmates or persons on supervision that would jeopardize legitimate correctional interests of security, custody, supervision, or rehabilitation, to permit receipt of relevant information from other federal agencies, state and local law enforcement agencies, and federal and state probation and judicial offices, to allow private citizens to express freely their opinions for or against parole, to allow relevant criminal history type information of co-defendants to be kept in files, to allow medical, psychiatric and sociological material to be available to professional staff, and to allow a candid process of fact selection, opinion formulation, evaluation and recommendation to be continued by professional staff. The legal files contain case development material and, in addition to other reasons, should be exempt under the attorney-client privilege. Each labor or pension applicant has had served upon him the material in his file which he did not prepare and may see his own file at any time.

(4) From subsection (e)(2) because primary collection of information directly from federal inmates or persons on supervision about criminal sentence, criminal records, institutional performance, readiness for release from custody, or need to be returned to custody is highly impractical and inappropriate.

(5) From subsection (e)(3) because application of this provision to the operations and collection of information by the Commission which is primarily from sources other than the individual, is inappropriate.

(6) From subsections (e)(4) (G) and (H) because exemption from the access

## § 16.88

## 28 CFR Ch. I (7-1-24 Edition)

provisions of (d) makes publication of agency procedures under (d) inapplicable.

(7) From subsection (e)(8) because the nature of the Commission's activities renders notice of compliance with compulsory legal process impractical.

(8) From subsection (f) because exemption from the provisions of subsection (d) will render compliance with provisions of this subsection inapplicable.

(9) From subsection (g) because exemption from the provisions of subsection (d) will render the provisions on suits to enforce (d) inapplicable.

(c) Consistent with the legislative purpose of the Privacy Act of 1974 the U.S. Parole Commission will initiate a procedure whereby present and former prisoners and parolees may obtain copies of material in files relating to them that are maintained by the U.S. Parole Commission. Disclosure of the contents will be affected by providing copies of documents to requesters through the mails. Disclosure will be made to the same extent as would be made under the substantive exemptions of the Parole Commission and Reorganization Act of 1976 (18 U.S.C. 4208) and Rule 32 of the Federal Rules of Criminal Procedure. The procedure relating to disclosure of documents may be changed generally in the interest of improving the Commission's system of disclosure or when required by pending or future decisions and directions of the Department of Justice.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 14-78, 43 FR 45993, Oct. 5, 1978; Order No. 899-80, 45 FR 43703, June 30, 1980; Order No. 6-86, 51 FR 15477, Apr. 24, 1986]

### § 16.88 Exemption of Antitrust Division Systems—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(4) (G) and (H), and (f):

(1) Antitrust Caseload Evaluation System (ACES)—Monthly Report (JUSTICE/ATR-006).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because information in this system is maintained in aid of ongoing antitrust enforcement investigations and proceedings. The release of the accounting of disclosures made under subsection (b) of the Act would permit the subject of an investigation of an actual or potential criminal or civil violation to determine whether he is the subject of an investigation. Disclosure of the accounting would therefore present a serious impediment to antitrust law enforcement efforts.

(2) From subsection (d) because access to the information retrievable from this system and compiled for law enforcement purposes could result in the premature disclosure of the identity of the subject of an investigation of an actual or potential criminal or civil violation and information concerning the nature of that investigation. This information could enable the subject to avoid detection or apprehension. This would present a serious impediment to effective law enforcement since the subject could hinder or prevent the successful completion of the investigation. Further, confidential business and financial information, the identities of confidential sources of information, third party privacy information, and statutorily confidential information such as grand jury information must be protected from disclosure.

(3) From subsections (e)(4)(G) and (H), and (f) because this system is exempt from the individual access provisions of subsection (d).

(c) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(4)(G) and (H), and (f):

(1) Freedom of Information/Privacy—Requester/Subject Index File (JUSTICE/ATR-008).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(d) Because this system contains Department of Justice civil and criminal law enforcement, investigatory

**Department of Justice****§ 16.89**

records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the accounting of disclosures made under subsection (b) of the Act would permit the subject of an investigation of an actual or potential criminal or civil violation to determine whether he is the subject of an investigation. Disclosure of accounting would therefore present a serious impediment to antitrust law enforcement efforts.

(2) From subsection (d) because access to information in this system could result in the premature disclosure of the identity of the subject of an investigation of an actual or potential criminal or civil violation and information concerning the nature of the investigation. This information could enable the subject to avoid detection or apprehension. This would present a serious impediment to effective law enforcement since the subject could hinder or prevent the successful completion of the investigation. Further, confidential business and financial information, the identities of confidential sources of information, third party privacy information, and statutorily confidential information such as grand jury information must be protected from disclosure.

(3) From subsections (e)(4)(G) and (H), and (f) because this system is exempt from the individual access provisions of subsection (d).

[Order No. 2-86, 51 FR 884, Jan. 9, 1986]

**§ 16.89 Exemption of Civil Division Systems—limited access.**

(a) The following systems of records are exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4) (G) and (H), (e)(5), (e)(8), and (g); in addition, the following systems of records are exempted pursuant to 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4) (G) and (H):

(1) Civil Division Case File System, JUSTICE/CIV-001.

(2) Freedom of Information/Privacy Acts File System, JUSTICE/CIV-005.

These exemptions apply only to the extent that information in these systems

is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) Only that information which relates to the investigation, prosecution, or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy is exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3).* To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him or her would inform that individual (and others to whom the subject might disclose the records) of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and others to avoid criminal penalties and civil remedies.

(2) *Subsections (c)(4), (e)(4) (G) and (H), and (g).* These provisions are inapplicable to the extent that these systems of records are exempted from subsection (d).

(3) *Subsection (d).* To the extent that information contained in these systems has been properly classified, relates to the investigation and/or prosecution of grand jury, civil fraud, and other law enforcement matters, disclosure could compromise matters which should be kept secret in the interest of national security or foreign policy; compromise confidential investigations or proceedings; hamper sensitive civil or criminal investigations; impede affirmative enforcement actions based upon alleged violations of regulations or of civil or criminal laws; reveal the identity of confidential sources; and result in unwarranted invasions of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously re-investigated.

(4) *Subsection (e)(1).* In the course of criminal or civil investigations, cases, or matters, the Civil Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law

## § 16.89

## 28 CFR Ch. I (7-1-24 Edition)

enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.

(5) *Subsection (e)(2).* To collect information from the subject of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject (and others to whom the subject might be in contact) would be informed of the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) *Subsection (e)(3).* To comply with this requirement during the course of a criminal investigation or prosecution could jeopardize the investigation by disclosing the existence of a confidential investigation, revealing the identity of witnesses or confidential informants, or impeding the information gathering process.

(7) *Subsection (e)(5).* In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(8) *Subsection (e)(8).* To serve notice would give persons sufficient warning to evade law enforcement efforts.

(c) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1) and (e)(5); in addition, this system is also exempted pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d), and (e)(1).

Consumer Inquiry/Investigatory System,  
JUSTICE/CIV-006.

These exemptions apply only to the extent that information in this system of

records is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(d) Only that information compiled for criminal or civil law enforcement purposes is exempted for the reasons set forth from the following subsections:

(1) *Subsections (c)(3).* This system occasionally contains investigatory material based on complaints of actual or alleged criminal or civil violations. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him/her would inform that individual of the existence, nature, or scope of that investigation, and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties and civil remedies.

(2) *Subsections (c)(4).* This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d).* Disclosure of information relating to the investigation of complaints of alleged violation of criminal or civil law could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously re-investigated.

(4) *Subsection (e)(1).* In the course of criminal or civil investigations, cases, or matters, the Civil Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.

(5) *Subsection (e)(5).* In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of

**Department of Justice****§ 16.90**

the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(e) The following system of records is exempt pursuant to 5 U.S.C. 552a (j)(2) and (k)(2) from subsection (d):

Congressional and Citizen Correspondence File, JUSTICE/CIV-007.

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C 552a (j)(2) and (k)(2).

(f) Only that portion of the Congressional and Citizen Correspondence File maintained by the Communications Office which consists of criminal or civil investigatory information is exempted for the reasons set forth from the following subsection:

(1) *Subsection (d).* Disclosure of investigatory information would jeopardize the integrity of the investigative process, disclose the identity of individuals who furnished information to the government under an express or implied promise that their identities would be held in confidence, and result in an unwarranted invasion of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

[Order No. 27-88, 54 FR 113, Jan. 4, 1989]

**§ 16.90 Exemption of Civil Rights Division Systems.**

(a) The following system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j) and (k): Central Civil Rights Division Index File and Associated Records (JUSTICE/CRT-001). These exemptions apply only to the extent that information in a

record is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) *Subsection (c)(3).* To provide the subject of a criminal, civil, or administrative matter or case under investigation with an accounting of disclosures of records concerning him or her could inform that individual of the existence, nature, or scope of an actual or potential criminal or civil violation to gain valuable information concerning the nature and scope of the investigation, to determine whether he or she is the subject of the investigation, and seriously impede law enforcement efforts by permitting the record subject and other persons to whom he or she might disclose the records to avoid criminal penalties, civil remedies, or administrative measures.

(2) *Subsection (c)(4).* This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d)(1).* Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Disclosure of classified national security information would cause damage to the national security of the United States. In addition, these records may be subject to protective orders entered by federal courts to protect their confidentiality. Further, many of the records contained in this system are copies of documents which are the property of state agencies and were obtained under express or implied promises to strictly protect their confidentiality.

(4) *Subsection (d)(2).* Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) *Subsection (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

## § 16.91

## 28 CFR Ch. I (7-1-24 Edition)

(6) *Subsection (e)(1).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2).* To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigation.

(8) *Subsection (e)(3).* To inform individuals as required by this subsection could reveal the existence of a criminal or civil investigation and compromise investigative efforts.

(9) *Subsection (e)(5).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8).* To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g).* This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(c) The following system of records is exempted from subsections (d)(1), (2), (3) and (4) of the Privacy Act pursuant to 5 U.S.C. 552a (k): "Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission" (JUSTICE/CRT-007). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) *Subsection (d)(1).* Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. In addition, these records may be subject to protective orders entered by federal courts to protect their confidentiality. Further,

many of the records contained in this system are copies of documents which are the property of state agencies and were obtained under express or implied promises to strictly protect their confidentiality.

(2) *Subsection (d)(2).* Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously re-investigated.

(3) *Subsection (d)(1), (2), (3) and (4).* This system contains investigatory material compiled by the Equal Opportunity Commission pursuant to its authority under 42 U.S.C. 2000e-8. Titles 42 U.S.C. 2000e-5(b), 42 U.S.C. 2000e-8(e), and 44 U.S.C. 3508 make it unlawful to make public in any manner whatsoever any information obtained by the Commission pursuant to the authority.

(4) *Subsection (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

[Order No. 019-2003, 68 FR 61622, Oct. 29, 2003]

### § 16.91 Exemption of Criminal Division Systems—limited access, as indicated.

(a) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a; in addition, the following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of 5 U.S.C. 552a:

(1) Central Criminal Division, Index File and Associated Records System of Records (JUSTICE/CRM-001)—Limited Access. This system of records and associated exemptions is adopted by and applies with equal force and effect to the National Security Division, until modified, superseded, or revoked in accordance with law.

(2) General Crimes Section, Criminal Division, Central Index File and Associated Records System of Records (JUSTICE/CRM-004)—Limited Access.

These exemptions apply to the extent that information in those systems are

subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) The systems of records listed under paragraphs (b)(1) and (b)(2) of this section are exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3). (d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, or the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4). (e)(1). The notices of these systems of records published in the FEDERAL REGISTER set forth the basic stat-

utory or related authority for maintenance of this system. However, in the course of criminal or other law enforcement investigations, cases, and matters, the Criminal Division or its components will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(5). (e)(2). In a criminal investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6). (e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that these systems of records are exempted from subsections (f) and (d).

(8). (e)(4)(I). The categories of sources of the records in these systems have been published in the FEDERAL REGISTER in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of

## § 16.91

## 28 CFR Ch. I (7-1-24 Edition)

the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9). (e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10). (e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal, civil, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules require pursuant to subsection (f) (2) through (5) are inap-

plicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(12). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(13). In addition, exemption is claimed for these systems of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): Subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in these systems are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(c) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j) (2) from subsection (c) (3) and (4), (d), (e) (1), (2) and (3), (e) (4) (G), (H) and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a:

Criminal Division Witness Security File System of Records(JUSTICE/CRM-002).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(d) The system of records listed under paragraph (c) of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(8) The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, to determine whether he is the subject of a criminal investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, or the identity of witnesses and informants and the nature of their reports, and would therefore present a serious impediment to law

enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records. Moreover, disclosure of the disclosure accounting to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to obtain, and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

(2). (c)(4) Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d) Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, access to the records in these systems to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to obtain, and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

(4). Exemption is claimed from subsection (e)(1) for the reasons stated in subsection (b)(4) of this section.

(5). (e)(2) In the course of preparing a Witness Security Program for an indi-

vidual, much of the information is collected from the subject. However, the requirement that the information be collected to the greatest extent practicable from the subject individual would present a serious impediment to criminal law enforcement because the individual himself may be the subject of a criminal investigation or have been a participant in, or observer of, criminal activity. As a result, it is necessary to seek information from other sources. In addition, the failure to verify the information provided from the individual when necessary and to seek other information could jeopardize the confidentiality of the Witness Security Program and lead to the obtaining and maintenance of incorrect and uninvestigated information on criminal matters.

(6). (e)(3) The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise or reveal the identity of witnesses and informants protected under the Witness Security Program.

(7). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable.

(8). (e)(4)(I). The categories of sources of the records in these systems have been published in the FEDERAL REGISTER in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in the system, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal law, enforcement information and of witnesses and informants protected under the Witness Security Program.

(9). Exemption is claimed from subsections (e)(5) and (e)(8) for the reasons stated in subsection (b)(9) and (b)(10) of this section.

(10). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records contained in these systems pertaining to him would

## § 16.91

## 28 CFR Ch. I (7-1-24 Edition)

inform the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful conduct and/or completion of an investigation pending or future, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, notices as to the existence of records contained in these systems to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to obtain, and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable.

(11. (g) Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable and is exempted for the reasons set forth for those subsections.

(e) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (4) (G), (H) and (I), (f), and (g) of 5 U.S.C. 552a:

Organized Crime and Racketeering Section, Intelligence and Special Services Unit, Information Request System of Records (JUSTICE/CRM-014).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(f) The system of records listed under paragraph (e) of this section is exempted for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation to determine whether he is the subject of a criminal investigation and would therefore present a serious impediment to law enforcement. The records in these systems contain the names of the subjects of the files in question and the system is accessible by name of the person checking out the file and by name of the subject of the file. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation. This would present a serious impediment to effective law enforcement because it could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4). Exemption is claimed from subsections (e)(4) (G), (H) and (I) for the reasons stated in subsections (b)(7) and (b)(8) of this section.

(5). (f). These systems may be accessed by the name of the person who is the subject of the file and who may also be the subject of a criminal investigation. Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him, which may deal with an actual or potential criminal investigation or prosecution, must be exempted

because such notice to an individual would be detrimental to the successful conduct and/or completion of the investigation or prosecution pending or future. In addition mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable.

(6). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) of the Act this section is inapplicable and is exempted for the reasons set forth for those subsections.

(g) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(4), (d), (e)(4) (G), (H) and (I), (f) and (g) of 5 U.S.C. 552a.

File of Names Checked to Determine If Those Individuals Have Been the Subject of an Electronic Surveillance System of Records (JUSTICE/CRM-003).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(h) The system of records listed under paragraph (g) of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable to the extent that this system of records is exempted from subsection (d).

(2). (d). The records contained in this system of records generally consist of information filed with the court in response to the request and made available to the requestor. To the extent that these records have been so filed, no exemption is sought from the provisions of this subsection. Occasionally, the records contain pertinent logs of intercepted communications and other

investigative reports not filed with the court. These records must be exempted because access to such records could inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation and of the nature of the information and evidence obtained by the government. This would present a serious impediment to effective law enforcement because it could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(3). Exemption is claimed from subsections (e)(4) (G), (H) and (I) for the reasons stated in subsections (b)(7) and (b)(8) of this section.

(4). (f). The records contained in this system of records generally consist of information filed with the court and made available to the requestor. To the extent that these records have been so filed, no exemption is sought from the provisions of this subsection. Occasionally, the records contain pertinent logs of intercepted communications and other investigative reports not filed with the court. These records must be exempted from a requirement of notification as to their existence because such notice to an individual would be detrimental to the successful conduct and/or completion of a criminal investigation or prosecution pending or future. In addition, mere notice of the existence of such logs or investigative reports could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable to the extent that this system of records is exempted for subsection (d).

(6). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted

## § 16.91

## 28 CFR Ch. I (7-1-24 Edition)

for the reasons set forth for those subsections, to the extent that this system of records is exempted from subsections (d) and (f).

(i) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2), and (3), (e)(4) (G), (H), and (I), (e) (5) and (8), (f) and (g) of 5 U.S.C. 552a:

(1) Information File on Individuals and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities System of Records (JUSTICE/CRM-006).

(2) The Stocks and Bonds Intelligence Control Card File System of Records (JUSTICE/CRM-021).

(3) Tax Disclosure Index File and Associated Records (JUSTICE/CRM-025).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(j) The systems of records listed in paragraphs (i)(1), (i)(2), and (i)(3) of this section are exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3) The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation to determine whether he is the subject of a criminal investigation, to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for this system of records.

(2)(c)(4) Since an exemption is being claimed for subsection (d) of the act (access to records), this section is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3)(d) Access to the records contained in these systems would inform the subject of an investigation of an actual or

potential criminal violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4) Exemption is claimed from subsections (e) (1), (2), and (3), (e)(4) (G), (H), and (I), (e)(5) and (e)(8) for the reasons stated in subsections (b)(4), (b)(5), (b)(6), (b)(7), (b)(8), (b)(9), and (b)(10) of this section.

(5)(f) Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Since an exemption is being claimed for subsection (d) of the act (access to records), the rules required pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records.

(6)(g) Since an exemption is being claimed for subsections (d) (access to records) and (f) (Agency rules), this section is inapplicable and is exempted for the reasons set forth for those subsections.

(k) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f) and

**Department of Justice****§ 16.91**

(g) of 5 U.S.C. 552a; in addition, the following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) from subsections (c) (3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) of 5 U.S.C. 552a:

Organized Crime and Racketeering Section, Criminal Division, General Index File and Associated Records System of Records (JUSTICE/CRM-012).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(1).

(1) The system of records listed under paragraph (m)<sup>1</sup> of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). Exemption is claimed from subsections (c) (3) and (4) and (d) for the reasons stated in subsections (j)(1), (j)(2) and (j)(3) of this section.

(2). (e)(1). The notice for this system of records published in the FEDERAL REGISTER sets forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal investigations, cases, and matters, the Organized Crime and Racketeering Section will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority, or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in this system of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(3). Exemption is claimed from subsections (e) (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f) and (g) for the reasons stated in subsections (b)(5), (b)(6), (b)(7), (b)(8), (b)(9), (b)(10), (b)(11) and (b)(12) of this section.

(4). In addition, exemption is claimed for this system of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a)

pursuant to the provisions of 5 U.S.C. 552a(k)(1): Subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in this system are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(m) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (2) and (3), (e) (4) (G), (H) and (I), (e) (8), (f) and (g) of 5 U.S.C. 552a:

Requests to the Attorney General For Approval of Applications to Federal Judges For Electronic Interceptions System of Records (JUSTICE/CRM-019).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(n) The system of records listed in paragraph (m) of this section is exempted for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an electronic interception to obtain valuable information concerning the interception, including information as to whether he is the subject of a criminal investigation, by means other than those provided for by statute. Such information could interfere with the successful conduct and/or completion of a criminal investigation, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d). Access to the records contained in these systems would inform the subject of an electronic interception of the existence of such surveillance including information as to

<sup>1</sup>Paragraph (m) was redesignated as paragraph (k) at 44 FR 54046, Sept. 18, 1979.

## § 16.91

## 28 CFR Ch. I (7-1-24 Edition)

whether he is the subject of a criminal investigation by means other than those provided for by statute. This could interfere with the successful conduct and/or completion of a criminal investigation and therefore present a serious impediment to law enforcement.

(4). (e)(2). In the context of an electronic interception, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and this would therefore destroy the efficacy of the interception.

(5). (e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential electronic interception or reveal the identity of witnesses or confidential informants.

(6). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable.

(7). Exemption is claimed from subsections (e)(4)(I) and (e)(8) for the reasons stated in subsections (b)(8) and (b)(10) of this section.

(8). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an electronic interception other than pursuant to statute must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation pending or future. In addition, mere notice of the fact of an electronic interception could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to

subsection (f)(2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(9). (g). Since an exemption is being claimed for subsection (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsection (d) and (f).

(o) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (2) and (3), (e) (4) (G), (H), and (I), (e)(8), (f) and (g) of 5 U.S.C. 552a; in addition the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), (e)(4) (G), (H) and (I), and (f) of 5 U.S.C. 552a:

Witness Immunity Records System of Records (JUSTICE/CRM-022).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(1) and (k)(2).

