

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of MILLIONS of pages
released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>



U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

September 14, 2018

MR. JOHN GREENEWALD JR.

[REDACTED]
[REDACTED]

FOIPA Request No.: 1353425-001
Subject: FOIA Request Manual ("The Green Book")

Dear Mr. Greenewald:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act (FOIA). Below you will find informational paragraphs relevant to your request. Please read each item carefully.

- A search of the Central Records System maintained at FBI Headquarters indicated that records responsive to your request have been sent to the National Archives and Records Administration (NARA). Since these records were previously processed under the provisions of the Freedom of Information Act, we are providing you a copy of the previously processed documents.

Please be advised if this release of previously processed material does not satisfy your information needs for this request, you may make a request to NARA at the following address, using file number insert FILE NUMBER as a reference:

National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740-6001

- A search of the Central Records System maintained at FBI Headquarters indicated that records responsive to your request were destroyed on DATE IF KNOWN. Record retention and disposal is carried out under supervision of the National Archives and Records Administration (NARA), Title 44, United States Code, Section 3301 as implemented by Title 36, Code of Federal Regulations, Part 1228; Title 44, United States Code, Section 3310 as implemented by Title 36, Code of Federal Regulations, Part 1229.10. Since these records were previously processed under the provisions of the Freedom of Information Act, we are providing you a copy of the previously processed documents.

Enclosed are 195 pages of previously processed documents and a copy of the Explanation of Exemptions. This release is being provided to you at no charge.

Documents or information referred to other Government agencies were not included in this release.

Please be advised that additional records potentially responsive to your subject may exist. If this release of previously processed material does not satisfy your information needs for this request, you may request an additional search for records. Submit your request by mail or fax to – Work Process Unit, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997. Please cite the FOIPA Request Number in your correspondence.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010)). This

response is limited to those records subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIA online portal by creating an account on the following web site: <https://www.foiaonline.gov/foiaonline/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Sincerely,



David M. Hardy
Section Chief,
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353425-1

Total Deleted Page(s) = 7
Page 16 ~ Referral/Consult;
Page 17 ~ Referral/Consult;
Page 18 ~ Referral/Consult;
Page 19 ~ Referral/Consult;
Page 20 ~ Referral/Consult;
Page 152 ~ Referral/Consult;
Page 153 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7c

FOIPA Manual Numbered Memo Index
(Numerical) (Alphabetical)

Memo Title

- 1 Abstracts
- 2 Accelerated Processing
- 3 Appeals, Administrative
- 4 Applicants
- 5 Autopsy Reports and Photographs
- 6 Bureau Teletypes, Telegrams and Radiograms Originating Prior to 1955
- 7 Caution Statements
- 8 Central Intelligence Agency
- 9 Classification Stamps, Use of
- 10 Classified Material, Handling of and Transmittal of
- 11 Closing a FOIPA Request
- 12 Congressional Documents
- 13 Coordination of FOIPA Releases
- 14 Correction/Expungement of FBI Records
- 15 Correspondence
- 16 Court Orders
- 17 Cross-References
- 18 Defunct Agencies or Departments
- 19 Department of Health and Human Services
- 20 Department of Justice, Civil Rights Division
- 21 Department of Justice, Criminal Division
- 22 Document Classification Unit
- 23 Drug Enforcement Administration
- 24 Duplicate Documents, Processing of
- 25 Duplication
- 26 Electronic Surveillance Records
- 27 Executive Secretariat Control Data Sheet
- 28 Exclusions
- 29 Exemption (b) (3)
- 30 Exemption (b) (7) (A)
- 31 Exemption (b) (7) (D)
- 32 Exemption (b) (7) (E)
- 33 Exemption (j) (1)
- 34 Field Offices
- 35 File Classification "73"
- 36 File Classification "77"
- 37 File Classification "92"
- 38 File Classification "161"
- 39 File Classification "197"
- 40 Filing of FOIPA Material

~~SECRET~~

(S) 41 Foreign Intelligence Surveillance Court
42 FD-376 Dissemination Letter to Secret Service
43 FD-430 Bank Robbery Summary Report
44 FD-515 Accomplishment Report
45 FD-761 Public Corruption Data Transmittal Form
46 Fugitive Requesters
47 Liaison with
48 High Visibility Communications
49 Historical Processing
50 Hoover Official and Confidential Files
51 House Select Committee on Assassinations
52 Identification Records
53 Immigration and Naturalization Service
54 Informant File Requests
55 Infrastructure Vulnerability/Key Asset Protection Program
56 Institutional Sources
57 Interesting Case Memoranda Located in Bureau Files
58 Internal Revenue Service
59 Interview Notes, Special Agent
60 Investigations
61 Iran-Contra/Front Door Material
62 Laboratory Notes
63 Legal Attaches
64 Mail Covers
65 Manuals, FBI
66 National Center for the Analysis of Violent Crime
67 National Crime Information Center
68 National Security Agency
69 Personnel Files
70 Photograph Albums, FBI
71 Polygraph Examinations
72 Previously Processed Material
73 Psychological Services to FBI Employees
74 Reading Room, FOIPA
75 Referrals-General Policy (Federal Government Only)
76 Selective Service System
77 Special Agent/Support Applicant Interview Form/Testing
Material
78 Special Agent/Support Employee Names and Initials
79 Special File Room
80 Subpoena Duces Tecum
81 Substantial Equivalents of Main Files
82 Telephone Application
83 Third Party Requests/Information
84 Undercover Operations

b1
b3

- 85 Visual Investigation Analysis Chart
- 86 White House Referrals/Consultations
- 87 Witnesses, Protection of
- 88 World War II Censorship Documents
- 89 Counter-Intelligence Program (COINTELPRO)
- 90 Department of the Army
- 91 Equal Employment Opportunity (EEO) Matters (File Classification "280")
- 92 Extradition

FOIPA Numbered Memo 1

Page 2

Abstracts

The **personnel and applicant matter abstracts** are maintained at an off-site location and are not available for use.

In 1979, the Automated Incoming Mail Serialization (AIMS) System became operational. This system provides computerized positive accountability for each serial placed on record in FBI files. Information maintained in AIMS includes the date, subject, type of communication, status of the case, file classification, source and destination of every document. AIMS provides virtually all of the data describing a document which is contained on abstracts with the exception of the narrative portion. **Therefore, mail generated after 1979 and entered into the AIMS system is accessible through the Automated Case Support (ACS) System.**

Purpose and Procedures for Abstract Checks

The purpose of an Abstract check is to ascertain the specific file and serial number(s) of documents located within Bureau files. This is an extremely useful means of locating FBI documents that have been referred from other government agencies to the FBI for processing under the FOIPA.

For Abstract checks to be conducted at Pickett Street on mail dated 1959-1979, Form 4-860 (currently referred to as OPCA-13), **Attachment 2**, to this memorandum must be completed and contain the following information:

- (1) The origin of the document
- (2) The date of the document
- (3) The subject matter
- (4) Indicate whether the mail is incoming to FBIHQ or outgoing and the type of mail (e.g., Airtel, teletype, Special Agent report, etc.)

For Abstract checks on mail prior to 1959, the same Form 4-860 (OPCA-13) should be completed and searched in the Micrographics Unit, Room 1B301, extension 3815 by the LT/PLS. Currently, this unit is in the process of destroying the older abstracts.

Mail generated after 1979 can be reviewed on the computer through the ACS System. If the LT/PLS does not have access to a computer to search the ACS System, he/she may submit Form 4-860 (OPCA-13) to the Service Unit located in the Special File Room, Room and they will conduct the search and advise the LT/PLS of the file number(s) on the records.

FOIPA Numbered Memo 3

Page 2

Appeals, Administrative

When an appeal has been submitted by a requester to OIP, the Field Coordination Team (FCT) will be notified of the appeal. The FCT will then identify the LT/PLS who is handling or handled the case and will forward a copy of the appeal letter to the LT/PLS. FCT will document this information in the appeal folder, including the date the LT/PLS was notified of the appeal. It is encouraged and recommended that the appeal review be handled by the PLS within ten working days from notification of the appeal. However, an appeal should not be scheduled until all files, processed documents, and any other pertinent materials have been located. Once all of the material is available, the LT/PLS is to schedule the appeal in the appointment book maintained in FCT by providing their name, extension, appeal number, and the approximate number of pages for review. On the date that the appeal has been scheduled, a DOJ appeals attorney will contact the LT/PLS for the material to be reviewed.

If during the appeal review, a determination is made to release additional material, that release may be made by either the PLS or the DOJ Attorney. If the release is to be made by the PLS, the additional release should not be made until a copy of the DOJ=s adjudication letter has been received. Regardless of who makes the release, the PLS should ensure a copy of the final DOJ letter and the additional release is retained in the 190 file.

In addition to the above procedures, when an appeal involves classified information where (b)(1) was cited to the requester, that information must be further reviewed during the appeal stage by the Departmental Review Committee (DRC). OPCA-33 form (formerly 4-809) must be completed by the PLS and submitted to DCU along with a copy of the original DCU addendum and all pertinent files containing the classified material. Following DRC=s review, any information which is declassified must be reviewed by the PLS for possible release or application of other FOIA exemptions. If information has been declassified by DRC and is now being withheld from disclosure pursuant to an exemption other than (b)(1), the OIP attorney is to review these excisions for their appropriateness. Upon completion of the entire DRC process, the requester must be advised in writing of the outcome and provided with copies of documents that contain any changes in processing. A copy of OPCA-33 form is attached.

Information From Other Agencies

For information which originated with another agency, notice to a requester of his right to appeal should advise him that any appeal concerning another agency's information should be sent to the appeal authority of that agency. The PLS should ensure throughout the appeal process that we are dealing only with information which originated with the FBI.

Classification Appeals Involving Referrals

When conducting a classification review, DCU prepares an addendum noting the results of the review. If appropriate, instructions are given regarding the referral of FBI documents to other agencies. Disclosure PLSs are responsible for making such referrals promptly.

In those cases where a classification decision is appealed, the results of the referral must be recorded prior to presentation of the appeal to the DRC. If the referral has not been made, DRC will instruct that it be done promptly. The results of the referral and the original documents are to be sent to the DCU for presentation to the DRC. DCU will note the classification action taken by DRC on the original documents.

Coordination of Headquarters/Field Office Appeals

If it is determined that a field office appeal involves an ongoing HQ request or appeal, the FCT Regional Program Manager, the PLS and his or her Team Captain will determine if the field office appeal should be assigned to the HQ PLS to ensure consistency in processing and coordination of the request and the appeal. Otherwise, if there are no apparent conflicts or problems, the FCT will routinely handle the field office appeal.

Exemption (b)(7)(A) Appeals

If a (b)(7)(A) case has been appealed, and the case is now closed, the processing of the material should commence after consultation with the OIP attorney. The appeal should be closed on the appeals statistical sheet under the Areversed@ category.

Appeals Involving Preprocessed Cases

From time to time, a PLS may handle a request which was previously processed (Apreprocessed@) for another requester. Preprocessed cases are assigned to the Disclosure Units for prompt handling, since they do not require any processing, but rather, just duplicating the material for release. However, in several instances, the preprocessed cases were originally processed prior to the Landano/Reno guidelines. If requesters appeal any denials contained in the preprocessed material and DOJ/OIP remands the case for processing under the Landano/Reno guidelines, this action will involve reprocessing the case for any additional information to be released. It is the policy of the FOIPA Section to reopen the request and place it in the backlog based on the date of receipt of the initial request letter. These cases will then wait their turn in

the queue along with those which require initial processing.

Appeals Involving the Cross-Reference Policy

The FOIPA Section's policy for processing requests is to only process identifiable main files even though cross-references for the subject may exist. Requesters are advised of this policy, and occasionally, will appeal this procedure. If an appeal by a requester includes an appeal of the cross-reference policy, the PLS should process the cross-reference(s) at this time.

FOIPA Numbered Memo 4

Page 2

Applicants

Further, at FBIHQ, FOIPA letters from applicants denied employment will be sent to the Unit Chief of either the Special Agent Applicant Unit or the Bureau Support Applicant Unit if the requester is seeking the reason he or she was not hired. If the respective Unit cannot give the reason for denied employment (i.e., source giving derogatory information), then the letter will be returned to the FOIPA Section to be handled.

Periodically, we will receive FOIPA requests for records on FBI background investigations conducted on individuals applying or being appointed for other federal government positions (i.e., DOJ positions, DEA, Special Inquiries for White House appointments). If the requester, a non-FBI applicant, clearly indicates in the letter that he is primarily interested in determining why he was not hired for government employment, and the releasable records would not clearly indicate the reason for that decision, then a letter should be sent to the requester advising him of this and that an FOIPA release would not be very informative. The letter should explain that, although the FBI may conduct background investigations for another agency, the FBI does not make hiring decisions for that agency. The letter should suggest that the requester contact the official who made the hiring decision at the other agency and explain the situation to him or her. We cannot, of course, refuse to process an FOIPA request, so the requester must be asked if he would still like his request processed.

A final point concerns verification of the identity of the requester. If the requester's address in the request letter is identical to the address documented in the background investigative file, then it is not necessary to obtain a notarized signature or a certificate of identity from the requester.

Source Information in Applicant/Background Type Files - Confidentiality?

In some instances, applicant files compiled after September 27, 1975, the effective date of the Privacy Act, will not indicate whether a source of information requested confidentiality. Often it is felt that many of these sources would want confidentiality because of the type of information (i.e., derogatory information) being provided to the FBI. Therefore, if this situation occurs and there is a concern in the release of the information, it is suggested that the PLS contact the field office Case Agent prior to releasing the material. If the field Agent indicates the source did request confidentiality and it was overlooked in documenting it on the typed interview statement, it should be made a matter of record in the applicant/background file. In processing this material, the identity of the source and any information which would tend to identify the source should be protected. If the field Agent is unable to articulate or provide proof that confidentiality was requested the information must be released.

To: All FBI FOIPA Personnel
From: John M. Kelso, Jr.
Subject: Bureau Teletypes, Telegrams and Radiograms Originating Prior to 1955
Date: January 3, 2000

**Handling of Bureau Teletypes, Telegrams and Radiograms
Originating Prior to 1955**

Prior to September 21, 1999, the FBI classified the coding information found in FBI Teletypes, Telegrams, and Radiograms dated between 1928 and 1954. This was done in order to further protect other classified information. However, on July 12, 1999, NSA informed the FBI that it is no longer necessary to classify the coding information contained in these documents. The determination to declassify the coding information was made based upon the age of the documents and the fact that continuing to classify the FBI coding schemes in these documents will no longer serve to further protect other classified information.

Due to this decision by NSA, it is no longer necessary to have DCU review these documents, whether located in Criminal or National Security files, prior to release.

FOIPA

MANUAL

MEMO 7

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Caution Statements
Date: March 31, 1998

When processing FBI documents pursuant to the FOIPA, caution statements may appear on the document such as AARMED AND DANGEROUS.@ In most cases, these statements are typed with upper case letters and/or underlined and usually appear at the bottom portion of the document, however, they may be found elsewhere. When caution type statements appear on a document, the PLS should thoroughly research the file(s) before releasing any statement in order to determine whether or not the statement was obtained from a confidential source. If the source=s identity is not recorded and the statement appears to be singular in nature, the PLS should consider protecting the statement under exemption (b)(7)(D).