(p) The system of records listed under paragraph (q)<sup>2</sup> of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). Release of the accounting of disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for this system of records, (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus creating a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activities, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

<sup>2</sup> Paragraph (q) was redesignated as paragraph (o) at 44 FR 54046, Sept. 18, 1979.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable to the extent that this system of records is exempted from subsection (d).

(3). (d). Access to the records contained in this system (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus presenting a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activities, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

(4). (e)(2). In a witness immunity request matter, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the immunity request and often the subject of the underlying investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(5). Exemption is claimed from subsections (e)(3), (e)(4)(G), (H) and (I), and (e)(8) for the reasons stated in subsections (b)(6), (b)(7), (b)(8) and (b)(10) of this section.

(6). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus presenting a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activity, if any, of the witness known to the government, which

would also create a serious impediment to effective law enforcement.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f)(2) through (5) are inapplicable to this system of records to the extent that this system of records is exempted from subsection (d).

(7). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that this system of records is exempted for subsections (d) and (f).

(8). In addition, exemption is claimed for this system of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in this system are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(q) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f), and (g):

(1) Freedom of Information/Privacy Act Records (JUSTICE/CRM-024)

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(r) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, it is exempted for the reasons set forth from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting would present a serious impediment to law enforcement by permitting the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation and the information obtained, or to identify witnesses and informants.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act

## § 16.91

## 28 CFR Ch. I (7-1-24 Edition)

(Access to Records), this subsection is inapplicable to the extent that this system of records is exempted from subsection (d).

(3)(d). Access to records contained in this system would enable the subject of an investigation of an actual or potential criminal or civil case or regulatory violation to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature and scope of the investigation, and information or evidence obtained as to his/her activities, to identify witnesses and informants, or to avoid detection or apprehension. Such results could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony, and thereby present a serious impediment to effective law enforcement. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4)(e)(1). In the course of criminal or other law enforcement investigations, cases, and matters, the Criminal Division will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority, or it may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(5)(e)(2). To collect information to the greatest extent practicable from the subject individual of a criminal investigation or prosecution would present a serious impediment to law enforcement. The nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible

to rely upon information furnished by the individual concerning his own activities.

(6) (e)(3). To provide individuals supplying information with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). These subsections are inapplicable to the extent that this system is exempt from the access provisions of subsection (d) and the rules provisions of subsection (f).

(8)(e)(4)(I). The categories of sources of the records in this system have been published in the *FEDERAL REGISTER* in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in this system, exemption from this provision is necessary to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9) (e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would inhibit the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or

**Department of Justice****§ 16.92**

subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). This subsection is inapplicable to the extent that this system is exempt from the access provisions of subsection (d).

(12)(g). Because some of the records in this system contain information which was compiled for law enforcement purposes and have been exempted from the access provisions of subsection (d), subsection (g) is inapplicable.

(s) The following system of records is exempted from 5 U.S.C. 552a(d).

Office of Special Investigations Displaced Persons Listings (JUSTICE/CRM-027).

This exemption applies to the extent that the records in this system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(t) Exemption from subsection (d) is justified for the following reasons:

(1) Access to records contained in this system could inform the subject of the identity of witnesses or informants. The release of such information could present a serious impediment to effective law enforcement by endangering the physical safety of witnesses or informants; by leading to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony; or by otherwise preventing the successful completion of an investigation.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 659-76, 41 FR 32423, Aug. 3, 1976; Order No. 11-78, 43 FR 38386, Aug. 28, 1978; Order No. 30-79, 44 FR 54046, Sept. 18, 1979; Order No. 6-86, 7-86, 51 FR 15475, 15477, Apr. 24, 1986; Order No. 018-2004, 69 FR 72114, Dec. 13, 2004; Order No. 015-2006, 71 FR 58278, Oct. 3, 2006; Order No. 003-2009, 74 FR 42776, Aug. 25, 2009; Order No. 006-2013, 78 FR 69754, Nov. 21, 2013]

**§ 16.92 Exemption of Environment and Natural Resources Division Systems—limited access.**

(a)(1) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(5), (e)(8), (f) and (g); in addition, the following systems of records are exempted pursuant to 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1):

(i) Environment and Natural Resources Division Case and Related Files System, JUSTICE/ENRD-003.

(ii) [Reserved]

(2) These exemptions apply only to the extent that information in this system relates to the investigation, prosecution or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy, and therefore is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigations, and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law or regulatory enforcement process, the applicable exemption may be waived by the Environment and Natural Resources Division.

(b) Only that information that relates to the investigation, prosecution or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy is exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3).* Subsection (c)(3) requires an agency to provide an accounting of disclosures of records concerning an individual. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records would inform that individual (and others to whom the subject might disclose the records) of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and others to avoid criminal penalties and civil remedies.

(2) *Subsections (c)(4) (requiring an agency to inform individuals about any corrections made to a record that has been disclosed) and (g) (providing for civil remedies when an agency fails to comply with these provisions).* These provisions are inapplicable to the extent that this system of records is exempted from subsection (d).

## § 16.92

## 28 CFR Ch. I (7-1-24 Edition)

(3) *Subsection (d).* Subsection (d) requires an agency to allow individuals to gain access to a record about him or herself; to dispute the accuracy, relevance, timeliness or completeness of such records; and to have an opportunity to amend his or her record or seek judicial review. To the extent that information contained in this system has been properly classified, relates to the investigation and/or prosecution of grand jury, civil fraud, and other law enforcement matters, disclosure could compromise matters which should be kept secret in the interest of national security or foreign policy; compromise confidential investigations or proceedings; impede affirmative enforcement actions based upon alleged violations of regulations or of civil or criminal laws; reveal the identity of confidential sources; and result in unwarranted invasions of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) *Subsection (e)(1).* Subsection (e)(1) requires an agency to maintain in its records only such information about an individual that is relevant and necessary to accomplish the agency's purpose. In the course of criminal or civil investigations, cases, or other matters, the Environment and Natural Resources Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.

(5) *Subsection (e)(2).* Subsection (e)(2) requires an agency to collect information to the greatest extent practicable from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs. To collect information from the subject of a criminal investigation or prosecution would present a serious impediment to law

enforcement in that the subject (and others with whom the subject might be in contact) would be informed of the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) *Subsection (e)(3).* Subsection (e)(3) requires an agency to inform each individual whom it asks to supply information, on a form that can be retained by the individual, the authority which authorizes the solicitation, the principal purpose for the information, the routine uses of the information, and the effects on the individual of not providing the requested information. To comply with this requirement during the course of a criminal investigation or prosecution could jeopardize the investigation by disclosing the existence of a confidential investigation, revealing the identity of witnesses or confidential informants, or impeding the information gathering process.

(7) *Subsection (e)(5).* Subsection (e)(5) requires an agency to maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual. In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(8) *Subsection (e)(8).* Subsection (e)(8) requires agencies to make reasonable efforts to serve notice on an individual when any record on the individual is made available to any person under compulsory legal process. To serve notice would give persons sufficient warning to evade law enforcement efforts.

(9) *Subsections (f) and (g).* Subsection (f) requires an agency to establish procedures to allow an individual to have

**Department of Justice****§ 16.93**

access to information about him or herself and to contest information kept by an agency about him or herself. Subsection (g) provides for civil remedies against agencies who fail to comply with the Privacy Act requirements. These provisions are inapplicable to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(c) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (d):

(1) Freedom of Information/Privacy Act Records System. (Justice/LDN-005).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c) (3) because that portion of the Freedom of Information/Privacy Act Records System that consists of investigatory materials compiled for law enforcement purposes is being exempted from access and contest; the provision for disclosure of accounting is not applicable.

(2) From subsection (d) because of the need to safeguard the identity of confidential informants and avoid interference with ongoing investigations or law enforcement activities by preventing premature disclosure of information relating to those efforts.

[Order No. 688-77, 42 FR 10000, Feb. 18, 1977, as amended by Order No. 207-2000, 65 FR 75158, Dec. 1, 2000]

**§ 16.93 Exemption of Tax Division Systems—limited access.**

(a) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f) and (g) of 5 U.S.C. 552a:

(1) Tax Division Central Classification Cards, Index Docket Cards, and Associated Records—Criminal Tax Cases (JUSTICE/TAX-001)—Limited Access.

(2) These exemptions apply to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) The system of records listed under paragraph (a)(1) of this section is exempted for the reasons set forth below, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting, for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for those systems of records, would enable the subject of an investigation of an actual or potential criminal tax case to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, and to determine the identity of witnesses or informants. Such access to investigative information would, accordingly, present a serious impediment to law enforcement. In addition, disclosure of the accounting would constitute notice to the individual of the existence of a record even though such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3) (d)(1); (d)(2); (d)(3); (d)(4). Access to the records contained in these systems would inform the subject of an actual or potential criminal tax investigation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his or her activities, and of the identity of witnesses or informants. Such access would, accordingly, provide information that could enable the subject to avoid detection, apprehension and prosecution. This result, therefore, would constitute a serious impediment to effective law enforcement not only because it would prevent the successful completion of the investigation but also because it could endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4)(e)(1). The notices for these systems of records published in the FEDERAL REGISTER, set forth the basic

## § 16.93

## 28 CFR Ch. I (7-1-24 Edition)

statutory or related authority for maintenance of these systems. However, in the course of criminal tax and related law enforcement investigations, cases, and matters, the Tax Division will occasionally obtain information concerning actual or potential violations of law that may not be technically within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain some or all of such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(5)(e)(2). In a criminal tax investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, influence witnesses improperly, destroy evidence, or fabricate testimony.

(6)(e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that these systems of records are exempted from subsection (f) and (d).

(8)(e)(4)(I). The categories of sources of the records in the systems have been published in the **FEDERAL REGISTER** in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this

provision is necessary in order to protect the confidentiality of the sources of criminal tax and related law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9)(e)(5). In the collection of information for criminal tax enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. Furthermore, the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal tax information and related data necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal tax, civil tax, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion or an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records to the extent that these systems of

**Department of Justice****§ 16.93**

records are exempted from subsection (d).

(12)(g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(c) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f) of 5 U.S.C. 552a:

(1) Tax Division Central Classification Cards, Index Docket Cards, and Associated Records—Civil Tax Cases (JUSTICE/TAX-002)—Limited Access.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(d) The system of records listed under paragraph (c)(1) is exempted for the reasons set forth below, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting, for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for this system of records, would enable the subject of an investigation of an actual or potential civil tax case to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, and to determine the identity of witnesses or informants. Such access to investigative information would, accordingly, present a serious impediment to law enforcement. In addition, disclosure of the accounting would constitute notice to the individual of the existence of a record even though such notice requirement under subsection (f)(1) is specifically exempted for this system of records.

(2) (d)(1); (d)(2); (d)(3); (d)(4). Access to the records contained in this system would inform the subject of an actual or potential civil tax investigation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his or her activities and of the identity of

witnesses or informants. Such access would, accordingly, provide information that could enable the subject to avoid detection. This result, therefore, would constitute a serious impediment to effective law enforcement not only because it would prevent the successful completion of the investigation but also because it could endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(3)(e)(1). The notices for this system of records published in the FEDERAL REGISTER set forth the basic statutory or related authority for maintenance of this system. However, in the course of civil tax and related law enforcement investigations, cases and matters, the Tax Division will occasionally obtain information concerning actual or potential violations of law that are not strictly or technically within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific case. In the interests of effective law enforcement, it is necessary to retain some or all of such information in this system of records since it can aid in establishing patterns of tax compliance and can provide valuable leads for Federal and other law enforcement agencies.

(4)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that this system of records is exempted from subsection (f) and (d).

(5)(e)(4)(I). The categories of sources of the records in this system have been published in the FEDERAL REGISTER in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in this system, exemption from this provision is necessary in order to protect the confidentiality of the sources of civil tax and related law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

(6)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to existence of records pertaining to the individual dealing with an actual or potential criminal tax, civil tax, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or case, pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsection (f) (2) through (5) are inapplicable to this system of records to the extent that this system of records is exempted from subsection (d).

(e) The following system of records is exempt from subsections (c)(3) and (d)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5): Files of Applicants for Attorney and Non-Attorney Positions with the Tax Division, Justice/TAX-003. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(f) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because an accounting could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a position with the Tax Division. Disclosure of an accounting could reveal the identity of a source of information and constitutes a breach of the promise of confidentiality by the Tax Division. This would result in the reduction in the free flow of information vital to a determination of an applicant's qualifications and suitability for federal employment.

(2) From subsection (d)(1) because disclosure of records in the system could reveal the identity of confidential

tial sources and result in an unwarranted invasion of the privacy of others. Many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a Tax Division position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Tax Division. Such breaches ultimately would restrict the free flow of information vital to a determination of an applicant's qualifications and suitability.

[Order No. 742-77, 42 FR 40906, Aug. 12, 1977, as amended by Order No. 6-86, 51 FR 15478, Apr. 24, 1986; Order No. 003-2006, 71 FR 11309, Mar. 7, 2006]

### **§ 16.96 Exemption of Federal Bureau of Investigation Systems—limited access.**

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g):

(1) Central Records System (CRS) (JUSTICE/FBI-002).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552(j) and (k). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by the FBI.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.

(2)(i) From subsections (d), (e)(4)(G) and (H), (f) and (g) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information classified in the interest of national security, interfere with the

**Department of Justice****§ 16.96**

overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety to law enforcement personnel.

(ii) Also, individual access to non-criminal investigative records, e.g., civil investigations and administrative inquiries, as described in subsection (k) of the Privacy Act, could also compromise classified information related to national security, interfere with a pending investigation or internal inquiry, constitute an unwarranted invasion of privacy, reveal a confidential source or sensitive investigative technique, or pose a potential threat to law enforcement personnel. In addition, disclosure of information collected pursuant to an employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the objectivity or fairness of a testing or examination process.

(iii) In addition, from paragraph (d)(2) of this section, because to require the FBI to amend information thought to be incorrect, irrelevant or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(3) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) In any investigation the FBI might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

(4) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(5) From subsection (e)(3) because disclosure would provide the subject with substantial information which could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take appropriate steps to evade the investigation or flee a specific area.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

(7) From subsection (e)(8) because the notice requirements of this provision

## § 16.96

could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(c) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (m):

(1) Electronic Surveillance (Elsur) Indices (JUSTICE/FBI-006).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of accounting disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, resulting in a serious impediment to law enforcement.

(2) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) because these provisions concern an individual's access to records which concern him and such access to records in this system would compromise ongoing investigations, reveal investigatory techniques and confidential informants, and invade the privacy of private citizens who provide information in connection with a particular investigation.

(3) From subsection (e)(1) because these indices must be maintained in order to provide the information as described in the "routine uses" of this particular system.

(4) From subsections (e) (2) and (3) because compliance is not feasible given the subject matter of the indices.

(5) From subsection (e)(5) because this provision is not applicable to the indices in view of the "routine uses" of the indices. For example, it is impossible to predict when it will be necessary to utilize information in the system and, accordingly it is not possible to determine when the records are timely.

(6) From subsection (e)(8) because the notice requirement could present a serious impediment to law enforcement by revealing investigative techniques, procedures and the existence of confidential investigations.

## 28 CFR Ch. I (7-1-24 Edition)

(7) From subsection (m) for the reasons stated in subsection (b)(7) of this section.

(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2) and (3); (e)(4)(G), (H) and (I); (e)(5) and (8); (f) and (g):

(1) The Next Generation Identification (NGI) System (JUSTICE/FBI-009).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where compliance would not appear to interfere with or adversely affect the purpose of this system to detect, deter, and prosecute crimes and to protect the national security, the applicable exemption may be waived by the FBI in its sole discretion.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning the subject would specifically reveal investigative interest by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and national security efforts and may provide the record subject with the opportunity to evade or impede the investigation.

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the accounting of disclosures provision of subsection (c)(3). The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases.

(3) From subsection (d) (1), (2), (3) and (4), (e)(4)(G) and (H), (e)(8), (f) and (g) because these provisions concern individual access to and amendment of law enforcement records and compliance

and could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the FBI and/or other law enforcement agencies. Providing access could compromise sensitive law enforcement information, disclose information that would constitute an unwarranted invasion of another's personal privacy, reveal a sensitive investigative technique, provide information that would allow a subject to avoid detection or apprehension, or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, or witnesses. Also, an alternate system of access has been provided in 28 CFR 16.30 through 16.34, and 28 CFR 20.34, for record subjects to obtain a copy of their criminal history records. However, the vast majority of criminal history records concern local arrests for which it would be inappropriate for the FBI to undertake correction or amendment.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes. The relevance and utility of certain information may not always be evident until and unless it is vetted and matched with other sources of information that are necessarily and lawfully maintained by the FBI. Most records in this system are acquired from state and local law enforcement agencies and it is not possible for the FBI to review that information as relevant and necessary.

(5) From subsection (e)(2) and (3) because application of this provision could present a serious impediment to the FBI's responsibilities to detect, deter, and prosecute crimes and to protect the national security. Application of these provisions would put the subject of an investigation on notice of that fact and allow the subject an opportunity to engage in conduct intended to impede that activity or avoid apprehension. Also, the majority of criminal history records and associated biometrics in this system are collected by state and local agencies at the time of arrest; therefore it is not feasible for the FBI to collect directly from the individual or to provide notice. Those

persons who voluntarily submit fingerprints into this system pursuant to state and federal statutes for licensing, employment, and similar civil purposes receive an (e)(3) notice.

(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the **FEDERAL REGISTER**. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI.

(7) From subsection (e)(5) because in the collection of information for authorized law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With time, seemingly irrelevant or untimely information may acquire new significance when new details are brought to light. Additionally, the information may aid in establishing patterns of activity and providing criminal leads. Most records in this system are acquired from state and local law enforcement agencies and it would be impossible for the FBI to vouch for the compliance of these agencies with this provision. The FBI does communicate to these agencies the need for accurate and timely criminal history records, including criminal dispositions.

(g) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (e)(8), (f), and (g):

(1) National Crime Information Center (NCIC) (JUSTICE/FBI-001).

(2) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(G) and (K). Where the FBI determines compliance with an exempted provision would not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the FBI in its sole discretion may waive an exemption, in whole or in part; exercise of this discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectation of waiver in that matter or any other matter. As

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

a condition of discretionary waiver, the FBI in its sole discretion may impose any restrictions deemed advisable by the FBI (including, but not limited to, restrictions on the location, manner, or scope of notice, access or amendment).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal law enforcement or national security investigative interest in the individual by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and defuse any potential acts of terrorism or other potential violations of criminal law. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to circumvent the investigation (e.g., destroy evidence or flee the area to avoid investigation).

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the accounting disclosures provision of subsection (c)(3). The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases.

(3) From subsection (d), (e)(4)(G) and (H), (e)(8), (f), and (g) because these provisions concern individual access to and amendment of law enforcement and intelligence records and compliance could alert the subject of an authorized law enforcement or intelligence activity about that particular activity and the investigative interest

of the FBI and/or other law enforcement or intelligence agencies. Providing access could compromise sensitive law enforcement information; disclose information that could constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; provide information that would allow a subject to avoid detection or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, and witnesses. The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases with subjects of the information.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. Relevance and necessity are questions of judgment and timing. For example, what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(5) From subsections (e)(2) and (3) because it is not feasible to comply with these provisions given the nature of this system. The majority of the records in this system come from other federal, state, local, joint, foreign, tribal, and international agencies; therefore, it is not feasible for the FBI to collect information directly from the individual or to provide notice. Additionally, the application of this provision could present a serious impediment to the FBI's responsibilities to detect, deter, and prosecute crimes and to protect the national security. Application of these provisions would put the subject of an investigation on notice of that fact and allow the subject an opportunity to engage in conduct intended to impede that activity or avoid apprehension.

(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding

**Department of Justice****§ 16.96**

the record sources in this system than has already been published in the FEDERAL REGISTER through the SORN documentation. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI.

(7) From subsection (e)(S) because in the collection of information for authorized law enforcement and intelligence purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With time, additional facts, or analysis, information may acquire new significance. The restrictions imposed by subsection (e)(S) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. Although the FBI has claimed this exemption, it continuously works with its federal, state, local, tribal, and international partners to maintain the accuracy of records to the greatest extent practicable. The FBI does so with established policies and practices. The criminal justice and national security communities have a strong operational interest in using up-to-date and accurate records and will foster relationships with partners to further this interest.

(j) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G) and (H), (e)(5), (f) and (g):

(1) National Center for the Analysis of Violent Crime (NCAVC) (JUSTICE/FBI-015).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(k) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because providing the accounting of disclosures to the subject could prematurely reveal investigative interest by the FBI and other law enforcement agencies, there-

by providing the individual an opportunity to impede an active investigation, destroy or alter evidence, and possibly render harm to violent crime victims and/or witnesses.

(2) From subsections (d), (e)(4) (G) and (H), and (f) because disclosure to the subject could interfere with enforcement proceedings of a criminal justice agency, reveal the identity of a confidential source, result in an unwarranted invasion of another's privacy, reveal the details of a sensitive investigative technique, or endanger the life and safety of law enforcement personnel, potential violent crime victims, and witnesses. Disclosure also could prevent the future apprehension of a violent or exceptionally dangerous criminal fugitive should he or she modify his or her method of operation in order to evade law enforcement. Also, specifically from subsection (d)(2), which permits an individual to request amendment of a record, because the nature of the information in the system is such that an individual criminal offender would frequently demand amendment of derogatory information, forcing the FBI to continuously retrograde its criminal investigations in an attempt to resolve questions of accuracy, etc.

(3) From subsection (g) because the system is exempt from the access and amendment provisions of subsection (d).

(4) From subsection (e)(1) because it is not always possible to establish relevance and necessity of the information at the time it is obtained or developed. Information, the relevance and necessity of which may not be readily apparent, frequently can prove to be of investigative value at a later date and time.

(5) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

(1) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d), (e) (1), (2), and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g).

(1) FBI Counterdrug Information Indices System (CIIS) (JUSTICE/FBI-016)

(2) [Reserved]

(m) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.

(2) From subsection (c)(4) to the extent it is not applicable because an exemption is being claimed from subsection (d).

(3)(i) From subsections (d), (e)(4) (G) and (H) because these provisions concern individual access to records, compliance with which could compromise sensitive information, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(ii) In addition, from paragraph (d), because to require the FBI to amend information thought to be incorrect, irrelevant or untimely, because of the

nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4)(i) From subsection (e)(1) because it is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed otherwise. It is only after the information is assessed that its relevancy and necessity in a specified investigative activity can be established.

(iii) In any investigation the FBI might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigations or to an investigative activity under the jurisdiction of another agency.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual often can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to principally rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) because disclosure would provide the subject with information which could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take appropriate steps to evade the investigation or flee a specific area.

(7) From subsection (e)(5) because in the collection of information for law

**Department of Justice****§ 16.96**

enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(9) From subsection (f) to the extent that this system is exempt from the provisions of subsection (d).

(10) From subsection (g) to the extent that this system of records is exempt from the provisions of subsection (d).

(n) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4); (d); (e) (1), (2), and 3; (e)(4) (G) and (H); (e) (5) and (8); and (g):

(1) National DNA Index System (NDIS) (JUSTICE/FBI-017).

(2) [Reserved]

(o) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available the accounting of disclosures of records to the subject of the record would prematurely place the subject on notice of the investigative interest of law enforcement agencies, provide the subject with significant information concerning the nature of the investigation, or permit the subject to take measures to impede the investigation (e.g., destroy or alter evidence, intimidate potential witnesses, or flee the area to avoid investigation and prosecution), and result in a serious impediment to law enforcement.

(2)(i) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) because these provisions concern an individual's access to records which concern him/her

and access to records in this system would compromise ongoing investigations. Such access is directed at allowing the subject of the record to correct inaccuracies in it. The vast majority of records in this system are from the DNA records of local and State NDIS agencies which would be inappropriate and not feasible for the FBI to undertake to correct. Nevertheless, an alternate method to access and/or amend records in this system is available to an individual who is the subject of a record pursuant to procedures and requirements specified in the Notice of Systems of Records compiled by the National Archives and Records Administration and published in the FEDERAL REGISTER under the designation: National DNA Index System (NDIS) (JUSTICE/FBI-017)

(ii) In addition, from paragraph (d)(2) of this section, because to require the FBI to amend information thought to be incorrect, irrelevant, or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde investigations attempting to resolve questions of accuracy, etc.

(iii) In addition, from subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

(3) From subsection (e)(1) because:

(i) Information in this system is primarily from State and local records and it is for the official use of agencies outside the Federal Government.

(ii) It is not possible in all instances to determine the relevancy or necessity of specific information in the early stages of the criminal investigative process.

(iii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary, and vice versa. It is only after the information is assessed that its relevancy in a specific investigative activity can be established.

(iv) Although the investigative process could leave in doubt the relevancy and necessity of evidence which had

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

been properly obtained, the same information could be relevant to another investigation or investigative activity under the jurisdiction of the FBI or another law enforcement agency.

(4) From subsections (e)(2) and (3) because it is not feasible to comply with these provisions given the nature of this system. Most of the records in this system are necessarily furnished by State and local criminal justice agencies and not by individuals due to the very nature of the records and the system.

(5) From subsection (e)(5) because the vast majority of these records come from State and local criminal justice agencies and because it is administratively impossible for them and the FBI to insure that the records comply with this provision. Submitting agencies are urged and make every effort to insure records are accurate and complete; however, since it is not possible to predict when information in the indexes of the system (whether submitted by State and local criminal justice agencies or generated by the FBI) will be matched with other information, it is not possible to determine when most of them are relevant or timely.

(6) From subsection (e)(8) because the FBI has no logical manner to determine whenever process has been made public and compliance with this provision would provide an impediment to law enforcement by interfering with ongoing investigations.

(p) The National Instant Criminal Background Check System (NICS), (JUSTICE/FBI-018), a Privacy Act system of records, is exempt:

(1) Pursuant to 5 U.S.C. 552a(j)(2), from subsections (c) (3) and (4); (d); (e) (1), (2) and (3); (e)(4) (G) and (H); (e) (5) and (8); and (g); and

(2) Pursuant to 5 U.S.C. 552a(k) (2) and (3), from subsections (c)(3), (d), (e)(1), and (e)(4) (G) and (H).

(q) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2), and (k)(3). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the accounting of disclosures would place the subject on notice that

the subject is or has been the subject of investigation and result in a serious impediment to law enforcement.

(2) From subsection (c)(4) to the extent that it is not applicable since an exemption is claimed from subsection (d).

(3)(i) From subsections (d) and (e)(4) (G) and (H) because these provisions concern an individual's access to records which concern the individual and such access to records in the system would compromise ongoing investigations, reveal investigatory techniques and confidential informants, invade the privacy of persons who provide information in connection with a particular investigation, or constitute a potential danger to the health or safety of law enforcement personnel.

(ii) In addition, from subsection (d)(2) because, to require the FBI to amend information thought to be not accurate, timely, relevant, and complete, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative burden by forcing the agency to continuously update its investigations attempting to resolve these issues.

(iii) Although the Attorney General is exempting this system from subsections (d) and (e)(4) (G) and (H), an alternate method of access and correction has been provided in 28 CFR, part 25, subpart A.

(4) From subsection (e)(1) because it is impossible to state with any degree of certainty that all information in these records is relevant to accomplish a purpose of the FBI, even though acquisition of the records from state and local law enforcement agencies is based on a statutory requirement. In view of the number of records in the system, it is impossible to review them for relevancy.

(5) From subsections (e) (2) and (3) because the purpose of the system is to verify information about an individual. It would not be realistic to rely on information provided by the individual. In addition, much of the information contained in or checked by this system is from Federal, State, and local criminal history records.

(6) From subsection (e)(5) because it is impossible to predict when it will be

necessary to use the information in the system, and, accordingly, it is not possible to determine in advance when the records will be timely. Since most of the records are from State and local or other Federal agency records, it would be impossible to review all of them to verify that they are accurate. In addition, an alternate procedure is being established in 28 CFR, part 25, subpart A, so the records can be amended if found to be incorrect.

(7) From subsection (e)(8) because the notice requirement could present a serious impediment to law enforcement by revealing investigative techniques and confidential investigations.

(8) From subsection (g) to the extent that, pursuant to subsections (j)(2), (k)(2), and (k)(3), the system is exempted from the other subsections listed in paragraph (p) of this section.

(r) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g):

(1) Terrorist Screening Records System (TSRS) (JUSTICE/FBI-019).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the counterterrorism purposes of this system, and the overall law enforcement process, the applicable exemption may be waived by the FBI in its sole discretion.

(s) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he/she is under investigation. This information could also permit the record subject to take measures to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation. Similarly, dis-

closing this information to individuals who have been misidentified as known or suspected terrorists due to a close name similarity could reveal the Government's investigative interest in a terrorist suspect, because it could make known the name of the individual who actually is the subject of the Government's interest. Consequently, the Government has as great an interest in protecting the confidentiality of identifying information of misidentified persons as it does in protecting the confidentiality of the identities of known or suspected terrorists.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of records contained in this system, which consists of counterterrorism, investigatory and intelligence records. Compliance with these provisions could alert the subject of a terrorism investigation of the fact and nature of the investigation, and/or the investigative interest of the FBI and/or other intelligence or law enforcement agencies; compromise sensitive information classified in the interest of national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. Similarly, compliance with these provisions with respect to records on individuals who have been misidentified as known or suspected

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

terrorists due to a close name similarity could reveal the Government's investigative interest in a terrorist suspect, because it could make known the name of the individual who actually is the subject of the Government's interest.

(4) From subsection (e)(1) because it is not always possible for TSC to know in advance what information is relevant and necessary for it to complete an identity comparison between the individual being screened and a known or suspected terrorist. Also, because TSC and the FBI may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3), to the extent that this subsection is interpreted to require TSC to provide notice to an individual if TSC receives information about that individual from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsection (e)(5) because many of the records in this system are derived from other domestic and foreign agency record systems and therefore it is not possible for the FBI and the TSC to vouch for their compliance with this provision; however, the TSC

has implemented internal quality assurance procedures to ensure that TSC terrorist screening data is as thorough, accurate, and current as possible. In addition, TSC supports but does not conduct investigations; therefore, it must be able to collect information related to terrorist identities and encounters for distribution to law enforcement and intelligence agencies that do conduct terrorism investigations. In the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. The TSC has, however, implemented internal quality assurance procedures to ensure that TSC terrorist screening data is as thorough, accurate, and current as possible. The FBI also is exempting the TSRS from the requirements of subsection (e)(5) in order to prevent the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the TSRS. The FBI has exempted TSRS records from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of counterterrorism investigations. Exempting the TSRS from subsection (e)(5) serves to prevent the assertion of challenges to a record's accuracy, timeliness, completeness, and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the FBI and the TSC and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact

of those investigations when not previously known.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(t) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act:

(1) Law Enforcement National Data Exchange (N-DEx), (JUSTICE/FBI-020).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the FBI in its sole discretion.

(u) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative interest in the individual. Revealing this information may thus compromise ongoing law enforcement efforts. Revealing this information may also permit the record subject to take measures to impede the investigation, such as destroying evidence, intimidating potential witnesses or fleeing the area to avoid the investigation.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4), because these provisions concern individual access to and amendment of investigatory records, compliance with which could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of the FBI and other law enforcement agencies; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; possibly identify a confidential source or disclose informa-

tion which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing investigations and other law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes and, in fact, a major tenet of the N-DEx information sharing system is that the relevance of certain information may not always be evident in the absence of the ability to correlate that information with other existing law enforcement data.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to efforts to solve crimes and improve homeland security in that it would put the subject of an investigation on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(6) From subsection (e)(3) because disclosure would put the subject of an investigation on notice of that fact and would permit the subject to engage in conduct intended to thwart that activity.

(7)(i) From subsection (e)(5) because many of the records in this system are records contributed by other agencies and the restrictions imposed by (e)(5) would limit the utility of the N-DEx system. All data contributors are expected to ensure that information they share is relevant, timely, complete and accurate. In fact, rules for use of the N-DEx system will require that information be updated periodically and not be used as a basis for action or disseminated beyond the recipient without the recipient first obtaining permission from the record owner/contributor. These rules will be enforced through robust audit procedures. The existence of these rules should ameliorate any perceived concerns about the integrity

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

of the information in the N-DEx system. Nevertheless, exemption from this provision is warranted in order to reduce the administrative burden on the FBI to vouch for compliance with the provision by all N-DEx data contributors and to encourage those contributors to share information the significance of which may only become apparent when combined with other information in the N-DEx system.

(ii) The FBI is also exempting the N-DEx from subsection (e)(5) in order to block the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the N-DEx. The FBI has exempted these records from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of law enforcement investigations. Exempting the N-DEx system from subsection (e)(5) complements this exemption and will provide the FBI with the ability to prevent the assertion of challenges to a record's accuracy, timeliness, completeness and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8), because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the FBI and may alert the subjects of law enforcement investigations to the fact of those investigations, when not previously known.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(v) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f); and (g) of the Privacy Act:

(1) FBI Data Warehouse System, (JUSTICE/FBI-022).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k). Where compliance with an exempted provision could not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the Department of Justice (DOJ) in its sole discretion may waive an exemption in whole or in part; exercise of this discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectation of waiver in that matter or any other matter. As a condition of discretionary waiver, the DOJ in its sole discretion may impose any restrictions deemed advisable by the DOJ (including, but not limited to, restrictions on the location, manner, or scope of notice, access, or amendment).

(w) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any law enforcement or national security investigative interest in the individual by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and defuse any potential acts of terrorism or other potential violations of criminal law. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to circumvent the investigation.

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the accounting of disclosures provision of subsection (c)(3).

(3) From subsections (d)(1), (2), (3), and (4) and (e)(4)(G) and (H) because these provisions concern individual access to and amendment of law enforcement, intelligence and counterintelligence, and counterterrorism records, and compliance could alert the subject of an authorized law enforcement or intelligence activity about that particular activity and the investigative interest of the FBI or other law enforcement or intelligence agencies. Providing access could compromise

sensitive information classified to protect national security; disclose information that would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; could provide information that would allow a subject to avoid detection or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, and witnesses. The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases with subjects of the information.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. The relevance and utility of certain information that may have a nexus to terrorism or other crimes may not always be evident until and unless it is vetted and matched with other sources of information that are necessarily and lawfully maintained by the FBI.

(5) From subsections (e)(2) and (3) because application of these provisions could present a serious impediment to efforts to solve crimes and improve national security. Application of these provisions would put the subject of an investigation on notice of that fact and allow the subject an opportunity to engage in conduct intended to impede that activity or avoid apprehension.

(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the FEDERAL REGISTER. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI. Further, greater specificity of properly classified records could compromise national security.

(7) From subsection (e)(5) because in the collection of information for au-

thorized law enforcement and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. With time, seemingly irrelevant or untimely information may acquire new significance when new details are brought to light. Additionally, the information may aid in establishing patterns of activity and providing criminal or intelligence leads. It could impede investigative progress if it were necessary to assure relevance, accuracy, timeliness and completeness of all information obtained during the scope of an investigation. Further, some of the records in this system come from other agencies and it would be administratively impossible for the FBI to vouch for the compliance of these agencies with this provision.

(8) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the FBI and may alert the subjects of law enforcement investigations, who might be otherwise unaware, to the fact of those investigations.

(9) From subsections (f) and (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(x) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f); and (g):

(1) The FBI Online Collaboration Systems (JUSTICE/FBI-004).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where the FBI determines compliance with an exempted provision would not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the FBI in its sole discretion may waive an exemption in whole or in part; exercise of this discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectation of waiver in that matter or any other matter. As a condition of discretionary waiver, the FBI in its sole discretion may impose any restrictions deemed advisable by

## § 16.96

## 28 CFR Ch. I (7-1-24 Edition)

the FBI (including, but not limited to, restrictions on the location, manner, or scope of notice, access or amendment).

(y) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any law enforcement or national security investigative interest in the individual by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and defuse any potential acts of terrorism or other potential violations of criminal law. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to circumvent the investigation (*e.g.* destroy evidence or flee the area to avoid investigation).

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the accounting disclosures provision of subsection (c)(3). The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases.

(3) From subsections (d)(1), (2), (3), and (4); (e)(4)(G) and (H); (e)(8); (f); and (g) because these provisions concern individual access to and amendment of law enforcement and intelligence records and compliance with such provisions could alert the subject of an authorized law enforcement or intelligence activity about that particular activity and the investigative interest of the FBI and/or other law enforcement or intelligence agencies. Pro-

viding access rights could compromise sensitive law enforcement information, disclose information that could constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; provide information that would allow a subject to avoid detection or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, and witnesses. The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases with subjects of the information.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. Relevance and necessity are questions of judgment and timing. For example, what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after information has been fully assessed that its relevancy and necessity in a specific investigative activity can be determined.

(5) From subsections (e)(2) and (3) because application of these provisions requiring collection directly from the subject individuals and informing individuals regarding information to be collected about them could present a serious impediment to efforts to solve crimes and improve national security. Application of these provisions could put the subject of an investigation on notice of the existence of the investigation and allow the subject an opportunity to engage in conduct intended to obstruct or otherwise impede that activity or take steps to avoid apprehension.

(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has already been published in the FEDERAL REGISTER through the SORN documentation. Should the subsection be so interpreted, exemption from this provision is necessary to protect the

**Department of Justice****§ 16.97**

sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI.

(7) From subsection (e)(5) because in the collection of information for authorized law enforcement and intelligence purposes it is often impossible to determine in advance what information is accurate, relevant, timely, and complete. With time, additional facts, or analysis, information may acquire new significance. The restrictions imposed by subsection (e)(5) would thus limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. Although the FBI has claimed this exemption, it continuously works with its federal, state, local, tribal, and international partners to maintain the accuracy of records to the greatest extent practicable. The FBI does so with established policies and practices. The criminal justice and national security communities have a strong operational interest in using up-to-date and accurate records and will apply their own procedures and foster relationships with their partners to further this interest.

[Order No. 40-80, 45 FR 5301, Jan. 23, 1980]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 16.96, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at [www.govinfo.gov](http://www.govinfo.gov).

**§ 16.97 Exemption of Bureau of Prisons Systems—limited access.**

(a) The following systems of records are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (H), (e)(8), (f) and (g):

- (1) Custodial and Security Record System (JUSTICE/BOP-001).
- (2) Industrial Inmate Employment Record System (JUSTICE/BOP-003).
- (3) Inmate Administrative Remedy Record System (JUSTICE/BOP-004).
- (4) Inmate Commissary Accounts Record System (JUSTICE/BOP-006).
- (5) Inmate Physical and Mental Health Record System (JUSTICE/BOP-007).

(6) Inmate Safety and Accident Compensation Record System (JUSTICE/BOP-008).

(7) Federal Tort Claims Act Record System (JUSTICE/BOP-009).

(8) Federal Tort Claims Act Record System (JUSTICE/BOP-009).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because inmates will not be permitted to gain access or to contest contents of these record systems under the provisions of subsection (d) of 5 U.S.C. 552a. Revealing disclosure accountings can compromise legitimate law enforcement activities and Bureau of Prisons responsibilities.

(2) From subsection (c)(4) because exemption from provisions of subsection (d) will make notification of formal disputes inapplicable.

(3) From subsection (d) because exemption from this subsection is essential to protect internal processes by which Bureau personnel are able to formulate decisions and policies with regard to federal prisoners, to prevent disclosure of information to federal inmates that would jeopardize legitimate correctional interests of security, custody, or rehabilitation, and to permit receipt of relevant information from other federal agencies, state and local law enforcement agencies, and federal and state probation and judicial offices.

(4) From subsection (e)(2) because primary collection of information directly from federal inmates about criminal sentences or criminal records is highly impractical and inappropriate.

(5) From subsection (e)(3) because in view of the Bureau of Prisons' responsibilities, application of this provision to its operations and collection of information is inappropriate.

(6) From subsection (e)(4)(H) because exemption from provisions of subsection (d) will make publication of agency procedures under this subsection inapplicable.

## § 16.97

## 28 CFR Ch. I (7-1-24 Edition)

(7) From subsection (e)(8) because the nature of Bureau of Prisons law enforcement activities renders notice of compliance with compulsory legal process impractical.

(8) From subsection (f) because exemption from provisions of subsection (d) will render compliance with provisions of this subsection inapplicable.

(9) From subsection (g) because exemption from provisions of subsection (d) will render provisions of this subsection inapplicable.

(c) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(5) and (e)(8), and (g). In addition, the following system of records is exempted pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d), and (e)(1):

Bureau of Prisons Access Control Entry/Exit, (JUSTICE/BOP-010).

(d) These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g. public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) for similar reasons as those enumerated in paragraph (3).

(2) From subsection (c)(4) to the extent that exemption from subsection (d) will make notification of corrections or notations of disputes inapplicable.

(3) From the access provisions of subsection (d) to the extent that exemption from this subsection may appear to be necessary to prevent access by record subjects to information that may jeopardize the legitimate correctional interests of safety, security, and good order of Bureau of Prisons facilities; to protect the privacy of third parties; and to protect access to relevant information received from third

parties, such as other Federal State, local and foreign law enforcement agencies, Federal and State probation and judicial offices, the disclosure of which may permit a record subject to evade apprehension, prosecution, etc.; and/or to otherwise protect investigatory or law enforcement information, whether received from other third parties, or whether developed internally by the BOP.

(4) From the amendment provisions of subsection (d) because amendment of the records would interfere with law enforcement operations and impose an impossible administrative burden. In addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that law enforcement and investigatory information be continuously reexamined, even where the information may have been collected from the record subject. Also, where records are provided by other Federal criminal justice agencies or other State, local and foreign jurisdictions, it may be administratively impossible to ensure compliance with this provision.

(5) From subsection (e)(1) to the extent that the BOP may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

(6) From subsection (e)(2) because primary collection of information directly from the record subject is often highly impractical, inappropriate and could result in inaccurate information.

(7) From subsection (e)(3) because compliance with this subsection may impede the collection of information that may be valuable to law enforcement interests.

(8) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance as an investigation progresses or with the

passage of time, and could be relevant to future law enforcement decisions.

(9) From subsection (e)(8) because the nature of BOP law enforcement activities renders notice of compliance with compulsory legal process impractical and could seriously jeopardize institution security and personal safety and/or impede overall law enforcement efforts.

(10) From subsection (g) to the extent that the system is exempted from subsection (d).

(e) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(5) and (e)(8), (f) and (g):

Telephone Activity Record System (JUS-TICE/BOP-011).