The following is an example of where the caution statement was released to the requester without excision: AARMED AND DANGEROUS, SUBJECT MAY TAKE RETALIATION AGAINST SENTENCING JUDGE.@ On appeal, a review of the HQ file failed to determine the source of the information and the field office was telephonically requested to search its file. Through the review of the field office file, it was determined the source was the subject=s mother, who had received the information from the subject=s brother, and had alerted the FBI on a very confidential basis. Had this been known prior to the release, the caution statement would not have been disclosed.

FOIPA Numbered Memo 9

Page 2

Classification Stamps, Use of

of classification indicated by the DCU addendum is **ASecret**, then the **ASecret** stamp should be placed on both the front and back and at the top and bottom of the page of the tickler and yellow copies. The **ASecret Material Enclosed** and **AThis Communication Is Unclassified Upon Removal of the Enclosures** stamps are to be placed on the bottom of the front of both copies. *Do not place the classification stamps on the copy of the disclosure letter going to the requester.* See Attachment 2.

Electronic Communications (EC)

There will be times when classification stamps will be placed on ECs. For example, if the Electronic Surveillance (Elsur) Indices search slip is classified and the LT/PLS is enclosing the search slip to the EC going to the field office(s). The **A_____ Material Attached** and **AThis Communication Is Unclassified Upon Removal of the Enclosures** stamps will need to be placed on all copies of the EC. The classification level will be indicated on the EC when it is prepared.

For information concerning the transmittal of classified material also review **Memo 10** concerning the **AHandling and Transmittal of Classified Material**.

C. Referrals of TS/SCI Information

1. When FBI information in other-agency documents is classified at the TS/SCI level, regardless of the date of the document, DCU will have the SFR remove the document from the file and stamp the file front **ATOP SECRET FILE EXISTS.** At the request of the Disclosure PLS, the SFR will copy the document. The PLS will prepare a referral to the other agency with directions to delete exempt FBI-originated information from its document. Once the referral has been finalized, the PLS will take all copies of the referral form (OPCA-6) and the enclosure(s) to the SFR where an FD-502a will be prepared. The SFR will place a note in the margin of the yellow copy to indicate that the originals of the enclosures are retained in the SFR. **Do not retain copies of the TS/SCI documents behind the yellow of the referral form.** The SFR will handle the delivery of other agency referrals with the exception of NSA. NSA referrals will be handled by the PLS who will hand deliver the material to the FBI's NSA Liaison Agent in Room 1B045. (See the "Special File Room" numbered memorandum for procedures when the SFR advises the LT/PLS that he/she does not have the appropriate clearance to review the document.)

2. When other-agency information in FBI documents is classified TS and/or contains SCI, DCU will not automatically act to have the TS/SCI information removed from the file, but will await notification from the other agency of its intent to retain the classification. Thus the FBI document will be retained in the file until after the PLS sends a referral to the other agency, and the other agency responds to the referral. The PLS will take all copies of the referral form (OPCA-6) and the enclosure(s) to the SFR where an FD-502a will be prepared by the SFR. **Do not retain copies of the TS/SCI documents behind the yellow of the referral form.**

a. If the other agency indicates that the information is to retain its classification, the PLS will hand carry the referral response along with the original FBI document to DCU. DCU will update the classification in the FBI document and hand carry the file to the SFR for filing in the SFR. The PLS will obtain a copy of the document from SFR in order to complete the processing of the FOIPA request. (See paragraph A.3.)

b. If the other-agency information is downgraded below the TS level or no longer considered SCI, DCU will handle the document as described in paragraph B above.

D. Handling Disclosure Packages with TS/SCI

When the red-outs of a disclosure package contains TS/SCI material, the TC will date stamp all copies of the disclosure form, place appropriate stamps on the original and the yellow file copy, but the TC will not package the material or send it to the Mail Services Unit (MSU). The PLS will hand carry all copies of the disclosure form (OPCA-16) and all enclosure(s),

FOIPA Numbered Memo 10

Page 3

Classified Material

including the black-outs, to the SFR, who will then prepare an FD-501a. Once this has been handled the original disclosure form and the black-outs can be packaged for mailing.

E. Transfer of TS/SCI Information

If a TS/SCI document (that is not filed in a TS folder or file maintained by the SFR) needs to be reviewed by another individual, it is the responsibility of the person who has the document to ensure that the person to whom the document is transferred has a "need to know" and, if it is SCI, the necessary SCI access. This can be accomplished by calling the Personnel Security Unit on extension 4-3605. To transfer the TS/SCI document, call the SFR on extension

Any TS/SCI document must be hand carried to another individual. When not being used, the TS/SCI document must be maintained in a combination safe when it is outside of the SFR.

b7E

F. Filing TS/SCI And Elsur Documents

It is the policy of Information Resources Division that when any part of a document or enclosure to a document is TS, the entire serial is treated as TS. Therefore, when a TS document is in a FOIPA disclosure package (processed documents), the SFR considers the entire disclosure package as TS. The FOIPA disclosure form should be stamped "ATop Secret@ on the top and bottom and "ATop Secret Material Attached" and "This Communication Is Unclassified Upon the Removal of Classified Enclosures@on the bottom by the PLS. Similar handling is given to Elsur records. The disclosure package should be hand carried to the SFR for filing in their portion of the 190 file. **Be aware that any original document or yellow/white file copy that is stamped ATop Secret@ or has ATop Secret@ material attached must be filed in the SFR.**

Transmittal of Classified Materials Within FBIHQ

All FBIHQ employees are reminded of the importance of properly handling classified information in order to prevent the loss or disclosure of that information. The following procedures should be adhered to in all cases involving the routing of classified information within FBIHQ:

Top Secret (TS) Documents or documents containing Sensitive Compartmented Information (SCI) must have an attached form FD-501a and be hand-carried in an envelope when being moved within FBIHQ. SCI documents must be hand-carried by an individual who has been cleared for SCI access. TS and SCI documents must never be placed in outgoing

FOIPA Numbered Memo 10

Page 4

Classified Material

mailboxes or routed through MSU.

Confidential and Secret documents may be placed in outgoing mailboxes and be delivered by MSU, but must be inside a messenger envelope.

Transmittal of Classified Materials Outside FBIHQ

TS and SCI documents being sent outside FBIHQ must have an attached form FD-502a and be hand-carried to the Special File Room (Room [redacted]) for recording and packaging. These documents will be delivered by a designated FBI courier or the Defense Courier Service. If the package is designated for the Washington Metropolitan area, delivery will be handled by the FBI courier. For this reason, there must be a point of contact listed on the address label. If the PLS does not know who the point of contact is for a particular agency, the PLS should contact the agency for this information. If the designated addressee is outside of the Washington Metropolitan area, delivery will be handled by the Defense Courier Service.

b7E

Confidential and Secret Documents being sent to FBI offices must be placed in a messenger envelope and then routed to MSU, Room 1B341. Confidential and Secret documents being sent to other government agencies (including DOJ) must be placed in a messenger envelope and routed to MSU, Room 1B341, for recording, receipting, and packaging. However, if the TC packages this material, the TC should place a sticky on the outside mailing envelope indicating whether there is AConfidential@ or ASecret@ material inside the package, and place in a messenger envelope or hand carry to the MSU.

Everyone has a responsibility to protect classified information. Additional information concerning the handling and marking of classified information can be found in the MIOG, Part II, Section 26, AClassified National Security Information and Material.@ Questions may be directed to [redacted] Information Systems Security Unit, National Security Division, extension 1282. Questions regarding mail room procedures may be directed to MSU, Information Resources Division, extension 4-4301, Room 1B006.

b6

FOIPA Numbered Memo 11

Page 2

Closing a FOIPA Request

referred to FBIHQ by Electronic Communication (EC) for handling. Upon referring these requests to FBIHQ, the field office will no longer maintain their 190 file in a pending status as in the past, but rather, close the 190 field office file by the date of the EC. It is ultimately the responsibility of the FBIHQ PLS processing the case to ensure all issues in the request letter and further correspondence which pertain to your subject matter have been addressed. Once the processing of the case has been completed or if interim releases are made, the field office which originally referred the request should be provided with a copy of the disclosure letter(s) for their 190 file.

Abandoned Cases - Use of Form OPCA-25 **(Transmitting Processed Documents to File)**

To close FOIPA requests when material has been prepared for release and the requester has abandoned fees, withdrawn the request, etc., OPCA-25 (previously referred to as Form 4-780) should be completed in order to document the reason for closing the case and to send the processed material to the 190 file. Attached is copy of OPCA-25 which should be utilized for this purpose.

Closing of Multiple Requests from One Requester **When Failure to Submit Fees**

Some requesters submit numerous requests (multiple requests) for information concerning various subject matters. When these requesters do not submit requested fees, no further processing of their requests should be done. Further, no releases should be made to these individuals until they pay the requested fees. **A stop should be placed with RTSS** to insure that the FBI=s FOIPA Section does not accept further requests from the requester. If payment of fees is not made within 60 days from the date of the FBI=s request for payment, all of this individual=s requests should be closed for failure to pay requested fees.

To: All FBI FOIPA Personnel
From: John M. Kelso, Jr.
Subject: Correction/Expungement of Information in FBI Files
Date: June 8, 2000

When an incoming letter requests a correction, change or destruction of information in FBI records, it should be referred on the same day to the Team Captain of the Field Coordination Team (FCT) who handles all correction and amendment requests. Every effort should be made to provide the Team Captain with the following:

- 1) all correspondence between the Bureau and the requester
- 2) the actual excised (processed) documents of the material released to the requester

PLSs are expected to cooperate in any way possible in locating the above material and resolving the request, as the Privacy Act requires a response and notification of the FBI=s intentions within ten working days after the date of receipt of the request.

Furthermore, there are times when a citizen requests only an addition to his or her file clarifying material which was submitted to the FBI. In such cases, the PLS should follow the above procedures and promptly refer the request to the FCT.

The only person who can make a request for amendment/correction is the subject of the record. However, even improper requests, such as repeated submissions of written data from an organization for inclusion in the organizational file, should be coordinated with Team Captain of the FCT.

FOIPA Numbered Memo 15

Page 2

Correspondence

If there is a previous history of either the requester or subject, RTSS will affix the appropriate computer printout(s) to the letter.

Incoming mail concerning requests which have been closed administratively will be handled by RTSS in one of two ways. If the request was closed for no notary, insufficient information, no fees guaranteed, or abandoned fees, RTSS will reopen the old request if warranted. If the request was closed administratively for any other reason, such as a no record or withdrawn, RTSS will open a new request. However, if a request was closed by a Disclosure PLS through processing and the same requester writes in about the same subject matter, if necessary, RTSS will confer with the Disclosure PLS and/or team captain for instructions on opening, reopening or assignment of the case.

When correspondence assigned to a LT in RMU is identified as a previous request on the same subject matter, they will indicate the name and team of the PLS who previously processed the request. If the processed material is maintained in the FOIPA Reading Room, RMU will handle the new request. If the previous request is still pending in Disclosure, the LT should consult with the PLS handling the prior request for a response to the new request. RMU will then direct the new request to the PLS handling the subject matter. If the previous request has been closed, RMU will consult with Disclosure to determine if fees are at issue. If there are no fees involved, RMU will designate the new request to the same PLS who previously processed the subject.

Classification of Notes and Addenda

Classification regulations require that any notes or addenda which are added to a communication/correspondence, or to certain copies of it should be treated separately. In order to comply with these regulations, the following guidelines should be followed:

1. When classifiable national security information is set forth in a note or addendum to a communication, the note or addendum should be prepared on a separate page. This allows for independent classification marking of the note or addendum.
2. Top Secret or Sensitive Compartmentalized (SCI) Information should be avoided in a note or addendum. If possible, every effort should be made to exclude all classifiable information from the note or addenda.

FOIPA

MANUAL

MEMO 16

To: All FBI FOIPA Personnel
From: John M. Kelso, Jr.
Subject: Court Orders Affecting FBI Processing of FOIPA Requests
Date: November 27, 2001

National Caucus of Labor Committees (NCLC)
United States Labor Party (USLP)
Fusion Energy Foundation (FEF)

On 8/13/00, an Order of Settlement and Dismissal was entered in Lyndon H. LaRouche, Jr. v. Clarence M. Kelley, Civil Action Number 75-CIV-6010, (S.D.N.Y. 1975). This settlement requires: (1) until January 1, 2025, all FBI documents contained in FBIHQ and Field Office files relating to the NCLC investigation or individual plaintiffs= files will be segregated and held apart and not disseminated for any purpose **except as required by law, including FOIA & PA or court order**; (2) all NCLC files when requested pursuant to FOIA **will be processed in accordance with FOIA and PA**; (3) all NCLC files processed pursuant to FOIA **will not be placed in the Public Reading Room or disseminated to non-requesters**; (4) any Department of Justice component that receives an FOIA request for NCLC files **shall refer the material to FBI for processing**; (5) in any FOIA releases of NCLC files, the FBI **shall include** on a separate page, to be the first page of every package, **the ASTATEMENT@** and (6) in the event of a future investigation of the NCLC or any plaintiff, the Department of Justice/FBI will comply with all laws, regulations and internal guidelines. This action was dismissed with prejudice. All materials in the court file which were filed under seal will remain sealed.

The FBI files are being retained by Civil Discovery Review Unit, OGC, contact b6
 See **attachment 1A** for a copy of the order. The statement to be placed in all releases is **attachment 1B** of this memo. This list of individuals and plaintiffs this settlement pertains to is **attachment 1C** of this memo.

National Lawyers Guild

On 10/13/89, an Order of Settlement and Dismissal was entered in National Lawyers Guild v. Attorney General, 77 Civ. 999 (U.S.D.C., S.D.N.Y.). The settlement requires in part that the FBI's investigative files on the National Lawyers Guild (NLG) be maintained in secure storage at FBIHQ until they are transferred to the National Archives and Records Administration

FOIPA Numbered Memo 16

Page 2

Court Orders

(NARA) in or after the year 2025. Covered are the following records:

- (1) all Headquarters, Field Office and Legat main files on the NLG and its projects (see Appendix A), including all enclosures behind the files (EBF's) and bulky exhibits;
- (2) electronic surveillance (ELSUR) logs contained in the Headquarters and Field Office main file of ROBERT SILBERSTEIN, including all EBFs;
- (3) reference cards and any similar computerized or non-computerized reference system capable of locating NLG-related information in files other than the NLG main file;
- (4) references to the NLG in the ELSUR Index and any informant file indices; and
- (5) any copies of the foregoing documents and any summaries thereof which may be included in the FBI litigation file (62-117572).

This portion of the Order, which is limited to documents created prior to 10/13/89, prohibits the FBI from using, or granting access to, these records prior to their transfer to NARA, subject to the following exceptions: (1) The records can be used by the government to defend itself in civil actions for activities prior to 10/13/89; and 2) The records can be used to respond to FOIA requests from the NLG submitted on or after 1/1/94. All other FOIA requests for these records should be denied.

Another portion of the Order covers records on an individual, created prior to 3/1/77, which reflect an affiliation with the NLG. Included are main files on the individual, cross-references to the NLG, and serials which are see-referenced to the individual and accessed through the name of the individual. (At this time these records are still being identified.) The FBI may not use, release, or disclose these records, within or outside the Government, except with the authorization of the individual mentioned in the records.

In order to clarify this Order, the following points should be noted: 1) The NLG may not receive information on one of its individual members; 2) An individual member may not receive information from an NLG file; 3) The NLG may not authorize release of information pertaining to it to a third party, and; 4) Cross-references to the NLG, as opposed to one of its members, are not protected by the Order. Only the reference cards, or equivalent finding aids, are protected.