(f) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) to the extent that this system of records is exempt from subsection (d), and for such reasons as those cited for subsection (d) in paragraph (f)(3) below.

(2) From subsection (c)(4) to the extent that exemption from subsection (d) makes this exemption inapplicable.

(3) From the access provisions of subsection (d) because exemption from this subsection is essential to prevent access of information by record subjects that may invade third party privacy; frustrate the investigative process; jeopardize the legitimate correctional interests of safety, security, and good order to prison facilities; or otherwise compromise, impede, or interfere with BOP or other law enforcement agency activities.

(4) From the amendment provisions from subsection (d) because amendment of the records may interfere with law enforcement operations and would impose an impossible administrative

burden by requiring that, in addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that law enforcement information be continuously reexamined, even where the information may have been collected from the record subject. Also, some of these records come from other Federal criminal justice agencies or State, local and foreign jurisdictions, or from Federal and State probation and judicial offices, and it is administratively impossible to ensure that the records comply with this provision.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since it may result in inaccurate information.

(6) From subsection (e)(3) because in view of BOP's operational responsibilities, application of this provision to the collection of information is inappropriate. Application of this provision could provide the subject with substantial information which may in fact impede the information gathering process or compromise an investigation.

(7) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Material which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance at a later date or as an investigation progresses. Also, some of these records may come from other Federal, State, local and foreign law enforcement agencies, and from Federal and State probation and judicial offices and it is administratively impossible to ensure that the records comply with this provision. It would also require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject.

## § 16.97

## 28 CFR Ch. I (7-1-24 Edition)

(8) From subsection (e)(8) because the nature of BOP law enforcement activities renders impractical the notice of compliance with compulsory legal process. This requirement could present a serious impediment to law enforcement such as revealing investigative techniques or the existence of confidential investigations, jeopardize the security of third parties, or otherwise compromise law enforcement efforts.

(9)–(10) [Reserved]

(11) From subsections (f) and (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(g) The following system of records is exempt pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2), and (3), (e)(5) and (e)(8), and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempt pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) of 5 U.S.C. 552a:

Bureau of Prisons, Office of Internal Affairs  
Investigative Records, JUSTICE/BOP-012

(h) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, the applicable exemption may be waived, either partially or totally, by the Office of Internal Affairs (OIA). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation, and reveal investigative interest by not only the OIA but also by the recipient agency. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the

investigation, release could result in activities that would impede or compromise law enforcement such as: the destruction of documentary evidence; improper influencing of witnesses; endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel; fabrication of testimony; and flight of the subject from the area. In addition, release of disclosure accounting could result in the release of properly classified information which could compromise the national defense or disrupt foreign policy.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could provide the subject of an investigation with information concerning law enforcement activities such as that relating to an actual or potential criminal, civil or regulatory violation; the existence of an investigation; the nature and scope of the information and evidence obtained as to his activities; the identity of confidential sources, witnesses, and law enforcement personnel; and information that may enable the subject to avoid detection or apprehension. Such disclosure would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation; endanger the physical safety of confidential sources, witnesses, and law enforcement personnel; and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which could compromise the national defense or disrupt foreign policy. Amendment

**Department of Justice****§ 16.97**

of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIA for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIA may obtain information concerning actual or potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIA should retain this information as it may aid in establishing patterns of criminal activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation, information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may relate also to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(5) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to inves-

tigators, and information relating to a subject's illegal acts, violations of rules of conduct, or any other misconduct must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

(6) From subsection (e)(3) because the application of this provision would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5) because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Material which may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance as an investigation progresses. The restrictions of this provision could interfere with the preparation of a complete investigation report, and thereby impede effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigation techniques, procedures, and/or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), and (k)(2) of the Privacy Act.

(i) Consistent with the legislative purpose of the Privacy Act of 1974 (Pub. L. 93-579) the BOP has initiated a procedure whereby federal inmates in custody may gain access and review their

## § 16.97

## 28 CFR Ch. I (7-1-24 Edition)

individual prison files maintained at the institution of incarceration. Access to these files will be limited only to the extent that the disclosure of records to the inmate would jeopardize internal decision-making or policy determinations essential to the effective operation of the Bureau of Prisons; to the extent that disclosure of the records to the inmate would jeopardize privacy rights of others, or a legitimate correctional interest of security, custody, or rehabilitation; and to the extent information is furnished with a legitimate expectation of confidentiality. The Bureau of Prisons will continue to provide access to former inmates under existing regulations as is consistent with the interests listed above. Under present Bureau of Prisons regulations, inmates in federal institutions may file administrative complaints on any subject under the control of the Bureau. This would include complaints pertaining to information contained in these systems of records.

(j) The following system of records is exempt pursuant to 5 U.S.C. 552a(j) and (k) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (H), and (I), (5), (8); (f); and (g): Inmate Central Records System (JUSTICE/BOP-005).

(k) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning the subject individual would specifically reveal any investigative interest in the individual. Revealing this information may thus compromise ongoing law enforcement ef-

orts, as well as efforts to identify and defuse any potential acts of terrorism. Revealing this information may also permit the subject individual to take measures to impede the investigation, such as destroying evidence, intimidating potential witnesses, or fleeing the area to avoid the investigation.

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4), because these provisions concern individual access to and amendment of records, compliance with which could jeopardize the legitimate correctional interests of safety, security, and good order of prison facilities; alert the subject of a suspicious activity report of the fact and nature of the report and any underlying investigation and/or the investigative interest of the BOP and other law enforcement agencies; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, and/or flight of the subject; possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Although the BOP has rules in place emphasizing that records should be kept up to date, the requirement for amendment of these records would interfere with ongoing law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for the proper safekeeping, care, and custody of incarcerated persons, and for the proper security and safety of federal prisons and the public. In addition, to the extent that the BOP may collect information that may also

be relevant to the law enforcement operations of other agencies, in the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with such relevant responsibilities.

(5) From subsections (e)(2) because the nature of criminal investigative and correctional activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations and activities, it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since it may result in inaccurate information and compromise ongoing criminal investigations or correctional management decisions.

(6) From subsections (e)(3) because in view of BOP's operational responsibilities, the application of this provision would provide the subject of an investigation or correctional matter with significant information which may in fact impede the information gathering process or compromise ongoing criminal investigations or correctional management decisions.

(7) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d).

(8) From subsection (e)(4)(I) because publishing further details regarding categories of sources of records in the system may compromise ongoing investigations, reveal investigatory techniques and descriptions of confidential informants, or constitute a potential danger to the health or safety of law enforcement personnel.

(9) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is difficult to determine in advance what information is accurate, relevant, timely, and complete. Data which may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance during the course of an investigation or with the passage of time, and could be relevant to future law enforcement decisions. In addition, because many of these records come from courts and other state and local criminal justice

agencies, it is administratively impossible for them and the BOP to ensure compliance with this provision. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the safety and security of the prisons and the public.

(10) From subsection (e)(8), because to require individual notice of disclosure of information due to a compulsory legal process would pose an impossible administrative burden on BOP and may alert subjects of investigations, who might otherwise be unaware, to the fact of those investigations.

(11) From subsection (f) to the extent that this system is exempt from the provisions of subsection (d).

(12) From subsection (g) to the extent that this system is exempted from other provisions of the Act.

(1) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Trust Fund Accounts and Commissary Record System, (Justice/BOP-006).

(m) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g. public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

## § 16.97

## 28 CFR Ch. I (7-1-24 Edition)

(2) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance as an investigation progresses or with the passage of time, and could be relevant to future law enforcement decisions. In addition, amendment of the records may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that law enforcement information be continuously reexamined, even where the information may have been collected from the record subject or other criminal justice agencies. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the safety and security of the prisons and the public.

(n) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Physical and Mental Health Records System, (Justice/BOP-007).

(o) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, *e.g.* public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

(2) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance during the course of an investigation or with the passage of time, and could be relevant to future law enforcement decisions. In addition, because many of these records come from sources outside the Bureau of Prisons, it is administratively impossible for them and the Bureau to ensure compliance with this provision. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the health care of the inmates and the safety and security of the prisons and the public.

(p) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4), (d)(1)-(4), (e)(2) and (3), (e)(5), and (g):

Inmate Electronic Message Record System (JUSTICE /BOP-013).

(q) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) to the extent that this system of records is exempt from subsection (d), and for such reasons as those cited for subsection (d) in paragraph (q)(3) below.

(2) From subsection (c)(4) to the extent that exemption from subsection (d) makes this exemption inapplicable.

(3) From the access provisions of subsection (d) because exemption from this subsection is essential to prevent

access of information by record subjects that may invade third party privacy; frustrate the investigative process; jeopardize the legitimate correctional interests of safety, security and good order to prison facilities; or otherwise compromise, impede, or interfere with BOP or other law enforcement agency activities.

(4) From the amendment provisions of subsection (d) because amendment of the records may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that, in addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that law enforcement information be continuously reexamined, even where the information may have been collected from the record subject. Also, some of these records come from other Federal criminal justice agencies or State, local and foreign jurisdictions, or from Federal and State probation and judicial offices, and it is administratively impossible to ensure that records comply with this provision.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since it may result in inaccurate information and compromise ongoing criminal investigations or correctional management decisions.

(6) From subsection (e)(3) because in view of BOP's operational responsibilities, application of this provision to the collection of information is inappropriate. Application of this provision could provide the subject with substantial information which may in fact impede the information gathering process or compromise ongoing criminal investigations or correctional management decisions.

(7) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Mate-

rial which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance at a later date or as an investigation progresses. Also, some of these records may come from other Federal, State, local and foreign law enforcement agencies, and from Federal and State probation and judicial offices and it is administratively impossible to ensure that the records comply with this provision. It would also require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject.

(8) From subsection (g) to the extent that this system is exempted from other provisions of the Act.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 16.97, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at [www.govinfo.gov](http://www.govinfo.gov).

#### **§ 16.98 Exemption of the Drug Enforcement Administration (DEA) Systems—limited access.**

(a) The following systems of records are exempt from 5 U.S.C. 552a(c)(3) and (d):

(1) Automated Records and Consummated Orders System/Diversion Analysis and Detection System (ARCOS/DADS) (Justice/DEA-003)

(2) Controlled Substances Act Registration Records (Justice/DEA-005)

(3) Registration Status/Investigatory Records (Justice/DEA-012)

(b) These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of the disclosure accounting would enable the subject of an investigation to gain valuable information concerning the nature and scope of the investigation and seriously hamper the regulatory functions of the DEA.

(2) From subsection (d) because access to records contained in these systems may provide the subject of an investigation information that could enable him to avoid compliance with the

## § 16.98

Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513).

(c) Systems of records identified in paragraphs (c)(1) through (6) of this section are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of 5 U.S.C. 552a. In addition, systems of records identified in paragraphs (c)(1) through (5) of this section are also exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) from subsections (c)(3); (d)(1), (2), (3) and (4); and (e)(1):

- (1) Air Intelligence Program (Justice/DEA-001).
- (2) Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002).
- (3) Planning and Inspection Division Records (Justice/DEA-010).
- (4) Operation Files (Justice/DEA-011).
- (5) Security Files (Justice/DEA-013).
- (6) System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014).

(d) Exemptions apply to the following systems of records only to the extent that information in the systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2): Air Intelligence Program (Justice/DEA-001); Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002); Planning and Inspection Division Records (Justice/DEA-010); and Security Files (Justice/DEA-013). Exemptions apply to the Operations Files (Justice/DEA-011) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Exemptions apply to the System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting would provide to the subjects of an investigation significant information concerning the nature of the investigation and thus would present the same impediments to law enforcement as those enumerated in paragraph (d)(3) regarding exemption from subsection (d).

## 28 CFR Ch. I (7-1-24 Edition)

(2) From subsection (c)(4) to the extent that it is not applicable because an exemption is being claimed from subsection (d).

(3) From the access provisions of subsection (d) because access to records in this system of records would present a serious impediment to law enforcement. Specifically, it could inform the record subject of an actual or potential criminal, civil, or regulatory investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. Similarly, it may alert collateral suspects yet unprosecuted in closed cases. It could prevent the successful completion of the investigation; endanger the life, health, or physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony; or it may simply reveal a sensitive investigative technique. In addition, granting access to such information could result in the disclosure of confidential/security-sensitive or other information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. From the amendment provisions of subsection (d) because amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the DEA for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations during which DEA may

obtain properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the DEA's investigative activities DEA may detect the violation of either drug-related or non-drug related laws. In the interests of effective law enforcement, it is necessary that DEA retain all information obtained because it can aid in establishing patterns of activity and provide valuable leads for Federal and other law enforcement agencies or otherwise assist such agencies in discharging their law enforcement responsibilities. Such information may include properly classified information, the retention of which could be in the interests of national defense and/or foreign policy.

(5) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful prosecution.

(6) From subsection (e)(3) because the requirements thereof would constitute a serious impediment to law enforcement in that they could compromise the existence of an actual or potential confidential investigation and/or permit the record subject to speculate on the identity of a potential confidential source, and endanger the life, health or physical safety or either actual or potential confidential informants and witnesses, and of investigators/law enforcement personnel. In addition, the

notification requirement of subsection (e)(3) could impede collection of that information from the record subject, making it necessary to collect the information solely from third party sources and thereby inhibiting law enforcement efforts.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1) and (k)(2) of the Privacy Act.

(e) The following systems of records are exempt from 5 U.S.C. 552a (d)(1) and (e)(1):

(1) Grants of Confidentiality Files (GCF) (Justice/DEA-017), and

(2) DEA Applicant Investigations (Justice/DEA-018).

(f) These exemptions apply only to the extent that information in these systems is subject to exception pursuant to 5 U.S.C. 552a(k)(5). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a grant of confidentiality

## § 16.98

## 28 CFR Ch. I (7-1-24 Edition)

with DEA. By permitting access to information which may reveal the identity of the source of that information—after a promise of confidentiality has been given—DEA would breach the promised confidentiality. Ultimately, such breaches would restrict the free flow of information which is vital to a determination of an applicant's qualifications for a grant.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluation purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other apparently irrelevant information, can on occasion provide a composite picture of an applicant which assists in determining whether a grant of confidentiality is warranted.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g): El Paso Intelligence Center (EPIC) Seizure System (ESS) (JUSTICE/DEA-022). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement and counter-drug purposes of this system, and the overall law enforcement process, the applicable exemption may be waived by the DEA in its sole discretion.

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would potentially reveal any investigative interest in the individual. Revealing this information would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants. Simi-

larly, disclosing this information could reasonably be expected to compromise ongoing investigatory efforts by notifying the record subject that he/she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of records contained in this system, which consists of counter-drug and criminal investigatory records. Compliance with these provisions could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation; endanger the physical safety of witnesses or informants; or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary to complete an identity comparison between the individual being screened and a known or suspected criminal or terrorist. Also, it may not always be known what information will be relevant to law enforcement for the purpose of conducting an operational response or on-going investigation.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to law enforcement and counter-drug efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting

the subject to engage in conduct designed to frustrate or impede that activity. The nature of counter-drug investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) because the requirements thereof would constitute a serious impediment to law enforcement in that they could compromise the existence of an actual or potential confidential investigation and/or permit the record subject to speculate on the identity of a potential confidential source, and endanger the life, health or physical safety of either actual or potential confidential informants and witnesses, and of investigators/law enforcement personnel. In addition, the notification requirement of subsection (e)(3) could impede collection of that information from the record subject, making it necessary to collect the information solely from third party sources and thereby inhibiting law enforcement efforts.

(7) From subsection (e)(5) because many of the records in this system are derived from other domestic record systems and therefore it is not possible for the DEA and EPIC to vouch for their compliance with this provision. In addition, EPIC supports but does not conduct investigations; therefore, it must be able to collect information related to illegal drug and other criminal activities and encounters for distribution to law enforcement and intelligence agencies that do conduct counter-drug investigations. In the collection of information for law enforcement and counter-drug purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the develop-

ment of intelligence necessary for effective law enforcement and counter-terrorism efforts. EPIC has, however, implemented internal quality assurance procedures to ensure that ESS data is as thorough, accurate, and current as possible. ESS is also exempt from the requirements of subsection (e)(5) in order to prevent the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the ESS. ESS records are exempt from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of investigations. Exempting ESS from subsection (e)(5) serves to prevent the assertion of challenges to a record's accuracy, timeliness, completeness, and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the DEA and EPIC and could alert the subjects of counter-drug, counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known. Additionally, compliance could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(i) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), (I), (5), and (8); (f); (g); and (h): Investigative Reporting and Filing System (IRFS) (JUSTICE/DEA-008). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement or counterterrorism purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the DEA in its sole discretion.

## § 16.98

## 28 CFR Ch. I (7-1-24 Edition)

(j) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide a record subject with an accounting of disclosure of records in this system could impede or compromise an ongoing investigation, interfere with a law enforcement activity, lead to the disclosure of properly classified information which could compromise the national defense or disrupt foreign policy, invade the privacy of a person who provides information in connection with a particular investigation, or result in danger to an individual's safety, including the safety of a law enforcement officer.

(2) From subsection (c)(4) because this subsection is inapplicable to the extent that an exemption is being claimed for subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of records in the system could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of confidential witnesses and informants, or of the investigative interest of the DEA; lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life, health, and physical safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Access to records could also result in the release of information properly classified pursuant to Executive order, thereby compromising the national defense or foreign policy.

(4) From subsection (d)(2) because amendment of the records thought to be incorrect, irrelevant, or untimely would also interfere with ongoing investigations, criminal or civil law en-

forcement proceedings, and other law enforcement activities; would impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised; and may impact information properly classified pursuant to Executive order.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because, in the course of its acquisition, collation, and analysis of information under the statutory authority granted to it, an agency may occasionally obtain information, including information properly classified pursuant to Executive order, that concerns actual or potential violations of law that are not strictly within its statutory or other authority, or may compile information in the course of an investigation which may not be relevant to a specific prosecution. It is impossible to determine in advance what information collected during an investigation will be important or crucial to the investigation and the apprehension of fugitives. In the interests of effective law enforcement, it is necessary to retain such information in this system of records because it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies. This consideration applies equally to information acquired from, or collated or analyzed for, both law enforcement agencies and agencies of the U.S. foreign intelligence community and military community.

(7) From subsection (e)(2) because in a criminal investigation, prosecution, or proceeding, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation, prosecution, or proceeding would be placed on notice as to the existence and nature of the investigation, prosecution, and proceeding and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Moreover, thorough

**Department of Justice****§ 16.99**

and effective investigation and prosecution may require seeking information from a number of different sources.

(8) From subsection (e)(3) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to criminal law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants and endanger their lives, health, and physical safety. The individual could seriously interfere with undercover investigative techniques and could take appropriate steps to evade the investigation or flee a specific area.

(9) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act, and from subsection (e)(4)(I) to preclude any claims that the Department must provide more detail regarding the record sources for this system than the Department publishes in the system of records notice for this system. Exemption from providing any additional details about sources is necessary to preserve the security of sensitive law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the DEA; and further, greater specificity of properly classified records could compromise national security.

(10) From subsection (e)(5) because the acquisition, collation, and analysis of information for criminal law enforcement purposes from various agencies does not permit a determination in advance or a prediction of what information will be matched with other information and thus whether it is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government at-

torneys to exercise their judgment in collating and analyzing information and would impede the development of criminal or other intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, evidence, or interest, and by interfering with the ability to issue warrants or subpoenas; could give persons sufficient warning to evade investigative efforts; and would pose an impossible administrative burden on the maintenance of these records and the conduct of the underlying investigations.

(12) From subsections (f) and (g) because these subsections are inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(13) From subsection (h) when application of this provision could impede or compromise an ongoing criminal investigation, interfere with a law enforcement activity, reveal an investigatory technique or confidential source, invade the privacy of a person who provides information for an investigation, or endanger law enforcement personnel.

[Order No. 88-94, 59 FR 29717, June 9, 1994, as amended by Order No. 127-97, 62 FR 2903, Jan. 21, 1997; Order No. 009-2003, 68 FR 14140, Mar. 24, 2003; 72 FR 54825, Sept. 27, 2007; CPCLO Order No. 002-2013, 78 FR 14672, Mar. 7, 2013]

**§ 16.99 Exemption of the Immigration and Naturalization Service Systems-limited access.**

(a) The following systems of records of the Immigration and Naturalization Service are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (1), (2) and (3), (e) (4)(G) and (H), (e) (5) and (8), and (g):

(1) The Immigration and Naturalization Service Alien File (A-File) and Central Index System (CIS), JUSTICE/INS-001A.

(2) The Immigration and Naturalization Service Index System, JUSTICE/INS-001 which consists of the following subsystems:

(i) Agency Information Control Record Index.

(ii) Alien Enemy Index.