FOIPA Numbered Memo 16

Page 3

Court Orders

Most of the records covered by this Order will be stored in the Special File Room (SFR). If you have any questions as to whether specific records are covered, please contact your Team Captain first, and then your Unit Chief, for guidance. If a determination cannot be made at that level, then the Civil Litigation Unit of the Office of General Counsel should be consulted.

Denial letters should cite the full caption of the NLG case and advise that the Order of Settlement and Dismissal dated 10/13/89 prohibits the FBI from releasing the requested records.

See Memorandum dated 8/9/90, designated as "**Attachment 2**," for a copy of the Court Order and a list of the National Projects and Committees, and individuals of the NLG protected under this Court Order. In addition, a memorandum dated 5/13/85 is attached for informational purposes on handling NLG material and a list of NLG Organizations with the known file numbers which are protected under the Court Order is also included in this attachment.

Spartacist League; Spartacus Youth League

On 11/30/84, settlement was reached in a civil action against the Department of Justice and the FBI by referenced Leagues. (FBIHQ Airtel to All SACS, 12/18/84, Captioned "SPARTACIST LEAGUE; SPARTACUS YOUTH LEAGUE; JAMES M. ROBERTSON AND SUSAN ADAMS V. ATTORNEY GENERAL OF THE UNITED STATES, et al., (U.S.D.C., S.D.N.Y.) CIVIL ACTION NO. 83-CIV-7680.)

In the settlement agreement, the FBI agreed to change its characterization of the Spartacist League. The text of the new characterization is provided below. Effective 11/30/84, all PLSs are instructed to advise the requester that a new characterization exists and should include the court-approved characterization in the disclosure letter of any future FOIPA releases containing a prior Spartacist League characterization.

"The Spartacist League (SPL), a Marxist political organization, was founded in 1966. The historical and theoretical roots of the SPL derive from the early Communist Party, U.S.A. and the Socialist Workers Party. The immediate precursor of the SPL was the Revolutionary Tendency of the Socialist Workers Party. The SPL has an official youth section named the Spartacus Youth League."

" The SPL was once the subject of an FBI domestic security investigation. The investigation was closed in 1977, however, and it did not result in any criminal prosecution."

ATTACHMENT 1B

THE FOLLOWING STATEMENT IS INCLUDED IN THIS RELEASE PURSUANT TO THE TERMS OF THE STIPULATION AND ORDER OF SETTLEMENT AND DISMISSAL IN LaRouche, et al. v. Freeh, et al., 75 Civ 6010 (S.D.N.Y.). THE STATEMENT IS THAT OF THE NATIONAL CAUCUS OF LABOR COMMITTEES, AND IS NOT IN ANY WAY ATTRIBUTABLE TO THE FEDERAL BUREAU OF INVESTIGATION OR THE DEPARTMENT OF JUSTICE:

ALydon H. LaRouche, Jr. and other members of the National Caucus of Labor Committees have reviewed some of the files which the FBI compiled as a result of the approximately 1968-1977 NCLC investigation. They believe these FBI files often contain false, distorted and highly misleading accounts of their activities and are not a reliable basis for reporting on their activities.

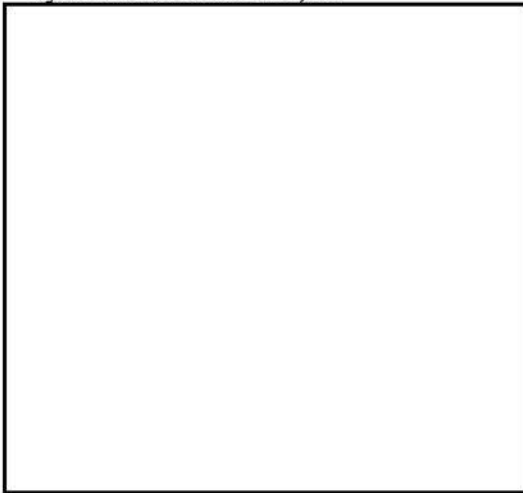
The National Caucus of Labor Committees is available for comment on these files through the Constitutional Defense Fund, 2 Cardinal Park Drive, Suite 104A, Leesburg, VA 20175."

ATTACHMENT 1C

LIST OF NCLC SUBJECTS (Plaintiffs)

Lyndon H. LaRouche, Jr.

b6



The United States Labor Party
National Caucus of Labor Committees

FOIPA Numbered Memo 18

Page 2

Defunct Agencies or Departments

DEFUNCT COMPONENTS OF DOJ

CURRENT RECORD HOLDER

Civil Liberties Unit

Civil Rights Division

Claims Division

Civil Division

Communications and Records Section

Justice Management Division

Criminal Statistical Bureau

FBI

Customs Division

Civil Division

Department of Veterans Insurance

Civil Division

Internal Security Division

Criminal Division

Office of Alien Property

Civil Division

Office of Criminal Justice

Office for Improvements in the
Administration of Justice

Office of Policy and Planning

Office for Improvements in the
Administration of Justice

Office of the Special Prosecutor

National Archives and Records
Administration

Public Lands Division

Land and Natural Resources Division

Special War Policies Unit

Criminal Division

War Contract Division

Criminal Division

War Division

Criminal Division

FOIPA

MANUAL

MEMO 20

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Department of Justice, Civil Rights Division
Date: March 31, 1998

The Department of Justice, Civil Rights Division, has requested that the FBI provide a clean copy of documents originated by their agency along with the redacted (blacked-out or highlighted) referral copy.

FOIPA Numbered Memo 22

Page 2

Document Classification Unit (DCU)

Additionally, the PLS will include a completed duplication request form in this package (with the serials sent to DCU listed thereupon) so that following their review, the DCU analyst can send the file to IPU for duplication of the necessary serials. Once copied, IPU will return the package to Disclosure.

Upon receiving the OPCA-18 package from Disclosure, the DCU analyst will request the raw file through ACS and review and mark the serials accordingly. If the DCU analyst recognizes other serials which require classification, they will mark those serials as well and add those serials to the duplication request form prior to sending the package to IPU for copying.

If the raw file cannot be retrieved in a reasonable amount of time, the DCU analyst is encouraged to review and mark the copies sent by Disclosure. In this case, the DCU analyst must retain a copy of the reviewed documents in order to mark the raw file when it is located.

When the DCU analyst sends the package to IPU for copying, he/she will send the addendum back to the Disclosure PLS in order to make him/her aware of the status.

If it is necessary to send an entire file for DCU review the Disclosure PLS will return the request to the Backlog Manager for corrective action.

Questions regarding this or any other DCU policy should be discussed with the DCU Unit Chief or Administrative Team Captain.

DCU Liaison to AG@ Street

In January, 2000 a Liaison between DCU and Disclosure Units assigned to AG@ Street was established in order to resolve minor classification issues that arise within a case after its being assigned to a Disclosure PLS at AG@ Street. Material that will be reviewed at AG@ Street must number **fewer than 25 pages**, and is limited to either material that was overlooked while undergoing initial classification in DCU, or material not normally reviewed by DCU, such as Personnel files. This page limit also includes referral documents that need to be marked or stamped in the file.

In order to utilize the Liaison program most efficiently, discuss the material with your Team Captain to ensure that it is appropriate for Liaison review. If the material is appropriate for Liaison review, enter your request for review on the sign-up log, being sure to include all requested information. The log is located on the secretary desk outside the Section Chief office on the third floor. The log is left in a space that is unsecured, so do not leave copies of the documents to be reviewed with the log. If you cannot locate the log, contact the Point of Contact Team Captain for that period.

FOIPA Numbered Memo 22

Page 3

Document Classification Unit (DCU)

Currently, the Liaisons come to AG@ Street every Wednesday between 8:30 a.m. and 12:30 p.m. Do not sign-up for review if you will be on leave or otherwise unavailable during this time. If you sign-up and then must take leave, remove your request from the log. If you miss the Liaison, you must re-enter your request for another week; unaddressed requests will not be carried over to the following week. If you did not sign up for a review, you may call the Liaison on extension 1198 to ask if they have time to handle your review that day. If they can review your material, enter your information on the log to make a record of the review.

Generally, you will not have the raw file. Therefore, after the Liaison reviews your copy, make a photocopy of the reviewed documents for the Liaison so that they can transpose their markings to the raw file when they return to Headquarters.

DCU "Regular Review" or "Walk-Up"

DCU will process all requests requiring classification review which involve **50 pages or less**, as part of its **Walk-up** program. This program was designed as an administrative practice in order to allow cases involving minimal pages requiring classification review to be handled within a few days of being submitted to DCU, rather than sitting in the backlog for an extended period of time. All other requests for DCU review of material containing **over 50 pages** will be conducted as a **"regular review."**

For those requests which involve only certain "serials" needing classification review, OPCA-18 form should contain the list of the serials being requested for review as well as placing tabs (yellow "stickies") on the actual serials in the raw file. The same procedures stated above for establishing a case as a walk-up or regular review is also applied to the submission of "serials" for DCU review.

File Classifications Requiring DCU Review

Documents in the following classifications, surfaced as a result of a FOIPA request, should be processed through DCU. This classification list is not meant to exclude reviews involving other classifications. If it appears that a question of national security protection is involved, the documents should be forwarded to DCU regardless of the classification.

- 2 Neutrality Matters
- 3 Overthrow or Destruction of the Government
- 9 Nuclear Extortion

FOIPA Numbered Memo 22

Page 4

Document Classification Unit (DCU)

14	Sedition
61	Treason; Misprision of Treason
64	Foreign Liaison
65	Espionage
97	Registration Act
98	Sabotage
100	Domestic Security/Revolutionary Activities Infrastructure Vulnerability/Key Asset
102	Voorhis Act
105	FCI - Russia
108	FCI - Foreign Travel Control
109	Foreign Political Matters
110	Foreign Economic Matters
111	Foreign Social Conditions
112	Foreign Funds
113	Foreign Military and Naval Matters
117	Atomic Energy Act
121	Labor Management Relations Act - 1947
134	Counterintelligence Assets
137	Domestic Security Informants
138	Loyalty Matters
155	National Aeronautics and Space Act of 1958
163	Foreign Police Cooperation
170	Extremist Matters
174	Bombing Matters
176	Anti-Riot Laws*
	183C Racketeer Influenced and Corrupt Organizations (RICO) - Terrorism
	185A Protection of Foreign Officials and Guests
	185B Protection of Foreign Officials and Guests - Special Events
199	International Terrorism
200 - 203	Foreign Counterintelligence Investigations
205	Foreign Corrupt Practices Act - 1977
212	Intelligence Community Support
215 - 229	Foreign Counterintelligence Investigations
230	Training Received - FCI
239	Training Received - Terrorism
243	Intelligence Identities Protection Act
246 - 248	Foreign Counterintelligence Investigations
253	Fraud and Related Activities-Ident Documents (FRAUD) - Terrorism

FOIPA Numbered Memo 22

Page 5

Document Classification Unit (DCU)

Terrorism	256A	Hostage Taking by International Terrorists; Hostage Taking -
	262	Overseas Homicide/Attempted Homicide - International Terrorism
	265	Acts of Terrorism in the United States - International Terrorists
	266	Acts of Terrorism in the United States - Domestic Terrorists
	268	Engineering Technical Matters - FCI
	270	Cooperative Witnesses-Domestic Terrorism Extraterritorial International Terrorism-Cooperating Witness
	271	Arms Control Treaty Matters
	277	Adoptive Forfeiture Matters - Counter Terrorism
	278	President's Intelligence Oversight Board
	279	Biological Weapons - Anti-Terrorism
	283	FCI
	284	Economic Counterintelligence
	285	Acts of Economic Espionage
	288	Computer Investigations - Threat Analysis
	290	Alien Terrorist Removal Court
	291	Animal Enterprise Protection Act
	292	Domestic Emergency Support Team
	293	Foreign Emergency Support Team
	294	Infrastructure Protection
	299	NIPCIP
	300	Domestic Terrorism
	302-304	FCI
	307	International Terrorism

*All 176 classifications that are 25 years or older (prior to and including 1971) have been sent to the National Archives along with the index cards.

Since minimal information from the files in the following list is classifiable, these files will be assigned directly to the FOIPA Section=s backlog for processing. However, prior to the PLS processing the file(s), he or she should peruse the file(s) first to determine if there is any information that may have been classified at the time the document originated or if there is information which appears to warrant classification. Should information of this type appear, the PLS will be responsible for sending the material to DCU for review.

- 40 Passport and Visa Matters
- 67 Personnel Matters - Reinvestigation of FBI Personnel

FOIPA Numbered Memo 22

Page 6

Document Classification Unit (DCU)

- 140 Security of Government Employees (SGE)
- 157 Civil Unrest (SEE ATTACHMENT 2)
- 259 Security Clearance Investigations Program
- 260 Industrial Security Program
- 261 Security Officer Matters
- 263 Office of Professional Responsibility (OPR) Matters

It is recognized that unique classification situations periodically arise which require special handling because of the unusual type of information or where short deadlines have been imposed. These situations should be brought to the attention of the DCU Unit Chief.

Classification of Notes and Addenda

Classification regulations require that any notes or addenda which are added to a communication/correspondence or to certain copies of it should be treated separately. In order to comply with these regulations, the following guidelines should be followed:

1. When classifiable national security information is set forth in a note or addendum to a communication, the note or addendum should be prepared on a separate page. This allows for independent classification marking of the note or addendum.
2. Top Secret or Sensitive Compartmentalized Information (SCI) should be avoided in a note or addendum. If possible, every effort should be made to exclude all classifiable information from the note or addenda.

Classification Review of Documents Previously Examined By DCU

A classification review by DCU of previously classified documents, cross-references as well as main files, is required under any of the following circumstances:

1. The requester is unwilling to accept the prior classification.
2. A classification review was conducted under a previous Executive Order prior to 10/14/95, and classified information still exists.
3. There has been no release of the previously classified documents and there is serious concern about the prior classification.

Notification to DCU of Prior Releases of Information

Generally, material which is already in the public domain cannot be classified. In some instances, however, material is being referred to DCU which already has been released in whole or part through another FOIPA release or civil litigation.

If a prior release of material from all or even a portion of a file has already been made, it would be of great assistance to DCU if this fact were noted on the referral memorandum. Such information might be known to the PLS either through a review of the search slip, preliminary review of the file, or knowledge of other previously processed requests for the same information or portions thereof. Do not engage yourself in a research effort to make this determination, but note it only if readily available to you.

Your cooperation in bringing this to the attention of DCU would be appreciated and should not only help in speeding up the classification process, but will assist in providing for a more uniform and consistent classification procedure.

Mandatory Classification Review

Included as **Attachment 3** are some examples of requests for mandatory classification reviews from the National Security Council (NSC). These requests have previously been placed with FOIPA referrals to be handled in the queue.

Requests for mandatory classification reviews are handled by DCU and/or the Historical and Executive Review Unit (HERU). These mandatory classifications require no action by the FOIPA Disclosure Units. The mandatory reviews are to be completed within one year; therefore, it is essential that they be appropriately routed to DCU or HERU for handling. Outlined below are certain items which distinguish a request for mandatory review from a referral made to the Bureau in connection with an FOIPA request.

--Mandatory review requests are usually made by a Presidential Library, Archives or NSC.

--Letters requesting mandatory review will cite Section 3.6 of Executive Order 12958, which is the provision for mandatory review.

--Letters requesting mandatory review will be delivered with a receipt requiring the signature of the recipient.

--Letters requesting mandatory review will have enclosed A Certification of Citizenship@

Document Classification Unit (DCU)

of the requester.

[Redacted box]

b7E

[Large redacted box]

Review of Special Compartmentalized Information (SCI) Material

Special security clearances are required in order to review or handle ATop Secret@ files or documents which contain SCI material. If you should be notified that you do not have the appropriate clearance to review the classified material requested, one of the following PLSs should be contacted to conduct the review. It is recommended that the individual contacted to review the classified material be from the same Unit as the PLS handling the case.

Disclosure Units:

- [Redacted] - Unit 1
- [Redacted] - Unit 2
- [Redacted] Field Coordination

- [Redacted] - Unit 3
- [Redacted] - Unit 4

b6

Litigation Unit:

[Redacted box]

Help Desk:

[Redacted box]

DCU:

All Team Captains in DCU are afforded SCI clearances. However, should there be any questions concerning classification matters on a case prior to DCU review, the LT or PLS should initially contact the DCU Administrative Team Captain.

RMU:

Currently, there are no RMU employees with the SCI clearance. If a RMU employee has been advised by the SFR that they do not have the proper clearance to review file material, they

should contact one of the above Disclosure PLSs.

Referrals of TS/SCI Information

When a DCU analyst encounters TS/SCI information that originated with another government agency, he/she will refer such information to the originating agency for a determination as to whether the TS/SCI information should be downgraded. The DCU analyst should request the other agency to respond within a reasonable amount of time regarding the classification level of the information. The DCU analyst will take all copies of the outgoing referral letter and enclosures to the Special File Room where an FD-502a will be prepared. Do not retain copies of TS/SCI documents behind the yellow file copy of the outgoing letter.

Upon receipt of the other government agency=s response letter, the DCU analyst will follow the instructions as specified, either updating and marking the TS/SCI classification, or downgrading the document.

FOIPA Numbered Memo 23

Page 2

Drug Enforcement Administration (DEA)

FBI field offices utilize DEA Form 6 (**See Attachment 3**), as a method of communication to automatically index subjects into DEA's computer system referred to as Narcotics And Drug Information System (NADDIS).

On 6-28-99, [redacted] DEA, advised that when DEA Form 6 is located in a Bureau file and the only DEA information in the document is a DEA agent's name, the agent's name should be redacted pursuant to (b)(7)(C) without contacting DEA. Also, if the DEA Form 6 contains no DEA information, no communication with DEA is required. (**Attachment 3 is an example of the DEA Form 6 which does not contain any DEA information**).

b6

[redacted] advised when DEA Form 6 contains DEA investigative information, it should be referred to DEA, after any FBI information has been processed. DEA will make a direct response to the requester. If the information relating to their agency is a small portion, a telephonic consultation with their agency can be made in order to save time. The file number at the top of the DEA Form 6 (item #3) indicates whether DEA or the FBI was the originator of the information. [redacted] advised that their file numbers usually start with C1.

b6

Duplication

Duplication of Microfiche/Microfilm

To have paper copies made of information that is maintained on microfilm or microfiche, contact the Micrographics Unit on extension 3815, Room 1B-301. An administrative duplication form must be completed for personnel of that unit to duplicate the material. This form can be completed over the phone by micrographics personnel or copies of the form can be sent to the LT or PLS for completion and returned to the Unit. Once the material has been duplicated, it will be sent to the LT or the PLS through the Bureau mail, unless a request had been made to be notified for it to be picked up.

Duplication of Processed Material

Where duplication fees are applicable, materials should not be duplicated until the requested amount of money has been received from the requester. This will eliminate unnecessary duplication costs to the FBI in the event the requester should abandon the fees.

Once responsive FOIPA files have been processed and fees, if applicable, have been received, the material may then be sent to the Duplication Center. At this time, the attached duplication form should be affixed to all volumes/sections in which duplication is requested. In addition to providing your name, date, extension and room number on this form, it should also indicate the number of copies requested, the subject matter, file number/section and any comments for special duplicating instructions, such as reducing the image to 98%, etc.

ELSUR Index Records

A search of the ELSUR index can surface three types of references: 1) a **principal** means the individual/organization is the target of the ELSUR, 2) an **overhear** indicates the conversation of a third party (other than the principal) has been recorded and 3) a **mention** indicates that a participant of the recorded conversation mentioned the name of a third party. Form 0-63 (copy attached) should be used when requesting an ELSUR search. Under "**REQUEST FOR SEARCH OF ELSUR INDEX FOR THE PURPOSE OF:**" check the FOIPA block and write **principals only** next to it.

ELSUR index records showing electronic coverage in foreign intelligence, counter intelligence or international terrorism investigations, should be carefully reviewed to determine whether or not the (c)(3) exclusion is appropriate before admitting the existence of the record. Where the mere existence of the electronic coverage is classified, the (c)(3) exclusion may be appropriate.

ELSURS Conducted in Criminal, Domestic Security and FCI Investigations

The history of electronic surveillance at the federal level is set forth in House of Representatives Report 95-1283 which pertains to the Foreign Intelligence Surveillance Act (FISA). This six page summary, which is available in the FOIPA library, explains the development of the FBI's authority to use electronic surveillance in criminal, domestic security and foreign counterintelligence/international terrorism investigations. Each of these investigative programs has a specific date identified after which a court order is required to conduct electronic surveillance as follows:

A) ELSUR Conducted in Criminal Investigations

Prior to 6/19/68, electronic surveillance in criminal investigations was generally conducted without a court order. **Effective 6/19/68**, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. ' 2510-2520) was enacted. With the establishment of this statute, Title III not only banned warrantless electronic surveillance in criminal investigations, it specified the offenses against which electronic surveillance could be used (18 U.S.C. ' 2516).

For electronic surveillance conducted in criminal investigations prior to 6/19/68 (pre-Title III), the following FOIA exemptions may be asserted depending upon the type of request being made:

- 1) When a request has been made by a non-participant in the intercepted

FOIPA Numbered Memo 26

Page 3

Electronic Surveillance (ELSUR) Records

conversation, Exemption (b)(7)(C) and/or (b)(7)(D) may be asserted on information which would tend to identify an individual or source.

2) When a request is made by a participant in the conversation, the requester's side of the conversation should be released, however, all conversations of a third party should be withheld pursuant to Exemption (b)(7)(C) if it would tend to identify the individual. If the release of information to a participant would pose potential harm or threaten the safety of the participant's life, then, Exemption (b)(7)(F) can be considered to withhold the information.

(In processing items 1 and 2, if any of the participants in the conversation are deceased, the information must be released. The only privacy interests left to be protected are those held by living persons who are mentioned in the conversation.)

3) Exemption (b)(7)(D) may be asserted, in addition to (b)(7)(C), for third party requests wherein the electronic surveillance was conducted with the consent of one of the parties to the conversation. **However, if the requester is the party who gave the consent**, then the requester should be given access to his/her side of the conversation as discussed in item 2.

4) If the investigation in question or a related investigation is pending when the request is received, Exemption (b)(7)(A) is appropriate if release will interfere with enforcement proceedings. This may be the case when an organized crime investigation is involved.

For those intercepts after 6/19/68, post-Title III, Exemption (b)(3) should be invoked in addition to the exemptions discussed above.

B) ELSUR Conducted in Domestic Security/Terrorism Investigations

In general, these investigations focus on organizations and individuals ("enterprises"), other than those involved in international terrorism or which have a nexus to a foreign government, whose goals are to achieve political or social change through activities that involve force or violence.

Prior to 6/19/72, electronic surveillance in domestic security cases was generally conducted without a court order. **On 6/19/72**, the decision in United States v. United States District Court 407 U.S. 297, changed this procedure. This decision, commonly called the Keith Case, mandated a court order in such cases. The Attorney General Guidelines on domestic security/terrorism investigations have, since 4/5/76, mandated that non-consensual electronic surveillance must be conducted pursuant to the warrant procedures and requirements of Title III

FOIPA Numbered Memo 26

Page 4

Electronic Surveillance (ELSUR) Records

of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended). In other words, when members of the group being investigated commit, or intend to commit imminently, an offense specified in 18 U.S.C. ' 2516, any non-consensual electronic

surveillance conducted to investigate that offense must be conducted pursuant to a Title III court order. **Therefore, the records from such intercepts conducted on or after 6/19/72, are withheld pursuant to Exemption (b)(3).**

For intercepts prior to 6/19/72, pre-Keith intercepts, or those involving the consent of one of the parties to the conversation, apply the principles discussed above regarding pre-Title III criminal investigations.

C) ELSUR Conducted in Foreign Counterintelligence/International Terrorism Investigations

Foreign Counterintelligence (FCI) investigations are conducted to protect against espionage and other intelligence activities, sabotage, or assassinations conducted by, or on behalf of foreign powers, organizations or persons, or international terrorist activities.

International terrorism investigations are conducted for activities of the following nature:

1. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any State; or that would be a criminal violation if committed within the jurisdiction of the U.S. or of any State;
2. Appears to be intended:
 - a) to intimidate or coerce a civilian population;
 - b) to influence the policy of a government by intimidating or coercion; or
 - c) to affect the conduct of a government by assassination or kidnaping; and
3. Occur totally outside the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

The Foreign Intelligence Surveillance Act (FISA), which was enacted on 10/25/78, was the first legislation governing the use of electronic surveillance in these investigative programs. **Prior to 10/25/78**, pre-FISA, electronic intercepts were generally conducted without a court order. **Post-FISA intercepts are generally conducted pursuant to a court order**, but in rare

FOIPA Numbered Memo 26

Page 5

Electronic Surveillance (ELSUR) Records

cases are conducted without one.

Exemptions (b)(1), (b)(7)(A) and (b)(7)(C) may be applicable to records from pre-FISA intercepts. The Exemption (b)(1) and (b)(7)(C) implications are obvious, but those involving (b)(7)(A) are less so. The National Security Division, Division 5, should be consulted if necessary to determine whether the investigation in question is ongoing in another form or whether there is a related, pending investigation which may be impaired through disclosure.

Post-FISA intercepts can be protected by these same exemptions, however, Exemption (b)(3) is also available. Application of Exemption (b)(3) is relevant when the records which resulted from the intercept can no longer be classified and Exemption (b)(1) can no longer be invoked.

Consensual monitoring situations occurring prior to 10/25/78, which are not covered by the FISA, did not require a court order. The Attorney General Guidelines for FCI investigations state that FBIHQ may authorize consensual monitoring for up to 90 days, with extensions available if necessary. Although Exemption (b)(3) would not be available, the other exemptions discussed above could be applicable.

Court Orders Prohibiting Disclosure of ELSUR Material

When a request is received for records which are covered by a court order prohibiting disclosure, that information should be denied as the FBI has no discretion to release the records. There can be no "improper withholding" under these circumstances. See GTE Sylvania, Inc. v. Consumers Union, 445 U.S. 375 (1980). The court order should be cited as the basis for withholding the records.

The following topics are listed for assistance in handling ELSUR material, particularly those topics which are known to involve court orders:

**ELSUR Information Pertaining to
Martin Luther King, Jr., and The Southern Christian
Leadership Conference (SCLC)**

The United States District Court for the District of Columbia has ordered results of certain microphone and telephone surveillance of Dr. King and the SCLC turned over to the National Archives and sealed for fifty years, Lee v. Kelley, No. 76-1185, and SCLC v. Kelley, No. 76-1186 (D.D.C. Jan. 31, 1977). This order includes paraphrased information obtained through electronic coverage which is included in documents such as letters, letterhead memoranda and reports.

FOIPA Numbered Memo 26

Page 6

Electronic Surveillance (ELSUR) Records

PLSs should be alert for documents reporting contacts between individuals and Dr. King or representatives of the SCLC. If the information reported could have originated from some electronic coverage of Dr. King or the SCLC, consult with Supervisory PLS

b6

ELSUR Records in the Matter of David Dellinger et al., (Chicago Seven)

On 2/26/74, a protective order was issued by the United States District Court for the District of Columbia in the matter of David Dellinger vs. John N. Mitchell, which placed restrictions on the release and dissemination of ELSUR documents and records involved in that case. The material in question dealt specifically with ELSUR coverage of the plaintiffs, David Dellinger, Jerry C. Rubin (deceased), Lee J. Weiner, John R. Froines, Abbott H. Hoffman aka Abbie Hoffman (deceased), Thomas E. Hayden, Rennard C. Davis aka Rennie Davis, as well as the Black Panther Party. Although the order did not specially prohibit the FBI from releasing documents involved in the case, the Court=s permission was sought each time such a disclosure was to be made.

On 11/28/77, this Order was modified to permit dissemination of the logs and transcripts mentioned above pursuant to FOIPA requests by any person who was overheard or mentioned in any of these electronic surveillance.

Release of Information from Wiretaps
NH 605-R* and NH 687-R*

Memorandum dated 11/28/80, advised that in the civil action of Miriam Abramovitz, et al., v. James Ahern, et al., (U.S.D.C., D Conn.) Civil Action No. N77-207, an agreement was entered into by the government and the plaintiffs. In this agreement a complete copy of the logs and transcripts from NH 605-R* and NH 687-R* (wiretaps on the Black Panther Party in New Haven, Connecticut) was provided to the plaintiffs. In exchange, the plaintiffs dropped allegations of illegal activity by the Federal defendants (four Former FBI Special Agents) which arose out of the Federal wiretaps.

Many of the 165 plaintiffs in this civil action are from the New Haven area and are represented by attorney John R. Williams. In addition, a number of them have made FOIPA requests, the processing of which may involve the same ELSUR logs, transcripts or information from NH 605-R* and NH 687-R*.

In view of the release already made of the logs and transcripts, any information from these two wiretaps, including the source symbol numbers, can generally be released without excision to any individual who was a party to the conversation, a plaintiff in the civil action or known to be represented by John R. Williams. See **Attachment 2** for the list of plaintiffs represented by Mr. Williams in the above-referenced civil suit.

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Executive Secretariat Control Data Sheet
Date: March 31, 1998

Executive Secretariat Control Data Sheet

Attached is a copy of an Executive Secretariat Control Data Sheet. These control sheets are used by the Departmental Executive Secretariat to track certain incoming correspondence and replies. From time to time these sheets are retrieved during a search for records responsive to FOIPA requests.

In processing the control sheets for release, it is not necessary to refer them to the Executive Secretariat for its determination, but please keep in mind that the sheets may contain sensitive information that warrants protection in the same way as the underlying records. In many instances, the sheets simply describe the correspondence in a summary fashion and indicate the office(s) to which the correspondence is being directed. In other cases, however, they may include information that may be withheld under various FOIA exemptions (for example, to protect material that is predecisional and deliberative or that implicates personal privacy concerns.)

The Executive Secretariat is no longer using the notation, **AT THIS DOCUMENT MUST BE DISPOSED OF BY SHREDDING,** so you do not need to be concerned about its significance on prior versions of the form. If you have any questions about processing the control sheets, please do not hesitate to call DOJ/OIP at 514-4251.

Procedures in Handling Possible Exclusion Records

For the most part, exclusions are rarely asserted on FBI records. In most instances, any consideration for the possible assertion of an exclusion will be initiated by the LT in RMU during the initial review of the file to determine if it is identifiable to the subject. On rare occasions, this may be determined after a case has been assigned to a Disclosure Unit.

If there is an indication by a review of the file that an exclusion might apply, immediately notify and discuss the case with your Team Captain. If the Team Captain is in agreement, then the FOIPA Exclusion Coordinator should be contacted and provided with the case folder along with the identifiable file(s). If an exclusion is appropriate, the LT or PLS will be advised by the Coordinator, who will in turn, handle all of the paperwork. If an exclusion is not necessary, the Coordinator will also advise the LT or PLS of such and routine processing of the file may be conducted.