## § 16.99

- (iii) Congressional Mail Unit Index.
- (iv) Air Detail Office Index.
- (v) Anti-smuggling Index (general).
- (vi) Anti-smuggling Information Centers Systems for Canadian and Mexican Borders.
- (vii) Border Patrol Sectors General Index System.
- (viii) Contact Index.
- (ix) Criminal, Narcotic, Racketeer and Subversive Indexes.
- (x) Enforcement Correspondence Control Index System.
- (xi) Document Vendors and Alterers Index.
- (xii) Informant Index.
- (xiii) Suspect Third Party Index.
- (xiv) Examination Correspondence Control Index.
- (xv) Extension Training Enrollee Index.
- (xvi) Intelligence Index.
- (xvii) Naturalization and Citizenship Indexes.
- (xviii) Personnel Investigations Unit Indexes.
- (xix) Service Look-Out Subsystem.
- (xx) White House and Attorney General Correspondence Control Index.
- (xxi) Fraudulent Document Center Index.
- (xxii) Emergency Reassignment Index.
- (xxiii) Alien Documentation, Identification, and Telecommunication (ADIT) System.

The exemptions apply to the extent that information in these subsystems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(3) The Immigration and Naturalization Service "National Automated Immigration Lookout System (NAILS) JUSTICE/INS-032." The exemptions apply only to the extent that records in the system are subject to exemptions pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosure pursuant to the routine uses published for these subsystems would permit the subject of a criminal or civil investigation to obtain valuable information concerning the nature of

## 28 CFR Ch. I (7-1-24 Edition)

that investigation and present a serious impediment to law enforcement.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in these subsystems would inform the subject of a criminal or civil investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and present a serious impediment to law enforcement.

(4) From subsection (e)(1) because in the course of criminal or civil investigations, the Immigration and Naturalization Service often obtains information concerning the violation of laws other than those relating to violations over which INS has investigative jurisdiction. In the interests of effective law enforcement, it is necessary that INS retain this information since it can aid in establishing patterns of criminal activity and provide valuable leads for those law enforcement agencies that are charged with enforcing other segments of the criminal law.

(5) From subsection (e)(2) because in a criminal or civil investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life or physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because these subsystems of records are exempt from individual access pursuant to subsection (j) of the Privacy Act of 1974.

**Department of Justice****§ 16.99**

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the Immigration and Naturalization Service's ability to issue administrative subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (g) because these subsystems of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(11) In addition, these systems of records are exempt from subsections (c)(3), (d), (e)(1), (e)(4)(G) and (H) to the extent they are subject to exemption pursuant to 5 U.S.C. 552a(k)(1). To permit access to records classified pursuant to Executive Order would violate the Executive Order protecting classified information.

(c) The Border Patrol Academy Index Subsystem is exempt from 5 U.S.C. 552a(d) and (f).

This exemption applies only to the extent that information in this subsystem is subject to exemption pursuant to 5 U.S.C. 552a(k).

(d) Exemptions for the particular subsections are justified for the following reasons.

(1) From subsection (d) because exemption is claimed only for those testing and examination materials used to determine an individual's qualifications for retention and promotion in the Immigration and Naturalization Service. This is necessary to protect

the integrity of testing materials and to insure fair and uniform examinations.

(2) From subsection (f) because the subsystem of records has been exempted from the access provisions of subsection (d).

(e) The Orphan Petitioner Index and Files (Justice/INS-007) system of records is exempt from 5 U.S.C. 552a(d). This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

(f) Exemption from paragraph (d) of this section is claimed solely because of the possibility of receipt of classified information during the course of INS investigation of prospective adoptive parents.

Although it would be rare, prospective adoptive parents may originally be from foreign countries (for example) and information received on them from their native countries may require classification under Executive Order 12356 which safeguards national security information. If such information is relevant to the INS determination with respect to adoption, the information would be kept in the file and would be classified accordingly. Therefore, access could not be granted to the record subject under the Privacy Act without violating E.O. 12356.

(g) The Office of Internal Audit Investigations Index and Records (Justice/INS-002) system of records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5) and (8); and (g), but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in the system are subject to exemption therefrom. In addition, this system of records is also exempt under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in the system are subject to exemption therefrom.

(h) The following justification apply to the exemptions from particular subsections:

(1) From subsection (c)(3) because the release of the disclosure accounting for

## § 16.99

## 28 CFR Ch. I (7-1-24 Edition)

disclosure could permit the subject of an actual or potential criminal or civil investigation to obtain valuable information concerning the existence and nature of the investigation, the fact that individuals are subjects of the investigation, and present a serious impediment to law enforcement.

(2) From subsection (c)(4) to the extent that the exemption from subsection (d) is applicable. Subsection (c)(4) will not be applicable to the extent that records in the system are properly withholdable under subsection (d).

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of a criminal or civil investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to their activities; of the identity of confidential sources, witnesses and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. Such disclosures would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation; endanger the physical safety of confidential sources, witnesses, and law enforcement personnel; and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to these records could result in a disclosure that would constitute an unwarranted invasion of the privacy of third parties. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because in the course of criminal or civil investigations, the Immigration and Naturalization Service often obtains information concerning the violation of laws other than those relating to violations over which INS has investigative jurisdiction, in the interests of effective law enforcement, it is necessary that INS retain this information since it can aid in establishing patterns of

criminal activity and provide valuable leads for those law enforcement agencies that are charged with enforcing other segments of the criminal law.

(5) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment of criminal law enforcement in that it could compromise the existence of a confidential investigation, reveal the identify of confidential sources of information and endanger the life or physical safety of confidential informants.

(7) From subsection (e)(5) because in the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to criminal law enforcement as this could interfere with the Immigration and Naturalization Service's ability to issue administrative subpoenas and could reveal investigative techniques and procedures.

(9) From subsection (g) for those portions of this system of records that

**Department of Justice****§ 16.99**

were compiled for criminal law enforcement purposes and which are subject to exemption from the access provisions of subsections (d) pursuant to subsection (j)(2).

(i) The Law Enforcement Support Center Database (LESC) (Justice/INS-023) system of records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4); (d); (e) (1), (2), (3), (5), (8) and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in the system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in the system are subject to exemption therefrom.

(j) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of a criminal or civil investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to their activities; and of information that may enable the subject to avoid detection or apprehension. Such disclosures would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation or other law enforcement operation such as deportation or exclusion. In addition, granting access to these records could result in a disclosure that would constitute an unwarranted invasion of the privacy of third parties. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to criminal law enforcement in that it could compromise the existence of a confidential investigation.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(k) The Attorney/Representative Complaint/Petition File (JUSTICE/INS-022) system of records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5), and (8); and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in this system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a (k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in this system are subject to exemption therefrom.

(l) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) for reasons stated in paragraph (h)(3) of this section.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

## § 16.100

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) for reasons stated in paragraph (h)(6) of this section.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

(m) The Worksite Enforcement Activity and Records Index (LYNX) (JUSTICE/INS-025) system of records is exempt under the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5), and (8); and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in this system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in this system are subject to exemption therefrom.

(n) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) for reasons stated in paragraph (h)(3) of this section.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) for reasons stated in paragraph (h)(6) of this section.

## 28 CFR Ch. I (7-1-24 Edition)

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 688-77, 42 FR 10001, Feb. 18, 1977; Order No. 6-84, 49 FR 20812, May 17, 1984; Order No. 25-88, 53 FR 41161, Oct. 20, 1988; Order No. 137-97, 62 FR 34169, June 25, 1997; Order No. 142-97, 62 FR 44083, Aug. 19, 1997; Order No. 196-2000, 65 FR 21139, Apr. 20, 2000; Order No. 197-2000, 65 FR 21140, Apr. 20, 2000]

## § 16.100 Exemption of Office of Justice Programs—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) The Civil Rights Investigative System (JUSTICE/OJP-008).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(b) Exemption from subsection (d) is claimed since access to information in the Civil Rights Investigative System prior to final administrative resolution will deter conciliation and compliance efforts. Consistent with the legislative purpose of the Privacy Act of 1974, decisions to release information from the system will be made on a case-by-case basis and information will be made available where it does not compromise the complaint and compliance process. In addition, where explicit promises of confidentiality must be made to a source during an investigation, disclosure will be limited to the extent that the identity of such confidential sources will not be compromised.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 5-78, 43 FR 36439, Aug. 17, 1978; Order No. 43-80, 45 FR 6780, Jan. 30, 1980; Order No. 6-86, 51 FR 15479, Apr. 24, 1986; Order No. 6-236-2001, 66 FR 35374, July 5, 2001]

**Department of Justice****§ 16.101 Exemption of U.S. Marshals Service Systems—limited access, as indicated.**

(a) The following system of records is exempt from 5 U.S.C. 552(a)(c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) Warrant Information System (JUSTICE/USM-007).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of disclosure accounting for disclosure made pursuant to subsection (b) of the Act, including those permitted under routine uses published for this system of records would permit a person to determine whether he is the subject of a criminal investigation, and to determine whether a warrant has been issued against him, and therefore present a serious impediment to law enforcement.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d) of the Act, this section is inapplicable.

(3) From subsection (d) because access to records would inform a person for whom a federal warrant has been issued of the nature and scope of information obtained as to his activities, of the identity of informants, and afford the person sufficient information to enable the subject to avoid apprehension. These factors would present a serious impediment to law enforcement in that they would thwart the warrant process and endanger lives of informants etc.

(4) From subsections (e)(1) and (e)(5) because the requirements of these subsections would present a serious impediment to law enforcement in that it is impossible to determine in advance what information collected during an investigation will be important or crucial to the apprehension of Federal fugitives. In the interest of effective law enforcement, it is appropriate in a thorough investigation to retain seemingly irrelevant, untimely, or inaccurate information which, with the passage of time, would aid in establishing patterns of activity and provide

**§ 16.101**

investigative leads toward fugitive apprehension and assist in law enforcement activities of other agencies.

(5) From subsection (e)(2) because the requirement that information be collected to the greatest extent practical from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the warrant and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal identity of confidential informants.

(7) From subsections (e)(4) (G) and (H) since an exemption is being claimed for subsections (f) and (d) of the Act, these subsections are inapplicable.

(8) From subsection (e)(8) because the individual notice requirement of this subsection would present a serious impediment to law enforcement in that it would give persons sufficient warning to avoid warrants, subpoena, etc.

(9) From subsection (f) because procedures for notice to an individual pursuant to subsection (f)(1) as to existence of records pertaining to him dealing with warrants must be exempted because such notice to individuals would be detrimental to the successful service of a warrant. Since an exemption is being claimed for subsection (d) of the Act the rules required pursuant to subsections (f) (2) through (5) are inapplicable to this system of records.

(10) From subsection (g) since an exemption is being claimed for subsection (d) and (f) this section is inapplicable and is exempted for the reasons set forth for these subsections.

(c) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e)(8), (f)(2) and (g):

(1) Witness Security System (JUSTICE/USM-008).

These exemptions apply only to the extent that information in this system is

## § 16.101

subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act including those permitted under routine uses published for this system of records would hamper the effective functioning of the Witness Security Program which by its very nature requires strict confidentiality vis-a-vis the records.

(2) From subsection (c)(4) for the reason stated in (b)(2) of this section.

(3) From subsection (d) because the U.S. Marshals Service Witness Security Program aids efforts of law enforcement officials to prevent, control or reduce crime. Access to records would present a serious impediment to effective law enforcement through revelation of confidential sources and through disclosure of operating procedures of the program, and through increased exposure of the program to the public.

(4) From subsection (e)(2) because in the Witness Security Program the requirement that information be collected to the greatest extent possible from the subject individual would constitute an impediment to the program, which is sometimes dependent on sources other than the subject witness for verification of information pertaining to the witness.

(5) From subsection (e)(3) for the reason stated in (b)(6) of this section.

(6) From subsection (e)(4) (G) and (H) for the reason stated in (b)(7) of this section.

(7) From subsection (e)(8) for the reason stated in (b)(8) of this section.

(8) From subsection (f)(2) since an exemption is being claimed for subsection (d) of the Act the rules required pursuant to subsection (f) (2) through (5) are inapplicable to this system of records.

(9) From subsection (g) for the reason stated in (b)(10) of this section.

(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g).

## 28 CFR Ch. I (7-1-24 Edition)

(1) Internal Affairs System (JUSTICE/USM-002)—Limited access. These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2) or (k)(5). Where compliance would not interfere with or adversely affect the law enforcement process, the USMS may waive the exemptions, either partially or totally.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3) and (d) to the extent that release of the disclosure accounting may impede or interfere with civil or criminal law enforcement efforts, reveal a source who furnished information to the Government in confidence, and/or result in an unwarranted invasion of the personal privacy of collateral record subjects or other third party individuals.

(2) From subsection (c)(4) for the reason stated in (b)(2) of this section.

(3) From subsection (e)(1) to the extent that it is necessary to retain all information in order not to impede, compromise, or interfere with civil or criminal law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law agencies in discharging their law enforcement responsibilities.

(4) From subsection (e)(2) because the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to compromise the investigation and avoid detection or apprehension.

(5) From subsection (e)(3) for the reason stated in (b)(6) of this section.

(6) From subsections (e)(4) (G) and (H) for the reason stated in (b)(7) of this section.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time,

**Department of Justice****§ 16.101**

seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes and interfere with the preparation of a complete investigative report or otherwise impede effective law enforcement.

(8) From subsection (e)(8) because the individual notice requirement of this subsection would present a serious impediment to law enforcement in that the subject of the investigation would be alerted as to the existence of the investigation and therefore be able to compromise the investigation and avoid detection, subpoena, etc.

(9) From subsection (f) because procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records dealing with investigations of criminal or civil law violations would enable the individual to compromise the investigation and evade detection or apprehension. Since an exemption is being claimed for subsection (d) of the Act, the rules required pursuant to subsections (f)(2) through (f)(5) are not applicable to this system.

(10) From subsection (g) for the reason stated in (b)(10) of this section.

(g) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) U.S. Marshals Service Threat Analysis Information System (JUSTICE/USM-009).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit a person to determine whether he or she has been identified as a specific threat to USMS protectees and to determine the need for countermeasures to USMS protective activities and thereby present a serious impediment to law enforcement.

(2) From subsection (c)(4) because it is inapplicable since an exemption is being claimed for subsection (d).

(3) From subsection (d) because to permit access to records would inform a person of the nature and scope of information obtained as to his or her threat-related activities and of the identity of confidential sources, and afford the person sufficient information to develop countermeasures to thwart protective arrangements and endanger lives of USMS protectees, informants, etc. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because the collection of investigatory information used to assess the existence, extent and likelihood of a threat situation necessarily includes material from which it is impossible to identify and segregate information which may not be important to the conduct of a thorough assessment. It is often impossible to determine in advance if all information collected is accurate, relevant, timely and complete but, in the interests of developing effective protective measures, it is necessary that the U.S. Marshals Service retain this information in order to establish patterns of activity to aid in accurately assessing threat situations. The restrictions of subsections (e)(1) and (5) would impede the protective responsibilities of the Service and could result in death or serious injury to Marshals Service protectees.

(5) From subsection (e)(2) because to collect information from the subject individual would serve notice that he or she is identified as a specific threat to USMS protectees and would enable the subject individual to develop countermeasures to protective activities and thereby present a serious impediment to law enforcement.

(6) From subsection (e)(3) because to inform individuals as required by this subsection would enable the subject individual to develop countermeasures to USMS protective arrangements or identify confidential sources and thereby present a serious impediment to law enforcement.

## § 16.101

## 28 CFR Ch. I (7-1-24 Edition)

(7) From subsections (e)(4) (G) and (H) because they are inapplicable since an exemption is being claimed for subsections (d) and (f) of the Act.

(8) From subsection (e)(8) because to serve notice would give persons sufficient warning to develop countermeasures to protective arrangements and thereby present a serious impediment to law enforcement through compromise of protective procedures, etc.

(9) From subsection (f) because this system of records is exempt from the provisions of subsection (d).

(10) From subsection (g) because it is inapplicable since an exemption is being claimed for subsections (d) and (f).

(i) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (d):

(1) Judicial Facility Security Index System (JUSTICE/USM-010)

These exemptions apply only to the extent that information in this system is exempt pursuant to 5 U.S.C. 552a(k)(5).

(j) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) only to the extent that release of the disclosure accounting would reveal the identity of a confidential source.

(2) From subsection (d) only to the extent that access to information would reveal the identity of a confidential source.

(k) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1), (2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) U.S. Marshals Service Freedom of Information/Privacy Act (FOIA/PA) Files (JUSTICE/USM-012).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(2) and (k)(5).

(l) Because this system contains Department of Justice civil and criminal law enforcement, investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the existence and nature of

the investigation and present a serious impediment to law enforcement.

(2) From subsection (c)(4) because that portion of this system which consists of investigatory records compiled for law enforcement purposes is being exempted from the provisions of subsection (d), rendering this provision not applicable.

(3) From subsection (d) because to permit access to investigatory records would reveal the identity of confidential sources and impede ongoing investigative or law enforcement activities by the premature disclosure of information related to those efforts. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (5) because it is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide leads in criminal investigations.

(5) From subsection (e)(2) because to collect information from the subject individual would serve notice that he or she is the subject of criminal investigative or law enforcement activity and thereby present a serious impediment to law enforcement.

(6) From subsection (e)(3) because to inform individuals as required by this subsection would enable the subject individual to identify confidential sources, reveal the existence of an investigation, and compromise law enforcement efforts.

(7) From subsections (e)(4) (G) and (H) because they are inapplicable since an exemption is being claimed for subsections (d) and (f) for investigatory records contained in this system.

(8) From subsection (e)(8) because to serve notice would give persons sufficient warning to evade law enforcement efforts.

(9) From subsection (f) because investigatory records contained in this system are exempt from the provisions of subsection (d).

(10) From subsection (g) because it is inapplicable since an exemption is being claimed for subsections (d) and (f).

(m) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e)(8), (f) and (g):

(1) U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files (JUSTICE/USM-013).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(5).

(n) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting for disclosures pursuant to the routine uses published for this system would permit the subject of a criminal or civil case or matter under investigation, or a case or matter in litigation, or under regulatory or administrative review or action, to obtain valuable information concerning the nature of that investigation, case or matter, and present a serious impediment to law enforcement or civil legal activities, or reveal a confidential source.

(2) From subsection (c)(4) because the exemption claimed for subsection (d) will make this section inapplicable.

(3) From subsection (d) because to permit access to records contained in this system would provide information concerning litigation strategy, or case development, and/or reveal the nature of the criminal or civil case or matter under investigation or administrative review, or in litigation, and present a serious impediment to law enforcement or civil legal activities, or reveal a confidential source.

(4) From subsection (e)(2) because effective legal representation, defense, or claim adjudication necessitates collecting information from all individuals having knowledge of the criminal or civil case or matter. To collect information primarily from the subject individual would present a serious impediment to law enforcement or civil legal activities.

(5) From subsection (e)(3) because to inform the individuals as required by this subsection would permit the sub-

ject of a criminal or civil matter under investigation or administrative review to compromise that investigation or administrative review and thereby impede law enforcement efforts or civil legal activities.

(6) From subsections (e)(4) (G) and (H) because these provisions are inapplicable since this system is exempt from subsections (d) and (f) of the Act.

(7) From subsection (e)(8) because to serve notice would give persons sufficient warning to compromise a criminal or civil investigation or administrative review and thereby impede law enforcement of civil legal activities.

(8) From subsection (f) because this system of records is exempt from the provisions of subsection (d).

(9) From subsection (g) because it is inapplicable since an exemption is claimed for subsections (d) and (f).

(o) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (1), (2), (5) and (g):

(1) U.S. Marshals Service Prisoner Transportation System (JUSTICE/USM-003).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(p) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) where the release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act would reveal a source who furnished information to the Government in confidence.

(2) From subsection (c)(4) to the extent that the system is exempt from subsection (d).

(3) From subsection (d) because access to records would reveal the names and other information pertaining to prisoners, including sensitive security information such as the identities and locations of confidential sources, *e.g.*, informants and protected witnesses; and disclose access codes, data entry codes and message routing symbols used in law enforcement communications systems to schedule and effect prisoner movements. Thus, such a compromise of law enforcement communications systems would subject law

## § 16.101

## 28 CFR Ch. I (7-1-24 Edition)

enforcement personnel and other prisoners to harassment and possible danger, and present a serious threat to law enforcement activities. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden by requiring that information affecting the prisoner's security classification be continuously re-investigated when contested by the prisoner, or by anyone on his behalf.

(4) From subsections (e) (1) and (5) because the security classification of prisoners is based upon information collected during official criminal investigations; and, in the interest of ensuring safe and secure prisoner movements it may be necessary to retain information the relevance, necessity, accuracy, timeliness, and completeness of which cannot be readily established, but which may subsequently prove useful in establishing patterns of criminal activity or avoidance, and thus be essential to assigning an appropriate security classification to the prisoner. The restrictions of subsection (e) (1) and (5) would impede the information collection responsibilities of the USMS, and the lack of all available information could result in death or serious injury to USMS and other law enforcement personnel, prisoners in custody, and members of the public.

(5) From subsection (e)(2) because the requirement to collect information from the subject individual would impede the information collection responsibilities of the USMS in that the USMS is often dependent upon sources other than the subject individual for verification of information pertaining to security risks posed by the individual prisoner.

(6) From subsection (g) to the extent that the system is exempt from subsection (d).