I. Examples of Authorities Which are (b)(3) Statutes Central Intelligence Agency (CIA) Personnel

Section 6 of the Central Intelligence Agency Act of 1949, requires the Director of the CIA to protect from disclosure, the organization, functions, names, official titles, salaries and numbers of personnel employed by the CIA from public disclosure pursuant to 50 U.S.C., ' 403g.

CIA Intelligence Sources and Methods

50 U.S.C. ' 403-3(c)(6) requires the Director of the CIA to protect its intelligence sources and methods.

Grand Jury Information

Federal Rules of Criminal Procedure (FRCP) Rule 6(e) generally prohibits disclosure of matters occurring before a Federal grand jury. Since a FRCP is usually promulgated by the U.S. Supreme Court, the argument has been made that such a rule cannot be used as Exemption (b)(3) authority because no statute is involved. However, since Congress did enact Rule 6(e) by statute, the courts have held that Rule 6(e) can be used as an Exemption (b)(3) statute.

The District of Columbia Circuit Court (D.C. Circuit) has limited the use of Rule 6(e) as an Exemption (b)(3) statute, at least in that circuit. In order to prevent the Government from shielding information from the public simply by presenting the information to a grand jury, the D.C. Circuit has held that Rule 6(e) only prohibits the disclosure of information concerning the inner workings of the grand jury. Senate of Puerto Rico v. U.S. Department of Justice, 823 F. 2d 574, 582 (D.C. Cir. 1987). Included in the inner workings concept **protected by Exemption (b)(3) are such items as grand jury transcripts or subpoenas, the identities of witnesses or jurors, the substance of testimony to the grand jury, the strategy or direction of a grand jury investigation, and the deliberations or questions of the jurors.**

Records falling into such categories as grand jury transcripts and subpoenas are easy to recognize, but it is another matter to determine whether a record reveals the strategy or direction of a grand jury investigation. It can be especially difficult for someone not familiar with the investigation, with the background knowledge possessed by the subject concerning the matter under investigation. In Senate of Puerto Rico, for instance, the D.C. Circuit held that a release of all nonexempt records in an investigative file would not reveal the inner workings of the grand jury if the grand jury material was not labeled as such. Under those circumstances, the court reasoned the requester would be unable to even determine which records had been submitted to the grand jury. This overlooks the fact that a sophisticated requester can determine

FOIPA Numbered Memo 29

Page 3

Exemption (b)(3)

which records went to the grand jury if he has enough knowledge and experience to know which records could only be obtained with a grand jury subpoena. That, in turn, could reveal the direction of the grand jury investigation.

Compounding the problem is the fact that most of the other circuit courts have not decided this issue. Furthermore, at the time a FOIPA request is initially processed, one cannot be certain in which circuit a disgruntled requester will eventually file suit. Without that information, one cannot determine which rule of law to apply.

In light of these problems, the following processing procedure will be followed. At the initial processing stage, Exemption (b)(3) shall be applied to all properly stamped grand jury material. If it is obvious that records bearing the grand jury stamp were not actually submitted to the grand jury, that material should be reviewed for all other applicable FOIA exemptions which may be invoked. However, this procedure should be discussed with the Unit Chief prior to disclosure of any material.

Intelligence Sources and Methods of the FBI

50 U.S.C., § 403-3(c)(6) authorizes not only the CIA, but other intelligence gathering agencies of the Federal Government, including the FBI, to protect their intelligence sources and methods. Often there is an overlap between the Exemption (b)(1) and Exemption (b)(3) protection of intelligence sources and methods. Citing these two exemptions in conjunction with one another is appropriate; however, either can be cited independently of the other. The Exemption (b)(3) protection has an equal force to the Exemption (b)(1) protection. Therefore, should Exemption (b)(1) be downgraded, Exemption (b)(3) could still be applied in situations where release of the information would jeopardize the FBI's intelligence sources and methods.

Foreign intelligence and counterintelligence investigations are vital aspects of the FBI's law enforcement mission. When it engages in these activities, the FBI utilizes national security intelligence sources and methods and relies not only on the Executive Order, but also on Exemption (b)(3), 50 U.S.C. 403-3(c)(6) to protect these intelligence sources and methods from disclosure under the FOIA.

With respect to intelligence sources in particular, the Supreme Court has held that the broadest possible protection is necessary in order for intelligence agencies to carry out their mission and to protect the intelligence process. The Court recognized that intelligence sources are diverse and are not limited to covert or secret agents but may include such open and innocuous sources as books, magazines, newspapers, and the citizens who travel abroad. As to all intelligence sources, the court held that they must be provided an assurance of confidentiality that is as absolute as possible. @

Internal Revenue Code

26 U.S.C. Section 6103 of the Internal Revenue Code protects tax records obtained from the Department of the Treasury. If tax records were obtained from a source other than the Department of the Treasury, then Exemptions (b)(6) and (b)(7)(C) should be considered in third party requests. See FOIA Update, Volume IX, No. 2, page 5.

Juvenile Delinquency Act and Juvenile Justice Delinquency Prevention Act (JJDPA)

18 U.S.C. ' 5038, which is known as the Juvenile Delinquency Act, protects records of juvenile delinquency proceedings.

The attached memorandum of 11/17/87, from the Office of Information and Privacy (OIP), clarifies instructions regarding JJDPA documents. (See Attachment 1)

In summary, OIP suggests that although the Juvenile Justice and Delinquency Prevention Act (JJDPA) qualifies as an Exemption (b)(3) statute, it should not be invoked to deny the juvenile access to his/her own file. Similarly, information pertaining to other adult subjects unrelated to the juvenile and reasonably segregable cannot be withheld. OIP further suggests that to ensure the privacy interests of juvenile offenders, Exemption (b)(7)(C) in conjunction with Exemption (b)(3) should be used to protect records showing a juvenile's arrest regardless of whether the juvenile was subsequently released or formally charged.

OIP also notes that the JJDPA authorizes release of the final disposition to a victim or immediate members of a deceased victim's family. Should the court's sentence or court's disposition appear in the records (not the AUSA=s opinion concerning prosecution), it can be disclosed to the victim or deceased victim's family upon satisfactory proof of identity.

Furthermore, the JJDPA should not be confused with the Federal Youth Corrections Act which is not an Exemption (b)(3) statute. Thus, the PLS must be certain under which statute the subject was prosecuted before it can be determined if Exemption (b)(3) applies.

National Driver Register

23 U.S.C., Section 206 (c) protects from third party requesters information obtained by the Secretary of Transportation for the National Driver Register concerning drivers who have committed serious traffic offenses.

National Drivers Records Act

On 2/3/88, National Highway Safety Administration, Department of Transportation, advised that the National Drivers Records Act is a (b)(3) statute, and any information furnished to the FBI from this system of records is exempt from THIRD PARTY access under (b)(3). Information from this system is releasable to a FIRST PARTY requester.

National Security Agency

Public Law 86-36, Section 6(a) protects the organization of the National Security Agency, its function and activities, and the names, titles, salaries, and number of its employees.

Pre-sentence Reports

18 U.S.C. ' 4208(c) and Rule 32(c)((3)(A) of the Federal Rules of Criminal Procedure exempt those portions of a pre-sentence report pertaining to a probation officer=s sentencing recommendations, diagnostic opinions which would seriously disrupt a rehabilitation program if disclosed, information obtained upon a promise of confidentiality, and information which might result in harm to any person if disclosed.

Title III, Wiretap Intercepts

18 U.S.C., Section 2518 (8) governs the disclosure of information from Title III wiretap intercepts. This statute does not cover all wiretap intercepts. (**See Electronic Surveillance Records, Memo 26, for a detailed discussion of the applicable exemptions for wiretaps.**)

Visas and Permits; Issuance or Refusal of

8 U.S.C., ' 1202(f) protects records pertaining to the issuance or refusal of visas and permits to enter the United States. Generally, all Visa/Permit matters are referred to the Department of State for handling.

Witness Security Program

18 U.S.C., Section 3521 in conjunction with the implementing regulations found at 28 C.F.R., Section 0.111b protects information concerning the identity, location or any other details concerning a person receiving protection afforded by the Witness Security Program. Thus, if a request contains information on the Witness Security Program, the material is protectible pursuant to Exemption (b)(3). [REDACTED]

Exemption (b)(3)

Furthermore, use any other appropriate exemptions, such as (b)(7)(C) or (b)(7)(D). This has been coordinated with the Department of Justice (DOJ), Office of Information and Privacy.

II. Examples of Authorities Which Are Not (b)(3) Statutes:
Pen Registers and Trap & Trace Devices

A **pen register** is a device used to log dialing, routing, addressing and signaling information transmitted by a standard telephone, a cellular telephone, an internet user or e-mail account, or a web site internet protocol (IP) address. Typically, a pen register logs phone numbers dialed from a telephone or e-mail addresses and web site IP addresses reached by an internet account holder's computer. See 18 U.S.C. ' 3127(3), as amended by The USA Patriot Act, Public Law 107-56, ' 216(c)(2)(A) (October 26, 2001). A **trap & trace** is similarly used but instead, logs the telephone numbers of incoming phone calls, the e-mail addresses of incoming e-mail messages on an internet account holder's computer, or the IP addresses of incoming computer connections made to an internet account holder's web site. See 18 U.S.C. ' 3127(4), as amended by The USA Patriot Act, Public Law 107-56, ' 216(c)(3)(A) (October 26, 2001).

For devices installed on telephone lines prior to January 18, 1987, it was DOJ policy to obtain a court order before using a pen register or trap & trace device. Such orders were obtained pursuant to the Federal Rules of Criminal Procedure rather than 18 U.S.C. ' 3123 and were typically sealed orders so as not to disclose the existence of the surveillance effort. For devices installed on telephone lines **after January 18, 1987**, federal law mandates that absent consent of the party in whose name the telephone line is listed, a court order must be obtained prior to installing or using a pen register or trap & trace device. 18 U.S.C. ' 3123, as amended by The USA Patriot Act, Public Law 107-56, ' 216(b)(October 26, 2001). The judge authorizing a pen register or trap & trace device is required to seal the order so as not to disclose the existence of the surveillance effort. 18 U.S.C. ' 3123(d).

For devices used on cellular telephone communications, there will be three distinct time periods in which the law varies on the installation rules and regulations:

(1) **Prior to October 21, 1986**, there was no law requiring the FBI first obtain a court order before using a pen register or trap & trace device to obtain the telephone numbers dialed to or from a cellular telephone. Therefore, no court sealing order will exist to protect such material from disclosure. Thus, consider other FOIA Exemptions as discussed below.

(2) **From October 21, 1986 until October 26, 2001**, it was DOJ policy to interpret federal law as mandating that absent consent of the party in whose name the cellular telephone account

FOIPA Numbered Memo 29

Page 7

Exemption (b)(3)

was listed, a court order had to be obtained prior to using a pen register or trap & trace device to obtain the telephone numbers dialed to or from the cellular telephone. 18 U.S.C. ' 3123, as amended by The Electronic Communications Privacy Act of 1986, Public Law 99-508 ' 301 (October 21, 1986). Pursuant to this interpretation, whenever a pen register or trap & trace device was authorized, DOJ sought - and the judge was expected to issue - a sealing order so as not to disclose the existence of the surveillance effort. 18 U.S.C. ' 3123(d).

(3) After October 26, 2001, federal law mandates that absent consent of the party in whose name the cellular telephone account is listed, a court order must be obtained prior to using a pen register or trap & trace device to obtain the telephone numbers dialed to or from a cellular telephone. 18 U.S.C. ' 3123, as amended by The Electronic Communications Privacy Act of 1986, Public Law 99-508 ' 301 (October 21, 1986), as amended by The USA Patriot Act, Public Law 107-56, ' 216(b) (October 26, 2001). The judge authorizing a pen register or trap & trace device is required to seal the order so as not to disclose the existence of the surveillance effort. 18 U.S.C. ' 3123(d).

Note, with cellular telephone surveillance, a court order may not have been required if investigative agents, without the assistance of the cellular telephone company, collected via a pen register device only the electronic serial number (ESN) of the cellular telephone or the location of the cellular telephone caller ("cell site information"). If the ESN or cell site information is among the material responsive to the FOIA request and there is no indication that during the investigation a court order was obtained to collect this information, consider other FOIA Exemptions to withhold such material as discussed below.

For devices installed on an internet account holder's computer connections, there will also be three distinct time periods in which the law varies on the installation rules and regulations:

(1) Prior to October 21, 1986, there were few e-mail or internet communications occurring. Thus, it is extremely unlikely that there will be information in FBI files collected from surveillance of such electronic communications. Nonetheless, prior to October 21, 1986, there was no law requiring the FBI first obtain a court order before installing pen registers or trap & trace devices on an internet account holder's computer connection. Therefore, no court sealing order will exist to protect such material from disclosure. Thus, consider other FOIA Exemptions as discussed below.

(2) From October 21, 1986 until October 26, 2001, it was DOJ policy to interpret federal law as mandating that absent consent of the party in whose name the internet service account was listed, a court order had to be obtained prior to installing or using a pen register or trap & trace device. 18 U.S.C. ' 3123, as amended by The Electronic Communications Privacy Act of 1986, Public Law 99-508 ' 301 (October 21, 1986). Pursuant to this interpretation, whenever a pen

FOIPA Numbered Memo 29

Page 8

Exemption (b)(3)

register or trap & trace device was authorized, DOJ sought - and the judge was expected to issue - a sealing order so as not to disclose the existence of the surveillance effort. 18 U.S.C. ' 3123(d).

(3) After October 26, 2001, federal law mandates that absent consent of the party in whose name the internet service account is listed, a court order must be obtained prior to installing or using a pen register or trap & trace device. 18 U.S.C. ' 3123, as amended by The Electronic Communications Privacy Act of 1986, Public Law 99-508 ' 301 (October 21, 1986), as amended by The USA Patriot Act, Public Law 107-56, ' 216(b) (October 26, 2001). The judge authorizing a pen register or trap & trace device is required to seal the order so as not to disclose the existence of the surveillance effort. 18 U.S.C. ' 3123(d).

FOIA Processing: 18 U.S.C. ' 3123(d) requires the court seal: (1) the application for a pen register or trap & trace device and, (2) the court order approving use of the device. Typically, the court sealing order will read:

IT IS ORDERED FURTHER, pursuant to Title 18, United States Code, Section 3123(d), that this order and the application be sealed until otherwise ordered by the Court, and that (name the communications service provider(s)), its agents and employees shall not disclose the existence of the (pen register) (and/or) (trap and trace device), the existence of this order, or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

Thus, the court sealing order prohibits FOIA disclosure of the court order itself and the contents of the application which will include: the identity of the party on whose telephone line or internet account the device was placed, the identity of the party who is the subject of the criminal investigation, the identity or location of the telephone service provider or internet service provider (ISP) to which the pen register or trap & trace order applies, the geographic limits of any trap & trace effort, and the telephone number, e-mail address, or IP address to which the pen register or trap & trace order applies. **These items are therefore withheld from FOIA disclosure due to the court sealing order, not FOIA Exemption (b)(3).** See GTE Sylvania, Inc. v. Consumers Union, 445 U.S. 375 (1980). If the file does not indicate the court sealing order is lifted, assume it is still sealed and withhold this information pursuant to the court sealing order. You must locate and read the court sealing order to determine if it also applies to protect from disclosure the information collected by use of the pen register / trap & trace device.