(q) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2), (3), (e)(5) and (e)(8) and (g):

(1) U.S. Marshals Service Prisoner Processing and Population Management System (JUSTICE/USM-005).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(r) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit the subject of a criminal proceeding to determine the extent or nature of law enforcement authorities' knowledge regarding his/her alleged misconduct or criminal activities. The disclosure of such information could alert the subject to devise ways in which to conceal his/her activities and/or prevent law enforcement from learning additional information about his/her activities, or otherwise inhibit law enforcement efforts. In addition, where the individual is the subject of an ongoing or potential inquiry/investigation, such release could reveal the nature thereof prematurely, and may also enable the subject to determine the identity of witnesses and informants. Such disclosure could compromise the ongoing or potential inquiry/investigation, endanger the lives of witnesses and informants, or otherwise impede or thwart law enforcement efforts.

(2) From subsection (c)(4) to the extent that the system is exempt from subsection (d).

(3) From subsection (d) because to permit unlimited access would permit the subject of a criminal proceeding to determine the extent or nature of law enforcement authorities' knowledge regarding his/her alleged misconduct or criminal activities. The disclosure of such information could alert the subject to devise ways in which to conceal his/her activities and/or prevent law enforcement from learning additional information about his/her activities, or otherwise inhibit law enforcement efforts. Disclosure would also allow the subject to obtain sensitive information concerning the existence and nature of security measures and jeopardize the safe and secure transfer of the prisoner, the safety and security of other prisoners, informants and witnesses, law enforcement personnel, and the public. In addition, disclosure may enable the subject to learn prematurely of an ongoing or potential inquiry/investigation, and may also permit him/her to determine the identities of confidential

sources, informants, or protected witnesses. Such disclosure could compromise the ongoing or potential inquiry/investigation, endanger the lives of witnesses and informants, or otherwise impede or thwart law enforcement efforts. Disclosure may also constitute an unwarranted invasion of the personal privacy of third parties. Further, disclosure would reveal access codes, data entry codes and message routing symbols used in law enforcement communications systems. Access to such codes and symbols would permit the subject to impede the flow of law enforcement communications and compromise the integrity of law enforcement information, and thus present a serious threat to law enforcement activities. To permit amendment of the records would expose security matters, and would impose an impossible administrative burden by requiring that security precautions, and information pertaining thereto, be continuously reevaluated if contested by the prisoner, or by anyone on his or her behalf. Similarly, to permit amendment could interfere with ongoing or potential inquiries/investigations by requiring that such inquiries/investigations be continuously reinvestigated, or that information collected (the relevance and accuracy of which cannot readily be determined) be subjected to continuous change.

(4) From subsections (e)(1) and (5) because the system may contain investigatory information or information which is derived from information collected during official criminal investigations. In the interest of effective law enforcement and litigation, of securing the prisoner and of protecting the public, it may be necessary to retain information the relevance, necessity, accuracy, timeliness and completeness of which cannot be readily established. Such information may nevertheless provide investigative leads to other Federal or law enforcement agencies, or prove necessary to establish patterns of criminal activity or behavior, and/or prove essential to the safe and secure detention (and movement) of prisoners. Further, the provisions of (e)(1) and (e)(5) would restrict the ability of the USMS in exercising its judgment in reporting information during

investigations or during the development of appropriate security measures, and thus present a serious impediment to law enforcement efforts.

(5) From subsection (e)(2) because the requirement to collect information from the subject individual would impede the information collection responsibilities of the USMS which is often dependent upon sources other than the subject individual for verification of information pertaining to security risks posed by the individual prisoner, to alleged misconduct or criminal activity of the prisoner, or to any matter affecting the safekeeping and disposition of the individual prisoner.

(6) From subsection (e)(3) because to inform individuals as required by this subsection could impede the information gathering process, reveal the existence of an ongoing or potential inquiry/investigation or security procedure, and compromise law enforcement efforts.

(7) From subsection (e)(8) because to serve notice would give persons sufficient warning to compromise an ongoing or potential inquiry/investigation and thereby evade and impede law enforcement and security efforts.

(8) From subsection (g) to the extent that the system is exempt from subsection (d).

(s) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (1), (2), (3), (e) (5) and (e) (8) and (g):

Joint Automated Booking Stations,  
Justice/USM-014

(t) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not interfere with or adversely affect the law enforcement process, the USMS may waive the exemptions, either partially or totally. Exemption from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3) and (d) to the extent that access to records in this system of records may impede or interfere with law enforcement efforts, result in the disclosure of information that would constitute an unwarranted invasion of the personal privacy of collateral record subjects or other third

## § 16.101

## 28 CFR Ch. I (7-1-24 Edition)

parties, and/or jeopardize the health and/or safety of third parties.

(2) Where access to certain records may be appropriate, exemption from the amendment provisions of subsection (d)(2) is necessary to the extent that the necessary and appropriate justification, together with proof of record inaccuracy, is not provided, and/or to the extent that numerous, frivolous requests to amend could impose an impossible administrative burden by requiring agencies to continuously review booking and arrest data, much of which is collected from the arrestee during the arrest.

(3) From subsection (e)(1) to the extent that it is necessary to retain all information in order not to impede, compromise, or interfere with law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law enforcement agencies in discharging their law enforcement responsibilities.

(4) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement since it may be necessary to obtain and verify information from a variety of sources other than the record subject to ensure safekeeping, security, and effective law enforcement. For example, it may be necessary that medical and psychiatric personnel provide information regarding the subject's behavior, physical health, or mental stability, etc. To ensure proper care while in custody, or it may be necessary to obtain information from a case agent or the court to ensure proper disposition of the subject individual.

(5) From subsection (e)(3) because the requirement that agencies inform each individual whom it asks to supply information of such information as is required by subsection (e)(3) may, in some cases, impede the information gathering process or otherwise interfere with or compromise law enforcement efforts, e.g., the subject may deliberately withhold information, or give erroneous information.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible

to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes and may prevent the eventual development of the necessary criminal intelligence or otherwise impede effective law enforcement.

(7) From subsection (e)(8) to the extent that such notice may impede, interfere with, or otherwise compromise law enforcement and security efforts.

(8) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(u) Consistent with the legislative purpose of the Privacy Act of 1974, the United States Marshals Service will grant access to nonexempt material in records which are maintained by the Service. Disclosure will be governed by the Department's Privacy Regulations, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal, civil or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 8-83, 48 FR 19024, Apr. 27, 1983; Order No. 10-86, 51 FR 20275, June 4, 1986; Order No. 11-86, 51 FR 20277, June 4, 1986; Order No. 61-92, 57 FR 3284, Jan. 29, 1992; Order No. 66-92, 57 FR 20654, May 14, 1992; Order No. 105-95, 60 FR 30467, June 9, 1995; Order No. 212-2001, 66 FR 6470, Jan. 22, 2001]

**Department of Justice****§ 16.102****§ 16.102 Exemption of Drug Enforcement Administration and Immigration and Naturalization Service Joint System of Records.**

(a) The following system of records is exempted pursuant to provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H), and (I), (e)(5) and (8), (f), (g), and (h) of 5 U.S.C. 552a; in addition the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552 (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of 5 U.S.C. 552a.

(1) Automated Intelligence Record System (Pathfinder), JUSTICE/DEA-INS-111.

These exemptions apply to the extent that information in those systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) The system of records listed under paragraph (a) of this section is exempted, for the reasons set forth from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3)(d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, or the nature and

scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4)(e)(1). The notices of these systems of records published in the FEDERAL REGISTER set forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal or other law enforcement investigations, cases, and matters, the Immigration and Naturalization Service or the Drug Enforcement Administration will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(5)(e)(2). In a criminal investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6)(e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise

## § 16.103

## 28 CFR Ch. I (7-1-24 Edition)

the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Rules) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent that these systems of records are exempted from subsections (f) and (d).

(8)(e)(4)(I). The categories of sources of the records in these systems have been published in the FEDERAL REGISTER in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9)(e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or poten-

tial criminal, civil, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the rules required pursuant to subsections (f) (2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(12)(g). Since an exemption is being claimed for subsections (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(13)(h). Since an exemption is being claimed for subsection (d) (Access to Records) and (f) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for those subsections, to the extent that these systems of records are exempted from subsections (d) and (f).

(14) In addition, exemption is claimed for these systems of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provisions of 5 U.S.C. 552a(k)(1): subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) to the extent that the records contained in these systems are specifically authorized to be kept secret in the interests of national defense and foreign policy.

[Order No. 742-77, 42 FR 40907, Aug. 12, 1977]

### § 16.103 Exemption of the INTERPOL-United States National Central Bureau (INTERPOL-USNCB) System.

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4),

**Department of Justice****§ 16.104**

(d), (e) (1), (2), and (3), (e)(4) (G) and (H), (e)(5) and (8), (f) and (g):

(1) The INTERPOL-United States National Central Bureau (INTERPOL-USNCB) (Department of Justice) INTERPOL-USNCB Records System (JUSTICE/INTERPOL-001).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of accounting disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement.

(2) From subsections (c)(4), (d), (e)(4) (G), and (H), (f) and (g) because these provisions concern individual access to records and such access might compromise ongoing investigations reveal investigatory techniques and confidential informants, and invade the privacy of private citizens who provide information in connection with a particular investigation.

(3) From subsection (e)(1) because information received in the course of an international criminal investigation may involve a violation of state or local law, and it is beneficial to maintain this information to provide investigative leads to state and local law enforcement agencies.

(4) From subsection (e)(2) because collecting information from the subject of criminal investigations would thwart the investigation by placing the subject on notice.

(5) From subsection (e)(3) because supplying an individual with a statement of the intended use of the requested information could compromise the existence of a confidential investigation, and may inhibit cooperation.

(6) From subsection (e)(5) because the vast majority of these records come from local criminal justice agencies and it is administratively impossible to ensure that the records comply with this provision. Submitting agencies are, however, urged on a continuing

basis to ensure that their records are accurate and include all dispositions.

(7) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

[Order No. 8-82, 47 FR 44255, Oct. 7, 1982, as amended by Order No. 6-86, 51 FR 15479, Apr. 24, 1986]

**§ 16.104 Exemption of Office of Special Counsel—Waco System.**

(a) The following system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k): CaseLink Document Database for Office of Special Counsel—Waco, JUSTICE/OSCW-001. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(b) Only that portion of this system which consists of criminal or civil investigatory information is exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3)*. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him or her would inform that individual of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties and civil remedies.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others.

(4) *Subsection (d)(2)*. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring

## § 16.105

## 28 CFR Ch. I (7-1-24 Edition)

criminal investigations to be continuously reinvestigated.

(5) *Subsections (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsections (e)(1) and (5).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete; but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide leads in criminal investigations.

(7) *Subsection (e)(2).* To collect information from the subject individual would serve notice that he or she is the subject of criminal investigative or law enforcement activity and thereby present a serious impediment to law enforcement.

(8) *Subsection (e)(3).* To inform individuals as required by this subsection would reveal the existence of an investigation and compromise law enforcement efforts.

(9) *Subsection (e)(8).* To serve notice would give persons sufficient warning to evade law enforcement efforts.

(10) *Subsection (g).* This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 208-2000, 65 FR 75160, Dec. 1, 2000]

### § 16.105 Exemption of Foreign Terrorist Tracking Task Force System.

(a) The following system of records is exempt from 5 U.S.C. 552a, subsections (c)(3), (d)(1), (2), (3) and (4), and (e)(1) and (4)(I): Flight Training Candidates File System (JUSTICE/FTTTF-001). This exemption applies only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

(b) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures could reveal information that is classified in the interest of national security.

(2) From subsection (d)(1), (2), (3) and (4) because access to and amendment of certain portions of records within the system would tend to reveal or com-

promise information classified in the interest of national security.

(3) From subsection (e)(1) because it is often impossible to determine in advance if information obtained will be relevant for the purposes of conducting the risk analysis for flight training candidates.

(4) From subsection (e)(4)(I) to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than have been published in the FEDERAL REGISTER. Should the subsection be so interpreted, exemption from this provision is necessary because greater specificity concerning the sources of these records could compromise national security.

[Order No. 278-2002, 67 FR 51756, Aug. 9, 2002]

### § 16.106 Exemption of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—Limited Access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d)(1), (2), (3) and (4), (e)(1), (2), and (3), (e)(4)(G), (H) and (I), (e)(5) and (8), (f) and (g).

(1) Criminal Investigation Report System (JUSTICE/ATF-003).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest not only of ATF, but also of the recipient agency. This would permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.

(2) From subsection (c)(4) because an exemption being claimed for subsection (d) makes this subsection inapplicable.

(3) From subsections (d)(1), (e)(4)(G) and (H), (f) and (g) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information, including actual or potential tax information, which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(4) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because: (i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) In any investigation, ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or

to an investigative activity under the jurisdiction of another agency.

(7) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(8) From subsection (e)(3) because disclosure would provide the subject with substantial information that could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take steps to evade the investigation or flee a specific area.

(9) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the **FEDERAL REGISTER** in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(10) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting

## § 16.106

the subject of a criminal or other investigation of existing investigative interest.

(c) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Internal Security Record System (JUSTICE/ATF-006).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2) and (k)(5). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement investigation, and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or other measures.

(2) From subsection (d)(1) because disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Such breaches would restrict the free flow of information which is vital to the law enforcement process and the determination of an applicant's qualifications.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

## 28 CFR Ch. I (7-1-24 Edition)

(5) From subsection (e)(1) because it is often impossible to determine in advance if investigative records contained in this system are accurate, relevant, timely, complete, or of some assistance to either effective law enforcement investigations, or to the determination of the qualifications and suitability of an applicant. It also is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads. Information that may appear irrelevant, when combined with other apparently irrelevant information, can on occasion provide a composite picture of a subject or an applicant which assists the law enforcement process and the determination of an applicant's suitability qualifications.

(6) From subsection (e)(4)(G) and (H), and (f) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information, interfere with the overall law enforcement or qualification process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel. In addition, disclosure of information collected pursuant to an employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the objectivity or fairness of a testing or examination process.

(7) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the FEDERAL REGISTER in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to

**Department of Justice****§ 16.106**

protect the privacy and physical safety of witnesses and informants.

(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Personnel Record System (JUSTICE/ATF-007).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(5). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal the existence, nature, or scope of an actual or potential personnel action. This would permit the record subject to take measures to hamper or impede such actions.

(2) From subsections (d)(1), (e)(4)(G) and (H), and (f) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a position with ATF. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of ATF. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of

specific information in the early stages of a personnel-related action.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

(6) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the FEDERAL REGISTER in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(g) The following systems of records are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Regulatory Enforcement Record System (JUSTICE/ATF-008).

(2) Technical and Scientific Services Record System (JUSTICE/ATF-009).

(3) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

## § 16.130

## 28 CFR Ch. I (7-1-24 Edition)

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest, whether civil, criminal or regulatory, not only of ATF, but also of the recipient agency. This would permit the record subject to take measures to impede the investigation, *e.g.*, destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation thus seriously hampering the regulatory and law enforcement functions of ATF.

(2) From subsections (d)(1), (e)(4)(G) and (H), and (f) because these provisions concern individual access to investigative and compliance records, disclosure of which could compromise sensitive information, interfere with the overall law enforcement and regulatory process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information, including actual or potential tax information, which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations and compliance actions attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal, civil, regulatory, or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative or regulatory activity can be established.

(iii) In any investigation or compliance action ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or compliance action or to an investigative activity under the jurisdiction of another agency.

(6) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the **FEDERAL REGISTER** in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal, regulatory, and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

[Order No. 002-2003, 68 FR 3393, Jan. 24, 2003]

### **§ 16.130 Exemption of Department of Justice Systems: Correspondence Management Systems for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).**

(a) The following Department of Justice systems of records are exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to

**Department of Justice****§ 16.131**

5 U.S.C. 552a(j) and (k). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(1) Correspondence Management Systems (CMS) for the Department of Justice (DOJ), DOJ/003.

(2) Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ), DOJ/004.

(b) These systems are exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3)*. To provide the subject of a criminal, civil, or counterintelligence matter or case under investigation with an accounting of disclosures of records concerning him or her could inform that individual of the existence, nature, or scope of that investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) *Subsection (d)(2)*. Amendment of the records would interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously re-investigated.

(5) *Subsections (d)(3) and (4)*. These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsection (e)(1)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effec-

tive law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2)*. To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) *Subsection (e)(5)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8)*. To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g)*. This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 241-2001, 66 FR 41445, Aug. 8, 2001; 66 FR 43308, Aug. 17, 2001]

**§ 16.131 Exemption of Department of Justice (DOJ)/Nationwide Joint Automated Booking System (JABS), DOJ-005.**

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (2), (3), (4)(G) and (H), (e)(5) and (8), (f) and (g): Nationwide Joint Automated Booking System, Justice/DOJ-005. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Where compliance would not interfere with or adversely affect the law enforcement process, the DOJ may waive the exemptions, either partially or totally.

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3), (c)(4), and (d) to the extent that access to records in this system of records may impede

## § 16.132

## 28 CFR Ch. I (7-1-24 Edition)

or interfere with law enforcement efforts, result in the disclosure of information that would constitute an unwarranted invasion of the personal privacy of collateral record subjects or other third parties, and/or jeopardize the health and/or safety of third parties.

(2) From subsection (e)(1) to the extent that it is necessary to retain all information in order not to impede, compromise, or interfere with law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law enforcement agencies in discharging their law enforcement responsibilities.

(3) From subsection (e)(2) because, in some instances, the application of this provision would present a serious impediment to law enforcement since it may be necessary to obtain and verify information from a variety of sources other than the record subject to ensure safekeeping, security, and effective law enforcement. For example, it may be necessary that medical and psychiatric personnel provide information regarding the subject's behavior, physical health, or mental stability, etc. to ensure proper care while in custody, or it may be necessary to obtain information from a case agent or the court to ensure proper disposition of the subject individual.

(4) From subsection (e)(3) because the requirement that agencies inform each individual whom it asks to supply information of such information as is required by subsection (e)(3) may, in some cases, impede the information gathering process or otherwise interfere with or compromise law enforcement efforts, e.g., the subject may deliberately withhold information, or give erroneous information.

(5) From subsection (4)(G) and (H) because the application of these provisions would present a serious impediment to law enforcement efforts.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely infor-

mation may acquire new significance and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes, may prevent the eventual development of the necessary criminal intelligence, or otherwise impede law enforcement or delay trained law enforcement personnel from timely exercising their judgment in managing the arrestee.

(7) From subsection (e)(8) to the extent that such notice may impede, interfere with, or otherwise compromise law enforcement and security efforts.

(8) From subsection 5 U.S.C. 552a(f) to the extent that compliance with the requirement for procedures providing individual access to records, compliance could impede, compromise, or interfere with law enforcement efforts.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

[Order No. 242-2001, 66 FR 41445, Aug. 8, 2001; 66 FR 44308, Aug. 17, 2001]

### § 16.132 Exemption of Department of Justice System—Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006.

(a) The following Department of Justice system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k): Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(b) Exemption from the particular subsections is justified for the following reasons:

(1) *Subsection (c)(3).* To provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence,

nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) *Subsection (c)(4).* This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) *Subsection (d)(1).* Disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) *Subsection (d)(2).* Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously re-investigated.

(5) *Subsections (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsection (e)(1).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2).* To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) *Subsection (e)(3).* To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) *Subsection (e)(5).* It is often impossible to determine in advance if investigatory records contained in this sys-

tem are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8).* To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g).* This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 297-2002, 67 FR 70163, Nov. 21, 2002]

#### **§ 16.133 Exemption of Department of Justice Regional Data Exchange System (RDEX), DOJ-012.**

(a) The Department of Justice Regional Data Exchange System (RDEX), DOJ-012, is exempted from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) This system is exempted from the following subsections for the reasons set forth below:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures of criminal law enforcement records concerning him or her could inform that individual of the existence, nature, or scope of an investigation, or could otherwise seriously impede law enforcement efforts.

(2) From subsection (c)(4) because this system is exempt from subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of criminal law enforcement information could interfere with an investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others.

(4) From subsection (d)(2) because amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously re-investigated.

## § 16.134

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent that exemption is claimed from subsections (d)(1) and (2).

(6) From subsection (e)(1) because it is often impossible to determine in advance if criminal law enforcement records contained in this system are relevant and necessary, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) From subsection (e)(2) because collecting information from the subject individual could serve notice that he or she is the subject of a criminal law enforcement matter and thereby present a serious impediment to law enforcement efforts. Further, because of the nature of criminal law enforcement matters, vital information about an individual frequently can be obtained only from other persons who are familiar with the individual and his or her activities and it often is not practicable to rely on information provided directly by the individual.

(8) From subsection (e)(3) because informing individuals as required by this subsection could reveal the existence of a criminal law enforcement matter and compromise criminal law enforcement efforts.

(9) From subsection (e)(5) because it is often impossible to determine in advance if criminal law enforcement records contained in this system are accurate, relevant, timely, and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and obtaining investigative leads.

(10) From subsection (e)(8) because serving notice could give persons sufficient warning to evade criminal law enforcement efforts.

(11) From subsection (g) to the extent that this system is exempt from other specific subsections of the Privacy Act.

[Order No. 007-2005, 70 FR 49870, Aug. 25, 2005]

### § 16.134 Exemption of Debt Collection Enforcement System, Justice/DOJ-016.

(a) The following system of records is exempt pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4); (d)(1),

## 28 CFR Ch. I (7-1-24 Edition)

(2), (3), and (4); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f) and (g) of the Privacy Act. In addition, the system is exempt pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d)(1), (2), (3), and (4); (e)(1); (4)(G), (H), and (I); and (f). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the DOJ in its sole discretion.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because certain records in this system are exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative interest in the individual. Revealing this information may thus compromise ongoing law enforcement efforts. Revealing this information may also permit the record subject to take measures to impede the investigation, such as destroying evidence, intimidating potential witnesses or fleeing the area to avoid the investigation.