The following other FOIA Exemptions should be considered if: (1) the court sealing order cannot be located, (2) the court sealing order does not indicate that it applies to protect the

FOIPA Numbered Memo 29

Page 9

Exemption (b)(3)

information collected by use of the pen register or trap & trace device, (3) the file indicates that the court sealing order is lifted, (4) the file reveals technical or mechanical details about the pen register or trap & trace device, (5) a court order was not required due to the inapplicability of the pen register / trap & trace statute at the time of the communication (see the relevant dates, above) or, (6) the pen register or trap & trace device was installed with the consent of the party in whose name the telephone, cellular, or internet service account is listed.

(a) Exemption (b)(7)(C) should still be asserted absent a privacy waiver, to protect the identifiers of any living third party on whose telephone line, cellular service, or internet account the device was placed, the identifiers of any living third party who is the subject of the criminal investigation, the identifiers or location of the telephone service provider, cellular service provider, or ISP to which the pen register or trap & trace order applies, the geographic limits of any trap & trace effort, the telephone number, e-mail address, IP address, or cellular telephone ESN, of any living third party to which the pen register or trap & trace order applies, and the identifiers, telephone numbers, e-mail addresses, or IP addresses of any living third parties obtained from utilization of the device.

(b) Exemptions (b)(2) / (b)(7)(E): Exemption (b)(7)(E) will not protect the use or existence of pen register or trap & trace devices as "investigative tools" since their general principles of operation have been widely publicized. However, Exemptions (b)(2) / (b)(7)(E) will apply to protect the technical or mechanical details regarding these devices. For cellular telephone surveillance, Exemptions (b)(2) / (b)(7)(E) protect details such as computer code words, terms, and phrases; testing and calibration procedures and results; software configurations concerning the surveillance system; the vulnerabilities or capabilities of such systems; techniques and methods for locating a cellular telephone caller; and any other information that would enable those using wireless telecommunications for criminal activities to alter or redirect their actions to avoid having their communications collected. For ISP computer connection surveillance, Exemptions (b)(2) / (b)(7)(E) protect details such as computer code words, terms, and phrases; testing and calibration procedures and results; software and network configurations concerning the surveillance system; vulnerabilities or capabilities of such systems; and any other information that would enable those using internet connections for criminal activities to alter or redirect their actions to avoid having their communications collected.

Others

1) **Executive Orders** and **Federal Regulations** do not qualify because they are not statutes.

2) **Federal Rules of Procedure** promulgated by the Supreme Court generally do not qualify unless they are modified and specifically enacted into law by Congress, thus becoming

FOIPA Numbered Memo 29

Page 10

Exemption (b)(3)

Astatutes. @ See Fund for Constitutional Government v. National Archives and Records Service, 656 F. 2d 856 (D.C. Cir. 1981). [See prior discussions of **Rule 6(e)** and **Rule 32 of the Federal Rules of Criminal Procedure**, which were specifically enacted into law by Congress.]

3) **5 U.S.C., Section 551 of the Administrative Procedure Act** does not qualify because it merely defines terms. (This section, which defines the term AFederal Agency, @ apparently has been erroneously used to exempt documents prepared by the Judicial and Legislative Branches.)

4) The **Privacy Act** is not an Exemption (b)(3) statute because Congress explicitly provided so in Public Law 98-477.

5) **28 U.S.C., Section 534** does not qualify because it does not expressly prohibit the disclosure of Arap sheets. @ See Reporters Committee for Freedom of the Press v. Department of Justice, 816 F. 2d 730, at 736 n.9 (D.C. Cir. 1987). Note, however, that Exemptions (b)(6) and (b)(7)(C) may be used to protect third party requests for rap sheets of living subjects.

6) The **Copyright Act of 1976**, 17 U.S.C., Section 101-810, does not qualify because it specifically permits public inspection of copyrighted documents. Note, however, that application of Exemption (b)(4) to copyrighted documents may be appropriate. For an overview of this issue, see FOIA Update, Fall 1983, at 3-5, ACopyrighted Materials and the FOIA. @

7) **The Federal Youth Corrections Act (FYCA)** which began as 18 U.S.C. ' 5005, is not an Exemption (b)(3) statute. Thus, a PLS must be certain under which statute the subject was processed, the previously mentioned Juvenile Justice Delinquency Prevention Act or the FYCA, before making a determination on whether Exemption (b)(3) applies or not. Furthermore, if the requester=s conviction was set aside under Section 5021 of the FYCA, one must determine whether the court issued an order for the record to be sealed. If conviction records have been ordered sealed, they should not be released pursuant to an FOIA or PA request. The PLS should advise the requester that records are sealed from disclosure pursuant to FYCA Court Order by citing the court case number and the date of the order (i.e., #84-726-CR-RYSKAMP, dated September 4, 1987).

Exemption (b)(7)(D)

Aforeseeable harm@ in releasing the information could be subject to discretionary release.

In most instances, it will no longer be appropriate to protect the source of information under Exemption (b)(7)(D) in the following situations when it is an exchange of routine information@:

1) **Police Departments (PD)** negative record checks, arrest records
(Exception: Exemption (b)(7)(D) may be applied to actual PD records which contain information from their investigation or intelligence reports.)

2) **State and local agencies** (marriage records, court documents, Department of Motor Vehicles, Board of Elections, etc.)

3) **Credit Bureau reports**
(Exception: Dunn and Bradstreet reports which are protected under expressed confidentiality.)

4) **Commercial Institutions** (schools or college registrars, utility companies {telephone, electric, gas companies}, insurance companies, etc.)

If any of the above information indicates that the material may not be released to the public or otherwise used without the production of a subpoena duces tecum, then Exemption (b)(7)(D) should be utilized to protect the identity of the source and, if necessary, the information since this statement is paramount to an expressed assurance of confidentiality.

Exemption (b)(7)(C) should continue to be applied to protect information, the release of which would be an unwarranted invasion of privacy, i.e., the name of the individual who provided the information and information pertaining to third parties.

Expressed Confidentiality

The Landano ruling did not affect instances where an expressed assurance of confidentiality was granted to the source. The identity of and the information provided by these sources may be protected by the first and second clauses of Exemption (b)(7)(D), respectively. However, the Reno policy should be applied to the source=s information and discretionary releases made where there is no Aforeseeable harm@ to the confidential source. **The following are examples of sources granted an expressed assurance of confidentiality:**

1) **T-symbols and permanent symbol source numbers** - assert exemptions (b)(2) and (b)(7)(D) for human sources. For non-human sources (i.e., techs, mikes, telephones, etc.) assert only exemption (b)(2), unless doing so will identify human sources. (See, Mosaic Theory, infra.)

2) **Paid informants**

Exemption (b)(7)(D)

3) **Potential Security Informant (PSI) and Potential Criminal Informant (PCI)**

4) **Specifically stated ARequest Identity,@ AProtect Identity by Request (PIBR),@ AConfidentiality Requested,@ etc.**

5) **Foreign Agencies/Authorities** (Refer to the G-1 Guide)

Informant File Numbers

It is also important to protect the file number of an informant case as well as any other material which would identify the informant. The informant file designations are shown below:

- 134 - Security Informant
- 137 - Criminal Informant
- 170 - Extremist Informant
- 270 - Cooperative Witness

FOIA exemptions (b)(7)(D) and (b)(2) are appropriate to protect these file numbers.

Mosaic Theory

Once it has been established that Exemption (b)(7)(D) is being utilized for informant information, the PLS should be aware of the A mosaic theory,@ which involves the analysis of apparently innocuous bits of information to identify sensitive sources, methods or investigative direction. The PLS should become familiar with the overall investigation and any related files to be processed. He/she should be aware of the informant information and its reappearance later in the same investigation or any related files abbreviated or written in paraphrased form. If this information is singular in nature or would tend to identify the source, even though the normal identifiers are not indicated (i.e., the source=s name, symbol number, etc.), then the information may be exempt pursuant to Exemption (b)(7)(D) under the mosaic theory.

Foreign Agencies and Authorities

In many instances, foreign police departments or foreign authorities are classified; however, several are not. The PLS should refer to the G-1 Classification Guide to identify foreign agencies/authorities (listed in alphabetical order by countries) cooperating with the FBI and whether confidentiality has been requested. In those cases where a foreign agency/authority

FOIPA Numbered Memo 31

Page 4

Exemption (b)(7)(D)

is not classified, it is the responsibility of the PLS to insure the level of protection requested by the foreign agency/authority is honored (i.e., some may request only their identity be protected, while others do not mind that their cooperation is made public and they may or may not request their information be protected. Others may request that neither their cooperation nor their information be made public). If the foreign agency/authority is not listed on the G-1 Guide and there is no indication on the document of whether confidentiality was requested, the PLS should review the material to determine if there was implied confidentiality and process accordingly.

Police Departments/Sheriff Offices Requesting Confidentiality

In processing FBI records, the following police departments and sheriff offices have requested confidentiality for their identity and information provided:

- 1)
- 2)
- 3)

--

b7D

For a further discussion and an in-depth review of exemption (b)(7)(D), please refer to the Freedom of Information Act Guide and Privacy Act Overview publication provided by the Department of Justice.

FOIPA Numbered Memo 32

Page 2

Exemption (b)(7)(E)

Listed below are some situations where Exemption (b)(7)(E) might apply:

- 1) Location, denomination, and serial numbers of bait money (See Memo 43)
- 2) Location, activation, and type of bank security devices (See Memo 43)
- 3) Location and type of cars used in a surveillance
- 4) Mechanics of surveillance
- 5) Airplane surveillance to include the locations of the surveillance and types of aircraft used.
- 6) Model, serial number and type of recording equipment (e. g. transmitters)
{Exemption (b)(7)(E) does not provide protection for the fact that a Nagra body recorder was utilized in an investigation.}
- 7) Mechanics of installation of recording equipment
- 8) Mechanics of wire tap monitoring
- 9) Certain polygraph information (See Memo 71)
- 10) Computerized Telephone Number File (CTNF)/Telephone Application (TA)
(See Memo 82)
- 11) Effectiveness ratings of known techniques (FD-515) (See Memo 44)
- 12) Personality profiles, equivocal death analysis (See Memo 66)
- 13) Infrastructure Vulnerability/Key Asset Protection Program (See Memo 55)
- 14) Mail Covers (limited use) (See Memo 64)
- 15) Pretext phone calls (Use only in the more current cases or where there is significant describable harm to the future use of this technique)
- 16)
 (See Memo 84)

b7E

b7E

FOIPA Numbered Memo 32

Page 3

Exemption (b)(7)(E)

17)

[Redacted]

[Redacted]

(See Memo 84)

b7E

Field Offices

- X. When a field office searches its indices upon receipt of a FOIPA request and determines that one or more main files exist and the investigation(s) were "reported" to FBIHQ, the field office will follow established procedures in referring those files to FBIHQ for processing. In addition, if cross-references exist, the field office will advise the FBIHQ PLS of this fact, and it will be his or her responsibility to advise the requester in the disclosure letter of the existence and that the requester must specifically request them to be processed.

- X. When a field office searches its indices and only "unreported" main files and/or "cross-references" exist, the field office PLS will process the responsive file(s) and release the material directly to the requester.

Field Office Files Transmitted to FBIHQ
(Use of Green File Fronts)

Since the field offices use the same type of file fronts as FBIHQ, on many occasions they had been confused with FBIHQ files and misplaced into the FBIHQ filing system. Therefore, it was necessary to develop special procedures for field office files being transmitted to FBIHQ so they would be visibly distinguishable from FBIHQ files. To minimize this problem, the field file front remains on the field file, but is covered by a green file front that prevents intermingling of field and FBIHQ files. Furthermore, it allows the field file front to be marked appropriately relative to FOIPA processing. No file number or other markings should be placed on the green file front so that it can be used again.

All FBI FOIPA Personnel

Page 2

April 1, 2014

Pardon Applications

The FBI is authorized to release a copy of the pardon application in its entirety to first party requesters without consulting the Pardon Attorney's Office. However, continue to consult with the office with respect to any intra-departmental memoranda or information in FBI documents which originated with the Pardon Attorney office.

FOIPA

MANUAL

MEMO 36

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: File Classification "77"
Date: March 31, 1998

File Classification "77"
DOJ and Judicial Appointment Files

The Office of the Deputy Attorney General maintains DOJ and Federal judicial appointment files which include FBI background investigation reports. When DOJ receives a request for one of those files, the request letter will be referred to the FBI for handling. Prior procedures required that the proposed release be reviewed by any Office of Information and Privacy (OIP) attorney upon completion of processing these files. By memorandum dated 4/11/96, Richard L. Huff, Co-Director, OIP, advised that these files may now be released without OIP review.

FOIPA

MANUAL

MEMO 38

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: File Classification "161"
Date: March 31, 1998

File Classification "161" Special Inquiry Investigations

The 161 classification covers investigations requested by the White House, Congressional Committees and other Government agencies. From 1993 through May 1995, former Special Agent H. Gary Harlow from the A-1 squad at WFO, was assigned to investigate or conduct some aspect of Special Inquiry investigations. In January 1996, Harlow pled guilty to several counts of an indictment in which he was charged with, among other things, falsifying his investigations in certain 161 investigations and was sentenced in U.S. District Court, Eastern District of Virginia, Alexandria, Virginia.

Special Inquiry and General Background Investigations Unit (SIGBIU) advised that all of the applicant type investigations have not been identified wherein former SA Harlow was the investigator. As of December 31, 1996, discussions with SAs Richard Hildreth, Jr., Section Chief, and [redacted] Unit Chief, SIGBIU, resulted in the following procedures being implemented when processing a 161 file pursuant to a FOIPA request within the time frame of 1993 through 1995:

b6

1) When any portion of a 161 file has been identified by SIGBIU as having been handled by Harlow, a "Routing Slip" (example attached) should appear as the top document in the file and is to be released to the requester.

2) If there is no indication in the file that SIGBIU has reviewed the file (i.e., there is not "Routing Slip" in the file) and it contains investigative material conducted by former SA Harlow, contact James [redacted] SIGBIU, Room 4371, Ext. 2568, so that SIGBIU is made aware of that specific investigation.

b6

In all instances, when PLSs are processing 161 investigations which were conducted by former SA Harlow in the above time frame, his name is to be released throughout the file.

Numbered Memo 39

Page 2

Classification "197"

Records processed for first party requesters who are a party to the civil suit or claim (i.e., a plaintiff) must be reviewed pursuant to Exemption (d)(5) of the Privacy Act. It should be noted, however that this provision in certain respects is not as broad as Exemption (b)(5) and does not incorporate certain (b)(5) privileges. It should be kept in mind the application of other PA and FOIA exemptions may be contained within the documents maintained in these files and that information should be processed accordingly.

First party requests for 197 files wherein the requester was represented by a DOJ attorney (i.e., a DOJ attorney represents an Agent who is being sued), are also processed using the (d)(5) exemption, and generally, he or she should have access to the entire file.

It is recommended the PLS refer to the DOJ/OIP FOIA Guide and Privacy Act Overview publication for a detailed and in-depth discussion concerning the application of Exemptions (b)(5)/(d)(5) and the Aforeseeable harm@ standard.

FOIPA Numbered Memo 40

Page 2

Filing of FOIPA Material

(3) **Search Slips**: The search slip(s) should be attached to one of the following: a) the yellow no record letter, b) the processed package (place between the file cover sheet and the inventory sheet of the top enclosure in the processed package), or c) stapled to the front of the initial FOIPA request.

(4) **Duplicate Copies**: Do not send the following documents to file: tickler copies, extra copies, or duplicate copies which have been made of any correspondence. Carbon copies of original correspondence directed to the FBI may be detached and destroyed, however, a notation should be made on the copy count that the additional copies have been detached. Since each piece of mail is being recorded/serialized, this will ensure that only one piece of correspondence is placed on record.