(2) From subsection (c)(4) notification requirements because certain records in this system are exempt from the access and amendment provisions of subsection (d) as well as the access to accounting of disclosures provision of subsection (c)(3).

(3) From subsections (d)(1), (2), (3), and (4) because access to the records contained in this system might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation.

**Department of Justice****§ 16.135**

Amendment of the records would interfere with ongoing debt collection investigations or other law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes.

(5) From subsection (e)(2) to avoid impeding law enforcement efforts associated with debt collection by putting the subject of an investigation on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that investigation.

(6) From subsection (e)(3) to avoid impeding law enforcement efforts in conjunction with debt collection by putting the subject of an investigation on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that investigation.

(7) From subsection (e)(4)(G), (H) and (I) because portions of this system are exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (e)(5) because many of the records in this system are records contributed by other agencies and the restrictions imposed by (e)(5) would limit the utility of the system.

(9) From subsection (e)(8), because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on the DOJ and may alert the subjects of law enforcement investigations, who might be otherwise unaware, to the fact of those investigations.

(10) From subsections (f) and (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 009-2012, 77 FR 23117, Apr. 18, 2012]

**§ 16.135 Exemptions of Executive Office for Organized Crime Drug Enforcement Task Forces Systems.**

(a) The following systems of records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3),

(4)(G), (H), and (I), (5), and (8); (f); and (g):

(1) The Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS) (JUSTICE/OCDETF-001); and

(2) The Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System (JUSTICE/OCDETF-002).

(b) These exemptions apply only to the extent that information is subject to exemption under 5 U.S.C. 552a(j) and/or (k).

(c) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide the subject with an accounting of disclosures of records in these systems could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation by the Organized Crime Drug Enforcement Task Forces, the Organized Crime Drug Enforcement Task Force Fusion Center, the International Organized Crime Intelligence and Operations Center, or the recipient agency, and could permit that individual to take measures to avoid detection or apprehension, to learn of the identity of witnesses and informants, or to destroy evidence, and would therefore present a serious impediment to law enforcement or counterintelligence efforts. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record. Moreover, release of an accounting may reveal information that is properly classified pursuant to Executive Order.

(2) From subsection (c)(4) because this subsection is inapplicable to the extent that an exemption is being claimed for subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of records in the system could alert the subject of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his or her activities, of the identity of confidential witnesses and informants, of the investigative interest of

**§ 16.135****28 CFR Ch. I (7-1-24 Edition)**

the Organized Crime Drug Enforcement Task Forces, the Organized Crime Drug Enforcement Task Force Fusion Center, the International Organized Crime Intelligence and Operations Center, and other intelligence or law enforcement agencies (including those responsible for civil proceedings related to laws against drug trafficking or related financial crimes or international organized crime); could lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or could otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life, health, and physical safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Access to records could also result in the release of information properly classified pursuant to Executive Order.

(4) From subsection (d)(2) because amendment of the records thought to be inaccurate, irrelevant, incomplete, or untimely would also interfere with ongoing investigations, criminal or civil law enforcement proceedings, and other law enforcement activities; would impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised; and may impact information properly classified pursuant to Executive Order.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent that exemption is claimed from subsections (d)(1) and (2) and for the reasons stated in § 16.135(c)(3) and (c)(4).

(6) From subsection (e)(1) because, in the course of their acquisition, collation, and analysis of information under the statutory authority granted, the Organized Crime Drug Enforcement Task Forces, the Organized Crime Drug Enforcement Task Force Fusion Center, and the International Organized Crime Intelligence and Operations Center will occasionally obtain informa-

tion, including information properly classified pursuant to Executive Order, that concerns actual or potential violations of law that are not strictly within their statutory or other authority or may compile and maintain information which may not be relevant to a specific investigation or prosecution. This is because it is impossible to determine in advance what information collected during an investigation or in support of these mission activities will be important or crucial to an investigation. In the interests of effective law enforcement, it is necessary to retain such information in these systems of records because it can aid in establishing patterns of criminal activity of a suspect and can provide valuable leads for federal and other law enforcement agencies. This consideration applies equally to information acquired from, or collated or analyzed for, both law enforcement agencies and agencies of the U.S. foreign intelligence community and military community.

(7) From subsection (e)(2) because in a criminal, civil, or regulatory investigation, prosecution, or proceeding, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation, prosecution, or proceeding would be placed on notice as to the existence and nature of the investigation, prosecution, or proceeding and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Moreover, thorough and effective investigation and prosecution may require seeking information from a number of different sources.

(8) From subsection (e)(3) because to comply with the requirements of this subsection during the course of an investigation could impede the information-gathering process, thus hampering the investigation or intelligence gathering. Disclosure to an individual of investigative interest would put the subject on notice of that fact and allow the subject an opportunity to engage in conduct intended to impede that activity or avoid apprehension. Disclosure to other individuals would likewise put

them on notice of what might still be a sensitive law enforcement interest and could result in the further intentional or accidental disclosure to the subject or other inappropriate recipients, convey information that might constitute unwarranted invasions of the personal privacy of other persons, unnecessarily burden law enforcement personnel in information-collection activities, and chill the willingness of witnesses to cooperate.

(9) From subsections (e)(4)(G) and (H) because this system is exempt from the access and amendment provisions of subsection (d).

(10) From subsection (e)(4)(I) to the extent that this subsection could be interpreted to require more detail regarding system record sources than has been published in the FEDERAL REGISTER. Should this subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and other information sources. Further, greater specificity could compromise other sensitive law enforcement information, techniques, and processes.

(11) From subsection (e)(5) because the acquisition, collation, and analysis of information for law enforcement purposes from various agencies does not permit a determination in advance or a prediction of what information will be matched with other information and thus whether it is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light, and the accuracy of such information can often only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys to exercise their judgment in collating and analyzing information and would impede the development of criminal or other intelligence necessary for effective law enforcement.

(12) From subsection (e)(8) because the individual notice requirements could present a serious impediment to

law enforcement by revealing investigative techniques, procedures, evidence, or interest, and by interfering with the ability to issue warrants or subpoenas; could give persons sufficient warning to evade investigative efforts; and would pose an unacceptable administrative burden on the maintenance of these records and the conduct of the underlying investigations.

(13) From subsections (f) and (g) because these subsections are inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 006-2013, 78 FR 69754, Nov. 21, 2013; 78 FR 77586, Dec. 24, 2013]

**§ 16.136 Exemption of the Department of Justice, Giglio Information System, Justice/DOJ-017.**

(a) The Department of Justice, Giglio Information Files (JUSTICE/DOJ-017) system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f); and (g) of the Privacy Act. These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because this subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(2) From subsection (c)(4) because this subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(3) From subsection (d) because access to the records contained in this system may interfere with or impede an ongoing investigation as it may be related to allegations against an agent or witness who is currently being investigated. Further, other records that are derivative of the subject's employing agency files may be accessed through the employing agency's files.

(4) From subsection (e)(1) because it may not be possible to determine in advance if potential impeachment records collected and maintained in order to sufficiently meet the Department's *Giglio* requirements and obligations are all relevant and necessary. In

## § 16.137

order to ensure that the Department's prosecutors and investigative agencies receive sufficient information to meet their obligations under *Giglio*, it is appropriate to maintain potential impeachment information in accordance with Department policy as such records could later be relevant and necessary in a different case in which the same witness or affiant subsequently testifies.

(5) From subsection (e)(2) because collecting information directly from the subject individual could serve notice that the individual is the subject of investigation and because of the nature of the records in this system, which are used to impeach or demonstrate bias of a witness, requires that the information be collected from others.

(6) From subsection (e)(3) because federal law enforcement officers receive notice from their supervisors and prosecuting attorneys that impeachment information may be used at trial. Law enforcement officers are also given notice by the *Giglio* decision itself.

(7) From subsections (e)(4)(G), (H), and (I) because this system of records is exempt from the access and amendment provisions of subsection (d).

(8) From subsection (e)(5) because it may not be possible to determine in advance if all potential impeachment records collected and maintained in order to sufficiently meet the Department's *Giglio* requirements and obligations are all accurate, relevant, timely, and complete at the time of collection. Although the Department has policies in place to verify the records, the records may be originated from another agency, third party, or open source media and it may be impossible to ensure the accuracy, relevance, timeliness, and completeness of potential impeachment information maintained prior to and during the process of being verified.

(9) From subsection (e)(8) because the nature of the *Giglio* discovery process renders notice of compliance with the compulsory discovery process impractical.

(10) From subsections (f) and (g) because these subsections are inapplicable to the extent that the system is

## 28 CFR Ch. I (7-1-24 Edition)

exempt from other specific subsections of the Privacy Act.

[Order No. 008-2015, 80 FR 34051, June 15, 2015]

### § 16.137 Exemption of the Department of Justice Insider Threat Program Records—limited access.

(a) The Department of Justice Insider Threat Program Records (JUSTICE/DOJ-018) system of records is exempted from subsections 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2) and (3); (e)(4)(G), (H) and (I); (e)(5) and (8); (f) and (g) of the Privacy Act. These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where DOJ determines compliance would not appear to interfere with or adversely affect the purpose of this system to detect, deter, and/or mitigate insider threats, the applicable exemption may be waived by the DOJ in its sole discretion.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning him/her would specifically reveal any insider threat-related interest in the individual by the DOJ or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and/or mitigate insider threats. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to impede the investigation, e.g., destroy evidence or flee the area to avoid the investigation.

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the accounting of disclosures provision of subsection (c)(3). The DOJ

takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of DOJ records, it will share that information in appropriate cases.

(3) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), (e)(8), (f) and (g) because these provisions concern individual access to and amendment of law enforcement, intelligence and counter-intelligence, and counterterrorism records, and compliance with these provisions could alert the subject of an authorized law enforcement or intelligence activity about that particular activity and the interest of the DOJ and/or other law enforcement or intelligence agencies. Providing access could compromise or lead to the compromise of information classified to protect national security; disclose information that would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; disclose or lead to disclosure of information that would allow a subject to avoid detection or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, or witnesses.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. The relevance and utility of certain information that may have a nexus to insider threats may not always be fully evident until and unless it is vetted and matched with other information necessarily and lawfully maintained by the DOJ.

(5) From subsection (e)(2) and (3) because application of these provisions could present a serious impediment to efforts to detect, deter and/or mitigate insider threats. Application of these provisions would put the subject of an investigation on notice of the investigation and allow the subject an opportunity to engage in conduct intended to impede the investigative activity or avoid apprehension.

(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding

the record sources in this system than has been published in the FEDERAL REGISTER. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the DOJ. Further, greater specificity of sources of properly classified records could compromise national security.

(7) From subsection (e)(5) because in the collection of information for authorized law enforcement and intelligence purposes, including efforts to detect, deter, and/or mitigate insider threats, due to the nature of investigations and intelligence collection, the DOJ often collects information that may not be immediately shown to be accurate, relevant, timely, and complete, although the DOJ takes reasonable steps to collect only the information necessary to support its mission and investigations. Additionally, the information may aid DOJ in establishing patterns of activity and provide criminal or intelligence leads. It could impede investigative progress if it were necessary to assure relevance, accuracy, timeliness and completeness of all information obtained throughout the course and within the scope of an investigation. Further, some of the records in this system may come from other domestic or foreign government entities, or private entities, and it would not be administratively feasible for the DOJ to vouch for the compliance of these agencies with this provision.

[82 FR 43176, Sept. 14, 2017]

**§ 16.138 Exemption of the Department of Justice Information Technology, Information System, and Network Activity and Access Records, JUSTICE/DOJ-002.**

(a) The Department of Justice Information Technology, Information System, and Network Activity and Access Records (JUSTICE/DOJ-002) system of records is exempted from subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act of 1974, as amended. The exemptions in this paragraph (a) apply only to the extent that information in

**§ 16.139****28 CFR Ch. I (7-1-24 Edition)**

this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1) or (k)(2). The applicable exemption may be waived by the DOJ in its sole discretion where DOJ determines compliance with the exempted provisions of the Act would not interfere with or adversely affect the purpose of this system of records to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and DOJ information systems.

(b) Exemptions from the particular subsections listed in paragraph (a) of this section are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system of records is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning the subject would specifically reveal investigative interests in the records by the DOJ or other entities that are recipients of the disclosures. Revealing this information could compromise sensitive information classified in the interest of national security, or interfere with the overall law enforcement process by revealing a pending sensitive cybersecurity investigation. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to impede the investigation, *e.g.*, destroy evidence or alter techniques to evade discovery.

(2) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), and (f) because these provisions concern individual access to and amendment of records, compliance with which regarding certain law enforcement and classified records could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the DOJ and/or other law enforcement or intelligence agencies.

Providing access could compromise information classified to protect national security, or reveal sensitive cybersecurity investigative techniques; provide information that would allow a subject to avoid detection; or constitute a potential danger to the health or safety of law enforcement personnel or confidential sources.

(3) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. The relevance and utility of certain information that may have a nexus to cybersecurity threats may not always be fully evident until and unless it is vetted and matched with other information lawfully maintained by the DOJ or other entities.

(4) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the FEDERAL REGISTER. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information. Further, greater specificity of sources of properly classified records could compromise national security.

[CPCLO Order No. 010-2021, 86 FR 61689, Nov. 8, 2021]

**§ 16.139 Exemption of the Department of Justice Data Protection Review Court Records System, JUSTICE/OPCL-001.**

(a) The Department of Justice Data Protection Review Court system of records JUSTICE/OPCL-001 is exempted from subsections 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2) and (3); (e)(4)(G), (H) and (I); (e)(5) and (8); (f) and (g) of the Privacy Act. These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where DOJ determines that compliance would not appear to interfere with or adversely affect the purpose of this system to address certain violations of United States law in the conduct of United States signals intelligence activities, and not interfere with national security or law enforcement operations, the applicable

exemption may be waived by the DOJ in its sole discretion.

(b) Exemptions from these particular subsections are justified for the following reasons:

(1) From the subsection (c)(3) (accounting of disclosures) requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Where the individual is the subject of intelligence activities, to provide that individual with the disclosure accounting records would hinder authorized United States intelligence activities by informing that individual of the existence, nature, or scope of information that is properly classified pursuant to Executive Order 12958, as amended, and thereby cause damage to the national security. Revealing this information would also be contrary to Executive Order 14086 and could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and/or mitigate national security threats.

(2) From subsection (c)(4) (notice of amendment to record recipients) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the provision for making the accounting of disclosures available to an individual in subsection (c)(3). The DOJ takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of DOJ records, it will share that information in appropriate cases.

(3) From subsection (d)(1), (2), (3) and (4) (record subject's right to access and amend records), (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents), (e)(8) (notice of compelled disclosures), (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees) and (g) (civil remedies) because these provisions concern individual access to and amendment of records containing national security, law enforcement, intelligence, counter-

intelligence and counterterrorism sensitive information that could alert the subject of an authorized law enforcement or intelligence activity about that particular activity and the interest of the DOJ and/or other law enforcement or intelligence agencies in the subject. Providing access could compromise information classified to protect national security; disclose information that would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; provide information that would allow a subject to avoid detection or apprehension; or constitute a potential danger to the health or safety of law enforcement personnel, confidential sources, witnesses, or other individuals. Nevertheless, DOJ has published notice concerning notification, access, and contest procedures because it may in certain circumstances determine it appropriate to provide subjects access to all or a portion of the records about them in a system of records, particularly if information pertaining to the individual has been declassified.

(4) From subsection (e)(1) (maintain only relevant and necessary records) because the Data Protection Review Court (DPRC), in the course of receiving information pursuant to an application for review, including the Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer's (CLPO) record of review, may receive records that are ultimately deemed irrelevant or unnecessary for the adjudication of the matter. Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity can be established. Even if the records received are ultimately determined to be irrelevant or unnecessary to the adjudication of an application for review, the Office of Privacy and Civil Liberties (OPCL) generally must nevertheless retain such records to maintain an accurate and complete record of the information reviewed by the DPRC.

(5) From subsection (e)(2) (collection directly from the individual) and (3)

## § 16.200

## 28 CFR Ch. I (7-1-24 Edition)

(provide Privacy Act Statement to subjects furnishing information). The DPRC will rely on records received from the ODNI CLPO, including records that the ODNI CLPO received from other elements of the Intelligence Community. The collection efforts of agencies that supply information ultimately received by the DPRC would be thwarted if the agencies were required to collect information with the subject's knowledge. Application of these provisions would put the subject of United States signals intelligence activities on notice of the signals intelligence activities and allow the subject an opportunity to engage in conduct intended to impede the investigative activity or avoid apprehension.

(6) From subsection (e)(4)(I) (identifying sources of records in the system of records), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the *FEDERAL REGISTER*. Should the subsection be so interpreted, exemption from this provision is necessary to protect disclosure of properly classified national security and law enforcement sensitive information. Further, greater specificity of sources of properly classified records could compromise national security.

(7) From subsection (e)(5) (maintain timely, accurate, complete and up-to-date records) because many of the records in the system were derived from other domestic and foreign agency record systems over which DOJ exercises no control. It is often impossible to determine in advance if intelligence records contained in this system are accurate, relevant, timely and complete, but in the interest of maintaining a complete record of the information reviewed by the DPRC in each case, it is necessary to retain this information. The restrictions imposed by subsection (e)(5) would impede development of the record for review and limit the DPRC's ability to exercise independent judgment in the adjudication of applications for review.

(8) Continue in effect and assert all exemptions claimed under 5 U.S.C. 552a(j) or (k) by an originating agency from which DOJ obtains records where the purposes underlying the original

exemption remain valid and necessary to protect the contents of the record.

[88 FR 60585, Sept. 5, 2023]

### Subpart F—Public Observation of Parole Commission Meetings

SOURCE: 42 FR 14713, Mar. 16, 1977, unless otherwise noted.

#### § 16.200 Definitions.

As used in this part:

(a) The term *Commission* means the U.S. Parole Commission and any subdivision thereof authorized to act on its behalf.

(b) The term *meeting* refers to the deliberations of at least the number of Commissioners required to take action on behalf of the Commission where such deliberations determine or result in the joint conduct or disposition of official Commission business.

(c) Specifically included in the term *meeting* are:

(1) Meetings of the Commission required to be held by 18 U.S.C. 4203(a);

(2) Special meetings of the Commission called pursuant to 18 U.S.C. 4204(a)(1);

(3) Meetings of the National Commissioners in original jurisdiction cases pursuant to 28 CFR 2.17(a);

(4) Meetings of the entire Commission to determine original jurisdiction appeal cases pursuant to 28 CFR 2.27; and

(5) Meetings of the National Appeals Board pursuant to 28 CFR 2.26.

(6) Meetings of the Commission to conduct a hearing on the record in conjunction with applications for certificates of exemption under section 504(a) of the Labor-Management Reporting and Disclosure Act of 1959, and section 411 of the Employee Retirement Income Security Act of 1974 (28 CFR 4.1-17 and 28 CFR 4a.1-17).<sup>1</sup>

(d) Specifically excluded from the term *meeting* are:

(1) Determination made through independent voting of the Commissioners without the joint deliberation

<sup>1</sup> Part 4a was removed at 44 FR 6890, Feb. 2, 1979.

**Department of Justice****§ 16.203**

of the number of Commissioners required to take such action, pursuant to § 16.201;

(2) Original jurisdiction cases determined by sequential vote pursuant to 28 CFR 2.17;

(3) Cases determined by sequential vote pursuant to 28 CFR 2.24 and 2.25;

(4) National Appeals Board cases determined by sequential vote pursuant to 28 CFR 2.26;

(5) Meetings of special committees of Commissioners not constituting a quorum of the Commission, which may be established by the Chairman to report and make recommendations to the Commission or the Chairman on any matter.

(6) Determinations required or permitted by these regulations to open or close a meeting, or to withhold or disclose documents or information pertaining to a meeting.

(e) All other terms used in this part shall be deemed to have the same meaning as identical terms used in chapter I, part 2 of this title.

[42 FR 14713, Mar. 16, 1977, as amended at 43 FR 4978, Feb. 7, 1978]

**§ 16.201 Voting by the Commissioners without joint deliberation.**

(a) Whenever the Commission's Chairman so directs, any matter which (1) does not appear to require joint deliberation among the members of the Commission, or (2) by reason of its urgency, cannot be scheduled for consideration at a Commission meeting, may be disposed of by presentation of the matter separately to each of the members of the Commission. After consideration of the matter each Commission member shall report his vote to the Chairman.

(b) Whenever any member of the Commission so requests, any matter presented to the Commissioners for disposition pursuant to paragraph (a) of this section shall be withdrawn and scheduled instead for consideration at a Commission meeting.

(c) The provisions of § 16.206(a) of these rules shall apply in the case of any Commission determination made pursuant to this section.

**§ 16.202 Open meetings.**

(a) Every portion of every meeting of the Commission shall be open to public observation unless closed to the public pursuant to the provisions of § 16.203 (Formal Procedure) or § 16.205 (Informal Procedure).