(5) **Mail not Addressed to the FBI**: Place the notation "FBI" on the lower left-hand corner of correspondence not addressed to the FBI (e.g., copies of letters sent by DOJ to the requester acknowledging receipt of an administrative appeal or advising of the final determination of the appeal). This designates it as an official FBI copy.

(6) **Receipts**: Copies of receipts which FOIPA employees sign acknowledging receipt of mail from a requester, DOJ, or another Government agency should not be sent to file. The fact that the mail is in file is sufficient acknowledgment of our possession. The only receipts that are necessary to file are those which we might ask a requester to sign acknowledging his/her receipt of certain material. Therefore, all other receipts will be kept in IPU/RTSS.

(7) **Abandoned Cases**: Form OPCA-25 should be used to transmit documents to file in cases where the material has been processed but is not sent to the requester (i.e., the material was processed and the money letter sent to the requester, but no reply was received, or the material was processed and not sent because the request was withdrawn).

(8) **Mail Returned by the Postal Service**: When material is sent to the requester and then returned by the Postal Service for insufficient address, addressee unknown, etc., the LT/PLS will write the complete file number and, if known, the serial number of the outgoing yellow at the bottom of the original letter and send the letter **with the envelope on top** to the Serialization Team to be filed behind the original yellow. There is no need to send the enclosure (the black-out copy of the release material) to the 190-file, therefore, the LT/PLS should indicate on the original letter that the enclosure has been detached and destroyed.

(9) **Copies of Original Mail**: If the original piece of mail is not available (misplaced or inadvertently destroyed) and the LT/PLS maintained a copy of the original, then the copy of this mail may be sent to file with the notation "Treat as Original" in red pencil on the bottom left side of the copy.

If the original mail is located, it will be inserted in file in place of the copy.

FOIPA Numbered Memo 40

Page 3

Filing of FOIPA Material

(10) **Placing the 190 number on the documents:** The LT/PLS should **write the 190 file number in red across the bottom of every document.** In all instances, when sending the mail to be placed on record and filed by the Serialization Team, the salmon tag (O-100c) should be completed and attached to the upper right-hand corner of the most current piece of mail. If a Universal Case File Number for the 190-file (the case number consists of seven digits) has been assigned to the FOIPA case, the 190 number should be documented and placed on the O-100c by checking the block adjacent to "Place in Existing _____". If a pre-UCFN 190-file (six digits or less) is still being used, a new UCFN 190-file number will be assigned to the case when it is sent to the Serialization Team for placing the mail on record. In this situation, the O-100c should be completed by checking the blocks adjacent to "New 190" and "Place in Existing _____", entering the pre-UCFN on this line. At the time the Serialization Team places the mail on record, a new UCFN 190 number will be assigned to the case and the old 190 number will be referenced on the UCFN 190-file jacket and on the miscellaneous field in the computer. Keep in mind that these FOIPA requesters will now have both a pre-UCFN and a regular UCFN 190 file.

(11) **Indexing:** Underline the subject in green pencil on the most recent piece of mail when the package has been assembled. If the most recent piece of correspondence is something other than the disclosure letter, such as a DOJ/OIP letter affirming an appeal or an electronic communication returning field office files, the PLS should underline the subject of the request in green pencil on the disclosure letter. This allows IPU to easily determine the subject of the request for indexing purposes.

(12) **Enclosure Behind File (EBF)/ Bulky:** When an enclosure contains 50 pages or less, the material will be placed in the main 190 file behind the original mail. If the enclosure is approximately 51 to 99 pages, the material will be placed on record as an EBF, or when over 100 pages, it will be prepared as a Bulky. This step of preparing an EBF and Bulky will be done by the Serialization Team.

(13) **TS and SCI Mail:** This mail is now being handles by the Serialization Team in IPU. Two IPU employees have been trained and can handle this mail as long as the FD-501 or FD-502 is attached. Serialization will occur in the Serialization Team and they will then have the responsibility of carrying this mail to the Special File Room (SFR) to be filed. This mail should be directed to TC Room 6359, with a note to alert her that the mail needs to be filed in the SFR.

b6

Sending Processed Personnel Material to File

When preparing processed personnel material for file, the above procedures should be followed except the 62 {Administrative Inquiry (AI)}, 67, 263, or 280 file number should be

FOIPA Numbered Memo 40

Page 4

Filing of FOIPA Material

documented on the bottom of each document instead of a 190 file number. Each piece of mail (all incoming, outgoing and inter/intra office communications) should also have "FOIPA" or "OPCA" written or stamped on the bottom right corner and the PLS should initial through the FOIPA or OPCA.

When a Privacy Act request involves processing of material from a 62 (AI), 67 or 263 file classification, only those pages containing deletions should be forwarded to the Personnel Records Section, Room 11174, for filing into the respective 62 (AI), 67 or 263 file along with the original FD-488 and/or OPCA-16 form (Disclosure letter). Please note those documents from the 67 Sub M and/or the Sub S which contain redactions are to be filed in the 67 Sub M and/or Sub S, along with a copy of the FD-488 or the OPCA-16 form, and not in the main 67 file.

If processing also involves additional file classifications other than personnel type records, a 190 file should be opened and the processed documents from the other file classification(s) should be filed in the 190 file along with a copy of the FD-488 and/or OPCA-16 form. The 190 file number should be recorded in the AMiscellaneous@ block on the computer sheet.

Note: All personnel type records must be placed in and transmitted by a messenger envelope.

Filing of Previously Released FOIPA Material

When a request is made for the same information which has been previously released, it will not be necessary to have the released documents filed again. Instead, place the notation Apreviously processed material@ in the lower left margin next to the referral blocks on the disclosure letter. A notation of the prior release should be noted on the yellow outgoing communication (disclosure letter) by indicating the 190-file number where the preprocessed material is located and the serial number (Bulky and/or EBF). The note should also include a list of the preprocessed file numbers and/or documents as well as the number of pages being released to the subsequent FOIPA requester. Further, the PLS should forward a copy of the current FOIPA release letter to the preprocessed 190-file (where the documents were originally released) in order to keep the original 190-file from being destroyed.

190 Classification Control Files

Below is a list of FOIPA control files:

190	Main File for each requester
190-0	General Type Mail, Administrative Closings
190-00	FOIPA Policy and Federal Legislation
190-1	FOIPA Regional Field Division Conferences
190-HQ-1189353	FOIPA No Record Responses
190-3	FOIA Impact on Law Enforcement Activities
190-HQ-1196409	FOIPA Reading Room Requests and Releases
190-6	FOIA Annual Report to Congress
190-710	FOIPA - Instruction to Field Offices
190-711	State Privacy Legislation
190-56511	FOIPA Training FBIHQ
190-HQ-1046286	FOIPA Third Party Denials
190-HQ-1056344	FOIPA Referral Policy Matters
190-HQ-1219218	Fiscal Year Reports
197-122	FOIPA Litigation Cases
242-42	FOIPA Automation

FOIPA Referral Help Desk Sub File List

190-HQ-C1220639-AF	All Air Force
190-HQ-C1220639-Army	All Army
190-HQ-C1220639-BOP	Bureau of Prisons
190-HQ-C1220639-CIA	Central Intelligence Agency
190-HQ-C1220639-DOD	Defense Department
190-HQ-C1220639-DOJCR	DOJ Civil Rights Division
190-HQ-C1220639-DOJCD	DOJ Criminal Division
190-HQ-C1220639-DOJMISC	DOJ Miscellaneous
190-HQ-C1220639-DEA	Drug Enforcement Agency
190-HQ-C1220639-DOE	Energy Department
190-HQ-C1220639-EOUSA	Executive Office USA
190-HQ-C1220639-INS	Immigration and Naturalization
190-HQ-C1220639-DOI	Interior Department
190-HQ-C1220639-NSA	National Security Agency
190-HQ-C1220639-NAVY	All Navy
190-HQ-C1220639-OPM	Office of Personnel Management
190-HQ-C1220639-USPS	Postal Service (All)
190-HQ-C1220639-SD	State Department (All)

FOIPA Numbered Memo 40

Page 7

Filing of FOIPA Material

FOIPA Referral Help Desk Sub File List (cont.)

190-HQ-C1220639-DOT	Transportation Department
190-HQ-C1220639-TD	Treasury Department (All)
190-HQ-C1220639-USMS	U S Marshals Service
190-HQ-C1220639-WH	White House (All)
190-HQ-C1220639-FG	Any Foreign Government
190-HQ-C1220639-MISC	All Other Agencies

FOIPA Numbered Memo 41

Page 2

Foreign Intelligence Surveillance Court (FISC)

(DOJ). The certification is classified by the FBI Director or other certifying official and both the primary and secondary orders receive derivative classification by the FISC clerk of court based on the application.

Since the minimization procedures originate from DOJ and are classified by OIPR, that portion must be referred to OIPR for a decision regarding access under the FOIA. [redacted]

b7E

[redacted]

[redacted] Established procedures should then be followed as outlined in the memorandum pertaining to Exclusions.

Prior to processing FISC records or notifying the requester that FISC records were referred to DOJ for review, the PLS is to consult with the National Security Division (Room 1B045, Ext. 2235) as well as DOJ, OIPR.

FOIPA Numbered Memo 43

Page 2

FD-340 Summary Bank Robbery Reports

Many banks utilize what is known as Adye packs.® This exploding device, when detonated, releases a red dye on its surroundings. The denomination and serial numbers of the money in the dye pack are recorded by the bank in the same manner as bait money. The denomination and serial numbers should be redacted using the same criteria applied to the bait money mentioned above.

Exemption (b)(7)(E) should be cited for any mention or details of the construction of the dye pack and Exemption (b)(4) for the specific chemical makeup of the dye.

FOIPA

MANUAL

MEMO 45

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: FD-761 Public Corruption Data Transmittal Form
Date: March 31, 1998

Form FD-761 was previously utilized for statistical purposes by the Public Corruption Unit, Criminal Investigative Division. However, the use of this form was terminated in 1995. Since the form is no longer in use, it would be difficult to articulate harm or risk of circumvention of the law. Therefore, none of the information contained on this form is exempt pursuant to (b)(7)(E).

In certain instances, the code asserted for the subject (public official) in item number 6 of the form may warrant protection pursuant to (b)(7)(C).

FOIPA

MANUAL

MEMO 47

To: All FBI FOIPA Personnel

~~Secret~~

From: J. Kevin O'Brien

b1
b3

(S) Subject: [redacted] Liaison with

Date: May 15, 1998

[redacted] (S)

b1
b3

and the [redacted] (S)

(S) Information provided by [redacted]

[redacted] is to be classified in FBI investigative files as National Security information. Likewise, the mere relationship and/or contact between the FBI and these foreign agencies should also be classified. (S)

All information concerning the above foreign law enforcement agencies is to be classified ASecret@ in accordance with Executive Order 12958, Sections 1.5/1.6 (b)(5) and (b)(6) and Section 3.4(6). (U)

FOIPA Numbered Memo 48

Page 2

High Visibility Electronic Communications (ECs)

B) the FOIPA release may result in the accusation of improper FBI activities.

C) whenever the requester has the ability and intent to disseminate information to the public (typically requesters associated with the media, authors or journalists) and the subject matter:

1. Is or was a person in the public eye, e.g., public officials, entertainers, sports figures, persons prominently associated with a course or movement, etc.
2. Is controversial, derogatory, or shows improper activity on the part of the subject not previously known.
3. Relates to FBI internal administrative matters, e.g., use of representation funds, of Professional Responsibility summaries, shooting incident reports, schedules or telephone logs of high Bureau officials, or disclose the individual activities of the Director or other Bureau officials.
4. Has received recent publicity.
5. The request involves a deceased Congressman or other significant political figure. (It is OPCA=s policy to contact the next of kin, advising of the release and providing a copy of the release. Therefore, one week prior to the release to the requester, a copy of the release package should be forwarded to [redacted] OPCA, Room 7240, for delivery to the next of kin.)

If the need for the high visibility is questionable, contact [redacted] Congressional Affairs Office, telephone 324-2454 for requests involving political figures. If the requester has the ability and intent to disseminate information to the public (member of the news media, a journalist or an author), contact [redacted] National Press Office, telephone 324-8787. The National Press Office has also advised that inquiries should be made to [redacted] Unit Chief, Fugitive Publicity and Internet Media Services Unit, telephone 324-9850 to see if the requester has made previous requests that have resulted in publicity.

There may be situations when the EC will need to be directed to both [redacted] [redacted] and [redacted] i.e., an author is requesting information concerning a deceased Supreme Court Justice.

b6

b6

b6

FOIPA Numbered Memo 48

Page 3

High Visibility Electronic Communications (ECs)

Information to include in the EC:

The EC should be limited to one or two pages and include the following:

- 1) The identity of the requester.
- 2) The subject of the request.
- 3) The date of the request.
- 4) The number of pages to be released.
- 5) A brief summary of the material processed and the type of classification, i.e., Bank Robbery, Special Inquiry, etc. (Do not include the actual file number or caption of the investigation.)
- 6) A statement on whether or not derogatory information was found in material processed and, if so, a brief description of the derogatory information.
- 7) A characterization of the exemption(s) asserted, e.g., Unwarranted invasion of personal privacy instead of A(b)(7)(C).
- 8) Language indicating that the release will be made once the EC is returned to the FOIPA Section.
- 9) The copy count should include [] and/or [] (the Public Information Officer), the name of the Unit Chief and the Team Captain, followed by the appropriate room number. Mr. Collingwood's name appears in the attention line following the "To" field, and the name of the PLS will appear in the "Drafted by" field. Therefore, their names should not be added to the copy count

b6

Approval Process for the EC:

A rough draft of the EC is to be submitted to the PLS's Team Captain for approval. Once the TC has approved the draft, the EC should be submitted to the Unit Chief and the FOIPA Section Chief in final form for initialing. The Section Chief will thereafter deliver the EC to the OPCA Front Office. Once Mr. Collingwood has signed off on the EC, it should be returned to the Unit Secretary for uploading and copying. Using a red pencil, place a check mark on each copy to indicate that copy's designation.

FOIPA Numbered Memo 49

Page 2

Historical Processing of FBI Documents under the FOIA

The privacy rules for third parties mentioned in any high profile investigation being processed under historical guidelines will be determined on a case-by-case basis. The age of the document/information being processed will be a critical factor in this decision as well as if the investigation received wide publicity. The decision to release names and information pertaining to third parties mentioned in the file should be discussed between the PLS and the Team Captain and must have the approval of the Section Chief.

FOIPA

MANUAL

MEMO 51

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: House Select Committee on Assassinations
Date: March 31, 1998

House Select Committee on Assassinations (HQ File 62-117290)

The FBI was previously in litigation with requester, Mark Allen, for all material provided to the House Select Committee on Assassinations (HSCA) concerning its investigation into the assassination of President Kennedy. The House of Representatives joined the litigation in an attempt to claim Congressional privilege for all of the material connected to the HSCA investigation. This included all correspondence between the FBI and HSCA, as well as internal FBI communications. The HSCA's position was that these materials, as well as materials concerning its investigation of the assassination of Martin Luther King, are congressional documents and not agency records. (It is noted that the HSCA investigation of the assassination of Martin Luther King was not in litigation.)

Questions concerning any material contained in **Bufile 62-117290**, or duplicate documents which may be unrecorded in other Bureau files, should be directed to [redacted] prior to any disclosure of material. [redacted]

b6

Processing of Material Pertaining to La Costa Nostra Figures

In connection with the investigation of the HSCA, and the request of Mark Allen for information provided to the HSCA, voluminous material was released pertaining to La Costa Nostra (LCN) figures.