(b) The attendance of any member of the public is conditioned upon the orderly demeanor of such person during the conduct of Commission business. The public shall be permitted to observe and to take notes, but unless prior permission is granted by the Commission, shall not be permitted to record or photograph by means of any mechanical or electronic device any portion of meetings which are open to the public.

(c) The Commission shall be responsible for arranging a suitable site for each open Commission meeting so that ample seating, visibility, and acoustics are provided to the public and ample security measures are employed for the protection of Commissioners and Staff. The Commission shall be responsible for recording or developing the minutes of Commission meetings.

(d) Public notice of open meetings shall be given as prescribed in § 16.204(a), and a record of votes kept pursuant to § 16.206(a).

**§ 16.203 Closed meetings—Formal procedure.**

(a) The Commission, by majority vote, may close to public observation any meeting or portion thereof, and withhold from the public announcement concerning such meeting any information, if public observation or the furnishing of such information is likely to:

(1) Disclose matters:

(i) Specifically authorized under criteria established by an executive order to be kept secret in the interests of national defense or foreign policy and

(ii) In fact properly classified pursuant to such executive order;

(2) Relate solely to the internal personnel rules and practices of the Commission or any agency of the Government of the United States;

(3) Disclose matters specifically exempted from disclosure by statute (other than 5 U.S.C. 552, or the Federal Rules of Criminal Procedure): *Provided*,

## § 16.203

That such statute or rule (i) requires that the matters be withheld in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld, including exempted material under the Privacy Act of 1974 or the Commission's Alternate Means of Access under the Privacy Act of 1974, as set forth at 28 CFR 16.85;

(4) Disclose a trade secret or commercial or financial information obtained from any person, corporation, business, labor or pension organization, which is privileged or obtained upon a promise of confidentiality, including information concerning the financial condition or funding of labor or pension organizations, or the financial condition of any individual, in conjunction with applications for exemption under 29 U.S.C. 504 and 1111, and information concerning income, assets and liabilities of inmates, and persons on supervision;

(5) Involve accusing any person of a crime or formally censuring any person;

(6) Disclose information of a personal nature, where disclosure would constitute a clearly unwarranted invasion of personal privacy;

(7) Disclose an investigatory record compiled for law enforcement purposes, or information derived from such a record, which describes the criminal history or associations of any person under the Commission's jurisdiction or which describes the involvement of any person in the commission of a crime, but only to the extent that the production of such records or information would:

(i) Interfere with enforcement proceedings;

(ii) Deprive a person of a right to a fair trial or an impartial adjudication;

(iii) Constitute an unwarranted invasion of personal privacy;

(iv) Disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source;

## 28 CFR Ch. I (7-1-24 Edition)

(v) Disclose investigative techniques and procedures, or

(vi) Endanger the life or physical safety of law enforcement personnel;

(8) Disclose information, the premature disclosure of which would be likely to significantly frustrate implementation of proposed Commission action except where

(i) The Commission has already publicly disclosed the content or nature of its proposed action or

(ii) The Commission is required by law to make such disclosure on its own initiative prior to taking final Commission action on such proposal;

(9) Specifically concern the Commission's issuance of subpoena or participation in a civil action or proceeding; or

(10) Specifically concern the initiation, conduct, or disposition of a particular case of formal adjudication pursuant to the procedures in 5 U.S.C. 554, or of any case involving a determination on the record after opportunity for a hearing. Included under the above terms are:

(i) Record review hearings following opportunity for an in-person hearing pursuant to the procedures of 28 CFR 4.1 through 4.17 and 28 CFR 4a.1 through 4a.17<sup>1</sup> (governing applications for certificates of exemption under the Labor-Management Reporting and Disclosure Act of 1959 and the Employee Retirement Income Security Act of 1974), and

(ii) The initiation, conduct, or disposition by the Commission of any matter pursuant to the procedures of 28 CFR 2.1 through 2.58 (parole, release, supervision, and recommitment of prisoners, youth offenders, and juvenile delinquents).

(b) *Public interest provision.* Notwithstanding the exemptions at paragraphs (a)(1) through (a)(10) of this section, the Commission may conduct a meeting or portion of a meeting in public when the Commission determines, in its discretion, that the public interest in an open meeting clearly outweighs the need for confidentiality.

(c) *Nonpublic matter in announcements.* The Commission may delete from any

<sup>1</sup> Part 4a was removed at 44 FR 6890, Feb. 2, 1979.

announcement or notice required in these regulations information the disclosure of which would be likely to have any of the consequences described in paragraphs (a)(1) through (a)(10) of this section, including the name of any individual considered by the Commission in any case of formal or informal adjudication.

(d) *Voting and certification.* (1) A separate recorded vote of the Commission shall be taken with respect to each meeting or portion thereof which is proposed to be closed, and with respect to any information which is proposed to be withheld pursuant to this section. Voting by proxy shall not be permitted. In the alternative, the Commission may, by a single majority vote, close to public observation a series of meetings, or portion(s) thereof or withhold information concerning such series of meetings, provided that:

(i) Each meeting in such series involves the same particular matters, and

(ii) Each meeting is scheduled to be held no more than thirty days after the initial meeting in the series.

(2) Upon the request of any Commissioner, the Commission shall make a determination as to closure pursuant to this subsection if any person whose interests may be directly affected by a portion of a meeting requests the Commission to close such portion or portions to the public observation for any of the grounds specified in paragraph (a) (5), (6) or (7) of this section.

(3) The determination to close any meeting to public observation pursuant to this section shall be made at least one week prior to the meeting or the first of a series of meetings as the case may be. If a majority of the Commissioners determines by recorded vote that agency business requires the meeting to take place at any earlier date, the closure determination and announcement thereof shall be made at the earliest practicable time. Within one day of any vote taken on whether to close a meeting under this section, the Commission shall make available to the public a written record reflecting the vote of each Commissioner on the question, including a full written explanation of its action in closing the meeting, portion(s) thereof, or series of

meetings, together with a list of all persons expected to attend the meeting(s) or portion(s) thereof and their affiliation, subject to the provisions of paragraph (c) of this section.

(4) For every meeting or series of meetings closed pursuant to this section, the General Counsel of the Parole Commission shall publicly certify that, in Counsel's opinion, the meeting may be closed to the public and shall state each relevant exemptive provision.

#### § 16.204 Public notice.

(a) *Requirements.* Every open meeting and meeting closed pursuant to § 16.203 shall be preceded by a public announcement posted before the main entrance to the Chairman's Office at the Commission's headquarters, 5550 Friendship Boulevard, Chevy Chase, Maryland 20815-7286, and, in the case of a meeting held elsewhere, in a prominent place at the location in which the meeting will be held. Such announcement shall be transmitted to the FEDERAL REGISTER for publication and, in addition, may be issued through the Department of Justice, Office of Public Affairs, as a press release, or by such other means as the Commission shall deem reasonable and appropriate. The announcement shall furnish:

(1) A brief description of the subject matter to be discussed;

(2) The date, place, and approximate time of the meeting;

(3) Whether the meeting will be open or closed to public observation; and

(4) The name and telephone number of the official designated to respond to requests for information concerning the meeting. See § 16.205(d) for the notice requirement applicable to meetings closed pursuant to that section.

(b) *Time of notice.* The announcement required by this section shall be released to the public at least one week prior to the meeting announced therein except where a majority of the members of the Commission determines by a recorded vote that Commission business requires earlier consideration. In the event of such a determination, the announcement shall be made at the earliest practicable time.

(c) *Amendments to notice.* The time or place of a meeting may be changed following the announcement only if the

## § 16.205

Commission publicly announces such change at the earliest practicable time. The subject matter of a meeting, or determination of the Commission to open or close a meeting, or portion of a meeting, to the public may be changed following the announcement only if:

(1) A majority of the entire membership of the Commission determines by a recorded vote that Commission business so requires and that no earlier announcement of the change was possible, and

(2) The Commission publicly announces such change and the vote of each member upon such change at the earliest practicable time: *Provided*, That individual items which have been announced for Commission consideration at a closed meeting may be deleted without notice.

[42 FR 14713, Mar. 16, 1977, as amended by Order No. 960-81, 46 FR 52357, Oct. 27, 1981]

## § 16.205 Closed meetings—Informal procedures.

(a) *Finding.* Based upon a review of the meetings of the U.S. Parole Commission since the effective date of the Parole Commission and Reorganization Act (May 14, 1976), the regulations issued pursuant thereto (28 CFR part 2) the experience of the U.S. Board of Parole, and the regulations pertaining to the Commission's authority under 29 U.S.C. 504 and 29 U.S.C. 1111 (28 CFR parts 4 and 4a), the Commission finds that the majority of its meetings may properly be closed to the public pursuant to 5 U.S.C. 552 (d)(4) and (c)(10). The major part of normal Commission business lies in the adjudication of individual parole cases, all of which proceedings commence with an initial parole or revocation hearing and are determined on the record thereof.

Original jurisdiction cases are decided at bi-monthly meetings of the National Commissioners (28 CFR 2.17) and by the entire Commission in conjunction with each business meeting of the Commission (held at least quarterly) (28 CFR 2.27).

The National Appeals Board normally decides cases by sequential vote on a daily basis, but may meet from time to time for joint deliberations. In the period from October, 1975 through Sep-

## 28 CFR Ch. I (7-1-24 Edition)

tember, 1976, the National Appeals Board made 2,072 Appellate decisions.

Finally, over the last two years the Commission determined eleven cases under the Labor and Pension Acts, which are proceedings pursuant to 5 U.S.C. 554. The only meetings of the Commission not of an adjudicative nature involving the most sensitive inquiry into the personal background and behavior of the individual concerned, or involving sensitive financial information concerning the parties before the Commission, are the normal business meetings of the Commission, which are held at least quarterly.

(b) *Meetings to which applicable.* The following types of meetings may be closed in the event that a majority of the Commissioners present at the meeting, and authorized to act on behalf of the Commission, votes by recorded vote at the beginning of each meeting or portion thereof, to close the meeting or portions thereof:

(1) Original jurisdiction initial and appellate case deliberations conducted pursuant to 28 CFR 2.17 and 2.27;

(2) National Appeals Board deliberations pursuant to 28 CFR 2.26;

(3) Meetings of the Commission to conduct a hearing on the record regarding applications for certificates of exemption pursuant to the Labor-Management Reporting and Disclosure Act of 1959, 29 U.S.C. 504, and the Employee Retirement Income Security Act of 1974, 29 U.S.C. 1111 (28 CFR 4.1-17 and 29 CFR 4a.1-17).<sup>1</sup>

(c) *Written record of action to close meeting.* In the case of a meeting or portion of a meeting closed pursuant to this section, the Commission shall make available to the public as soon as practicable:

(1) A written record reflecting the vote of each member of the Commission to close the meeting; and

(2) A certification by the Commission's General Counsel to the effect that in Counsel's opinion, the meeting may be closed to the public, which certification shall state each relevant exemptive provision.

(d) *Public notice.* In the case of meetings closed pursuant to this section the

<sup>1</sup> Part 4a was removed at 44 FR 6890, Feb. 2, 1979.

**Department of Justice****§ 16.207**

Commission shall make a public announcement of the subject matter to be considered, and the date, place, and time of the meeting. The announcement described herein shall be released to the public at the earliest practicable time.

**§ 16.206 Transcripts, minutes, and miscellaneous documents concerning Commission meetings.**

(a) In the case of any Commission meeting, whether open or closed, the Commission shall maintain and make available for public inspection a record of the final vote of each member on rules, statements of policy, and interpretations adopted by it: 18 U.S.C. 4203(d).

(b) The Commission shall maintain a complete transcript or electronic recording adequate to record fully the proceedings of each meeting, or portion of a meeting, closed to the public pursuant to §16.203. In the case of a meeting, or portion of a meeting, closed to the public pursuant to §16.205 of these regulations, the Commission may maintain either the transcript or recording described above, or a set of minutes unless a recording is required by title 18 U.S.C. 4208(f). The minutes required by this section shall fully and clearly describe all matters discussed and shall provide a full and accurate summary of any actions taken, and the reasons therefor, including a description of each of the views expressed on any item and the record of any rollcall vote (reflecting the vote of each Commissioner on the question). All documents considered in connection with any action shall be identified in such minutes.

(c) The Commission shall retain a copy of every certification executed by the General Counsel's Office pursuant to these regulations, together with a statement from the presiding officer of the meeting, or portion of a meeting to which the certification applies, setting forth the time and place of the meeting, and the persons present.

(d) Nothing herein shall affect any other provision in Commission procedures or regulations requiring the preparation and maintenance of a record of all official actions of the Commission.

**§ 16.207 Public access to nonexempt transcripts and minutes of closed Commission meetings—Documents used at meetings—Record retention.**

(a) *Public access to records.* Within a reasonable time after any closed meeting, the Commission shall make available to the public, in the Commission's Public Reading Room located at 5550 Friendship Boulevard, Chevy Chase, Maryland 20815-7286, the transcript, electronic recording, or minutes of the discussion of any item on the agenda, or of any item of the testimony of any witness received at such meeting, maintained hereunder, except for such item or items of such discussion or testimony which contain information exempt under any provision of the Government in the Sunshine Act (Pub. L. 94-409), or of any amendment thereto. Copies of nonexempt transcripts, or minutes, or a transcription of such recording disclosing the identity of each speaker, shall be furnished to any person at the actual cost of duplication or transcription.

(b) Access to documents identified or discussed in any Commission meeting, open or closed, shall be governed by Department of Justice regulations at this part 16, subparts C and D. The Commission reserves the right to invoke statutory exemptions to disclosure of such documents under 5 U.S.C. 552 and 552a, and applicable regulations. The exemptions provided in 5 U.S.C. 552b(c) shall apply to any request made pursuant to 5 U.S.C. 552 or 552a to copy and inspect any transcripts, recordings or minutes prepared or maintained pursuant hereto.

(c) *Retention of records.* The Commission shall maintain a complete verbatim copy of the transcript, or a complete copy of the minutes, or a complete electronic recording of each meeting, or portion of a meeting, closed to the public, for a period of at least two years after such meeting, or until one year after the conclusion of any Commission proceeding with respect to which the meeting or portion thereof was held, whichever occurs later.

[42 FR 14713, Mar. 16, 1977, as amended by Order No. 960-81, 46 FR 52357, Oct. 27, 1981]

## § 16.208

### § 16.208 Annual report.

The Commission shall report annually to Congress regarding its compliance with Sunshine Act requirements, including a tabulation of the total number of meetings open to the public, the total number of meetings closed to the public, the reasons for closing such meetings, and a description of any litigation brought against the Commission under this section, including any costs assessed against the Commission in such litigation and whether or not paid.

### Subpart G—Access to Documents by Former Employees of the Department

SOURCE: Order No. 2333-2000, 65 FR 68892, Nov. 15, 2000, unless otherwise noted.

#### § 16.300 Access to documents for the purpose of responding to an official inquiry.

(a) To the extent permitted by law, former employees of the Department shall be given access to documents that they originated, reviewed, or signed while employees of the Department, for the purpose of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority. Documents include memoranda, drafts, reports, notes, written communications, and documents stored electronically that are in the possession of the Department. Access ordinarily will be provided on government premises.

(b) Requests for access to documents under this section must be submitted in writing to the head of the component where the employee worked when originating, reviewing, or signing the documents. If the employee requesting access was the Attorney General, Deputy Attorney General, or Associate Attorney General, the request may be granted by the Assistant Attorney General for Administration. This authority may not be delegated below the level of principal deputy component head.

(c) The written request should describe with specificity the documents to which access is sought (including time periods wherever possible), the

## 28 CFR Ch. I (7-1-24 Edition)

reason for which access is sought (including the timing of the official inquiry involved), and any intended disclosure of any of the information contained in the documents.

(d) The requester must agree in writing to safeguard the information from unauthorized disclosure and not to further disclose the information, by any means of communication, or to make copies, without the permission of the Department. Determinations regarding any further disclosure of information or removal of copies shall be made in accordance with applicable standards and procedures.

#### § 16.301 Limitations.

(a) The Department may deny or limit access under this subpart where providing the requested access would be unduly burdensome.

(b) Access under this subpart to classified information is governed by Executive Order 12958 and 28 CFR 17.46. Requests for access to classified information must be submitted to (or will be referred to) the Department Security Officer and may be granted by the Department Security Officer in consultation with the appropriate component head.

(c) Nothing in this subpart shall be construed to supplant the operation of other applicable prohibitions against disclosure.

(d) This subpart is not intended to, does not, and may not be relied upon to, create any right or benefit, substantive or procedural, enforceable at law by a party against the United States.

#### APPENDIX I TO PART 16—COMPONENTS OF THE DEPARTMENT OF JUSTICE

Please consult Attachment B of the Department of Justice FOIA Reference Guide for the contact information and a detailed description of the types of records maintained by each Department component. The FOIA Reference Guide is available at <https://www.justice.gov/oip/department-justice-freedom-information-act-reference-guide> or upon request to the Office of Information Policy (OIP).

The Department component offices, and any component-specific requirements, for making a FOIA or Privacy Act request are listed in this appendix. The Certification of Identity form, available at <https://>

## Department of Justice

Pt. 17

<p><i>www.justice.gov/oip/doj-reference-guide-attachment-d-copies-forms</i>, may be used by individuals who are making requests for records pertaining to themselves. For each of the six components marked with an asterisk, FOIA and Privacy Act requests for access must be sent to OIP, which handles initial requests for those six components.</p>	
<p>Antitrust Division, FOIA/PA Unit</p>	Office of Community Oriented Policing Services, FOIA Officer, Legal Division
<p>Bureau of Alcohol, Tobacco, Firearms, and Explosives, Disclosure Division</p>	Office of the Deputy Attorney General*
<p>Civil Division, FOIA/PA Officer</p>	Office of Information Policy
<p>Requests for records from case files must include a case caption or name, civil court case number, and judicial district.</p>	Office of the Inspector General, Office of the General Counsel
<p>Civil Rights Division, FOIA/PA Branch</p>	Office of Justice Programs, Office of the General Counsel
<p>Community Relations Service, FOIA/PA Coordinator</p>	Office of Legal Counsel
<p>Criminal Division, FOIA/PA Unit</p>	Office of Legal Policy*
<p>Drug Enforcement Administration, Freedom of Information Operations Unit, FOI/Records Management Section</p>	Office of Legislative Affairs*
<p>Environment and Natural Resources Division, FOIA Coordinator, Law and Policy Section</p>	Office of the Pardon Attorney, FOIA Officer
<p>Requests for records from case files must include a case caption or name, civil or criminal court case number, and judicial district.</p>	Office of Professional Responsibility, Special Counsel for Freedom of Information and Privacy Acts
<p>Executive Office for Immigration Review, Office of the General Counsel</p>	Office of Public Affairs*
<p>When seeking access to records concerning a named alien individual, requesters must include an alien registration number ("A" number). If the "A" number is not known or the case occurred before 1988, the date of an Order to Show Cause, country of origin, and location of the immigration hearing must be provided.</p>	Office of the Solicitor General
<p>Executive Office for United States Attorneys, FOIA/Privacy Unit</p>	Requests for records from case files must include a case name, docket number, or citation to case.
<p>Executive Office for Organized Crime Drug Enforcement Task Forces</p>	Office on Violence Against Women
<p>Requests for records from case files must include the judicial district in which the investigation/prosecution or other litigation occurred.</p>	Professional Responsibility Advisory Office, Information Management Specialist
<p>Executive Office for United States Trustees, FOIA/PA Counsel, Office of the General Counsel</p>	Tax Division, Division Counsel for FOIA and PA Matters
<p>Requests for records from bankruptcy case files must include a case caption or name, case number, and judicial district.</p>	Requests for records from case files must include a case caption or name, civil or criminal court case number, and judicial district.
<p>Federal Bureau of Investigation, Record/Information Dissemination Section, Records Management Division</p>	United States Marshals Service, Office of the General Counsel
<p>Federal Bureau of Prisons, FOIA/PA Section</p>	Requests for records concerning seized property must specify the judicial district of the seizure, civil court case number, asset identification number, and an accurate description of the property.
<p>Foreign Claims Settlement Commission</p>	United States Parole Commission, FOIA/PA Specialist
<p>INTERPOL-U.S. National Central Bureau, FOIA/PA Specialist, Office of General Counsel</p>	[AG Order No. 3517-2015, 80 FR 18113, Apr. 3, 2015, as amended by AG Order No. 5851-2024, 89 FR 1450, Jan. 10, 2024]
<p>Justice Management Division, FOIA Contact</p>	<b>PART 17—CLASSIFIED NATIONAL SECURITY INFORMATION AND ACCESS TO CLASSIFIED INFORMATION</b>
<p>National Security Division, FOIA Initiatives Coordinator</p>	Sec.
<p>Office of the Associate Attorney General*</p>	17.1 Purpose.
<p>Office of the Attorney General*</p>	17.2 Scope.
	17.3 Definitions.
	<b>Subpart A—Administration</b>
	17.11 Authority of the Assistant Attorney General for Administration.
	17.12 Component head responsibilities.
	17.13 National Security Division; interpretation of Executive Orders.
	17.14 Department Review Committee.
	17.15 Access Review Committee.
	17.16 Violations of classified information requirements.
	17.17 Judicial proceedings.
	17.18 Prepublication review.