Employees who are processing a file containing information concerning any LCN figure should contact [redacted] to determine if and/or obtain any material which may be in the public realm.

b6

A Message Key is a two-or three-character designator which identifies the type of entry or query sent. Although there are over 75 keys in present use, they will typically begin with the alpha characters "C" (Clear or Cancel), "E" (Enter), "M" (Modify), "O" (query), "X" (Clear), or "Z11" (Test). All letters in a Message Key are capital letters, and they generally appear at the beginning of a message. They often follow the entry code "MKE/", although they also appear in other places, such as in a header line, separated from the ORI by a period. (Note: the MKE/ code may also be followed by a narrative description of a message key for responses from system records.)

An ORI is a nine-character entry which identifies the agency entering the message, or another agency related to a previous NCIC message or event. ORIs begin with a two-letter state code, but may end in either a numeric or alphabetic character. They may or may not follow the entry code "ORI". They commonly appear in three places:

- 1) the beginning of a record, representing the agency requesting a record;
- 2) in the body of a record, representing the agency which entered the record; and
- 3) in an III record, following identification of an arrest event, representing the arresting agency.

Due to variances in state and federal system formats, the positions of message keys and ORIs may vary from record to record. In addition, anticipated changes in the NCIC system may create similar codes (An example is the proposed "CTI" identifier for courts issuing warrants.) The examples provided below are typical of how the codes may appear as discussed above:

1.) 2L0102077MJM .QH.DCFBIWA36.NAM [REDACTED]

b6

2.) 7L0102077MJM
DCFBIWA36
THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR
INQUIRY ON NAM [REDACTED] SEX/M RAC/W DOB [REDACTED]

NAME	FBI NO.	INQUIRY DATE
[REDACTED]	[REDACTED]	10/25/90

FINGERPRINT CLASS
PO PI CO PO PM
PI PM 10 PI 13

ALIAS NAMES
[REDACTED]

IDENTIFICATION DATA UPDATED 10/16/90

THE CRIMINAL HISTORY RECORD IS MAINTAINED AND AVAILABLE FROM THE

FOIPA Numbered Memo 52

Page 3

Identification Records (Rap Sheets), NCIC and III Printouts

FOLLOWING:

b6

FBI -FBI

THE RECORD(S) CAN BE OBTAINED THROUGH THE INTERSTATE IDENTIFICATION INDEX
BY USING THE APPROPRIATE NCIC TRANSACTION.
END

| 3) QW.DCFBIWA36.NAM/BADGUY,JOHN T.DOB/010101

| DCFBIWA36
NO NCIC WANT DOB/010101 NAM/BADGUY,JOHN T

Informant Files, Requests for

converted to an operational informant. If the case is closed because the individual is not suitable for an informant, all information volunteered by the individual regarding his background and substantive matters may be retained by the field office, however, current procedures require the field office to destroy all other information regarding the individual which was obtained without his consent. [MIOG Section 137-3.1.3(2)] If the individual is certified as an operational informant, the field agent gives the informant a number of admonishments regarding his status and activities, which usually clearly indicates that the FBI considers the individual an informant. Confidential Sources are given only a few admonishments which may not clearly indicate their status.

Only a small portion of the considerable paperwork which is generated in the field will be included in the FBIHQ informant file. In general, the FBIHQ file will contain only records of an administrative nature: the opening communication, the communication which converts the individual's status to that of a certified operational informant, requests from the field for funds to operate the informant, and communications concerning problems with the informant such as unauthorized criminal activity. The field office file, on the other hand, contains not only the administrative information, but also detailed substantive information received from the informant pertaining to crimes. This substantive information, generally contained in an FD-306 or FD-209, may be summarized in a communication to FBIHQ requesting funds to pay the informant, so at least some substantive information will be found in the FBIHQ file.

In order to avoid security problems inherent in the transmittal of informant files between offices, an informant file is generally processed for FOIA purposes by the office where it is located: field office files are processed by the field and FBIHQ files are processed by FBIHQ. This procedure can be changed only in exceptional cases and with the approval of the Section Chief. The classifications which should be processed as informant type files are: 134, 137, 170 (obsolete) and 270. The PLS should be alert for any informant information in the main investigative file which is also contained and being protected in the main informant file.

Processing Guidelines for Informant Files

Given the background circumstances, the processing guidelines which follow are meant to accomplish the following ends: 1) to protect the safety of informants who have submitted FOIPA requests under duress or who do not appreciate the dangers inherent in their requests; 2) to protect the viability of the informant program; 3) to protect the privacy of third parties named in informant files; 4) to protect ongoing investigations; 5) to protect the techniques involved in developing, operating, and evaluating informants; and 6) to avoid alienating confidential sources. The guidelines are not rules which must be followed even when the facts of an exceptional case require a different approach: they are some functional frameworks in which

FOIPA Numbered Memo 54

Page 3

Informant Files, Requests for

most informant file requests can be handled with the aforementioned goals in mind. Unusual cases should be referred to a FOIPA Section Supervisor and/or the substantive Division for advice.

II. First Party Requests:

A) Requester=s Incarcerated:

If the requester is incarcerated and has not specifically requested his informant file, [redacted]

b7E

[redacted] if the requester specifically mentioned his informant file in the request letter, the procedures in paragraph (C) should be followed after discussion with the Team Captain and/or Unit Chief.

B) Requester is Not Aware of "Informant" Status:

If the requester is not incarcerated and is unaware of his status as an informant or of the existence of his informant file, [redacted]

b7E

[redacted] In essence, the requester should be treated as a Cooperative Witness: the information he furnished should be processed using the pertinent exemptions [i.e., exemptions (b)(2), (b)(7)(A), (b)(7)(C), and (b)(7)(E)] except for exemption (b)(7)(D). Determining that a requester is unaware of his status as an informant is a matter of judgment. Some factors which may lead to such a conclusion are the following: 1) the requester was never certified as an operational informant; 2) the requester never furnished any information of value; 3) the requester was never paid, or never signed anything as an informant; 4) the informant file contains only a few serials; and 5) the requester=s letter does not specifically indicate a desire for his informant status, his informant file or the confidential information he provided to the FBI.

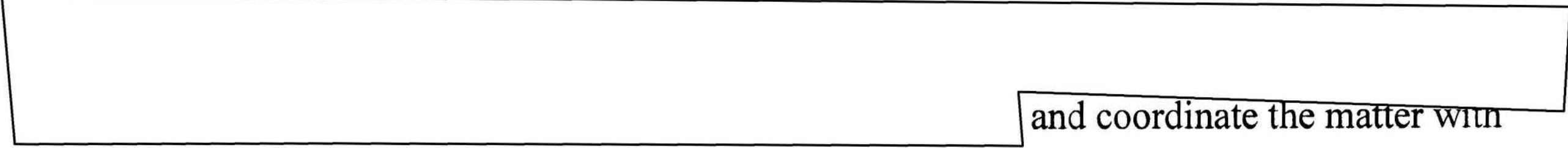
C) Requester is Aware of AInformant@ Status:

If the requester is not incarcerated and is aware of his status as an informant or the existence of his informant file, the field office which operated the informant should be notified of the request/ [redacted]

b7E

FOIPA Numbered Memo 54
Page 4
Informant Files, Requests for

The outgoing FOIPA Section's electronic communication to the field should advise the



b7E

and coordinate the matter with
the Informant Unit.

D) Informant Status Officially Confirmed:

If the requester is not incarcerated, is aware of his informant status/file, and he advises the request was submitted voluntarily, then a determination must be made as to whether the requester's informant status has been officially confirmed such as through testimony in open court or an official media release. When there has been no such official confirmation, the full range of applicable exemptions, to include exemption (b)(7)(D), can be used to avoid confirming the informant's status by the release. When there has been official confirmation through testimony or an official media release, the information which was publicly disclosed and which can be identified as such in FBI records is subject to release; the remaining information should be processed using the full range of relevant exemptions.

III. Third Party Requests:

If information about or from an informant is requested by a third party, the Case Agent handling the informant should be advised at once.

After first considering the (c)(2) exclusion, all of the potentially applicable FOIA exemptions should be considered. If an informant has been officially disclosed, only information concerning his identity as an informant and information about others which has been previously disclosed will be provided to the requester.

IV. The Exemptions:

In addition to the manner in which the FOIA exemptions are normally used, the following applications should be considered for informant files:

Exemption (b)(2) may be used to protect informant symbol numbers, informant code names, and the designation "informant" or its equivalent in a file. This exemption would be most useful in those situations where the requester was not yet aware that he was being considered to become an informant or when his informant status has not been officially confirmed.

Exemption (b)(7)(A) may be used if disclosure would reveal the direction of, or otherwise interfere with, a pending investigation. This may occur, for instance, when a report of an

FOIPA Numbered Memo 54

Page 5

Informant Files, Requests for

informant interview includes only some of the information furnished by the informant. The selective inclusion of information in the report may reveal the focus or direction of an investigation. Since even a thorough review of a file may not indicate whether disclosure could reasonably be expected to interfere with an investigation, it is recommended that the PLS discuss the matter with the case agent for the informant or investigation in question.

Exemption (b)(7)(C) may be used to protect the privacy rights of third parties mentioned in an informant file. Although one factor weighing in favor of disclosure is the public interest in ensuring that information is recorded properly in government files, the other side of the balance, at least where the informant receives some form of consideration or payment for the information, will include the notion that the proprietary right to that information has passed from the informant to the government. That factor, when combined with the traditional privacy concerns inherent in such information, will usually outweigh the factors favoring disclosure, especially in light of the Supreme Court decision in Reporters Committee for Freedom of the Press v. Department of Justice.

As mentioned in Section II part D of this memo, the first clause of exemption (b)(7)(D) should be used when the requester's informant status has not been officially confirmed. Thus, we would withhold any information which could reasonably be expected to disclose that the requester had been an informant. When the requester's informant status has been officially confirmed, exemption (b)(7)(D) can be used to withhold any information which could reasonably be expected to disclose that the requester had been an informant on matters which were not disclosed in the "official confirmation." Exemption (b)(7)(D) would also apply to information which had been provided by others on a confidential basis such as information provided by a local police department concerning the informant's criminal activities. It should be noted, however, that much of the substantive information provided by the requester will be withheld under exemption (b)(7)(C).

Exemption (b)(7)(E) may be used to protect FBI techniques involved in developing, operating, and evaluating informants which are not well known to the public.

Exemption (b)(7)(F) may be used to protect the physical safety of any individual, including the informant/requester.

In a particularly sensitive case, additional measures could be considered. Such action should only be taken after careful consideration and only with the approval of the Unit Chief and/or Section Chief personnel.

b7E

Finally, the Criminal Informant (Ext. 3144, Room 4944)/Witness Security Programs Unit (Ext. 5754, Room 4944) should be consulted prior to disclosing any information concerning an informant.

FOIPA

MANUAL

MEMO 55

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Infrastructure Vulnerability/Key Asset Protection Program
Date: March 31, 1998

The Infrastructure Vulnerability/Key Asset Protection Program is an extremely vital and sensitive program the existence of which is protectable under Exemptions (b)(1) and (b)(7)(E). The program is further characterized in the following excerpt from a R. M. Bryant Memorandum to Mr. Baugh dated 3/28/94:

As the lead agency for counterterrorism within the U.S., the FBI has developed and implemented an Infrastructure Vulnerability/Key Asset Protection Program to reduce the threat of terrorist violence [redacted] The objective of this proactive FBI project (as defined by Executive Order 12656, signed by former President Reagan on 11/18/88) is to identify key assets, develop liaison, and assist in contingency planning where necessary, and by doing so, to facilitate the protection of the U.S. infrastructure. @

b7E

Our infrastructure is defined as a system of interdependent networks [redacted]

b7E

It is important to note that although individual assets can be advised of their designation, the comprehensive list cannot be disseminated in its entirety outside the FBI. This restriction is based on the security classification [redacted]

b7E

FOIPA Numbered Memo 55

Page 2

Infrastructure Vulnerability/Key Asset Protection Program

b7E

[Redacted] were to be released or find its way into the public domain, it would serve as a blueprint of our nations most vital facilities to terrorists throughout the world. @

Alf you have any further questions, do not hesitate to contact the Counterterrorism Section, Counterterrorism Planning Unit, National Security Division, at extension 4656. @

FOIPA Numbered Memo 56

Page 2

Institutional Sources

4. Institutions providing assessments about the character or work of employees, if the information concerns a criminal suspect or is derogatory.

In other circumstances, involving less sensitive types of information, a theory of implied confidentiality will be more difficult to justify in the absence of some indication that the source treated the information as confidential. Examples of such information include the following:

1. Information concerning vehicle registration or ownership from motor vehicle departments.
2. Information about the fact that utility services were provided at particular locations and dates.
3. Routine information from state or local prison officials, such as release dates, etc.
4. Routine information provided by employers about starting and ending dates of employment, salaries, etc.
5. Contacts in which no information was provided or, on the other hand, where innocuous/unimportant information was provided.
6. Routine law enforcement record checks or credit checks.

In all of the above examples, it should be kept in mind that the identities of persons contacted at such organizations and supplying the information to the FBI should be protected under Exemption (b)(7)(C), unless such persons are known to be deceased. In the same respect, should the information itself pertain to a third party individual, the name(s) and any identifiers concerning the individual(s) should likewise be protected pursuant to Exemption (b)(7)(C).

In applying the standards of the Landano ruling, it should be kept in mind that this only affects the application of implied confidentiality. Wherein a confidential relationship does exist by virtue of an "expressed" or "specific" request of confidentiality, exemption (b)(7)(D) will be applied to protect the identity of the source, as well as, the information provided by the source.

However, if the information would not tend to identify the source, it may be released as addressed in Attorney General Janet Reno's policy of discretionary disclosure of October 1993.

The following institutional sources have requested confidentiality as indicated:

- 1.) [redacted] **Information** [redacted] file
[redacted] requires a subpoena duces tecum before substantive [redacted]

FOIPA Numbered Memo 56

Page 3

Institutional Sources

information is released if an investigation is not related to a violation against [redacted] In addition, [redacted] policy requires that the customer whose records are being sought must be advised of the issuance of the subpoena unless the subpoena directs [redacted] to refrain from notifying the customer.

b7D

Therefore, information from [redacted] should be considered as having been furnished under a promise of confidentiality if the document containing the [redacted] information does not mention whether [redacted] notified its customer. Assume it did not and protect the information under exemption (b)(7)(D) pursuant to an Aexpress@ grant of confidentiality. However, if [redacted] advises the customer that it has furnished information to the FBI, [redacted] should be considered to have waived its confidentiality rights and the information may be released in first party requests. Privacy issues may be warranted and the appropriate exemptions asserted when the information pertains to third party individuals.

b7D

2.) Dunn and Bradstreet Records Checks

Dunn and Bradstreet=s liaison for Federal Customers has requested confidentiality in criminal and civil matters for future and past information. Exemption (b)(7)(D) should be asserted to protect Dunn and Bradstreet and the information provided.

FOIPA

MANUAL

MEMO

57

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Interesting Case (I.C.) Memoranda Located In FBI Files
Date: March 31, 1998

Interesting Case (I.C.) Memoranda Located in Bureau Files

I.C.s were originally created by the public relations staff for the media and the public. These narratives consist of approximately 2-12 pages, span the years 1932-1972 and can be identified by the letters A.I.C. file No. ...@ located at the top left corner of the document. As all I.C.s have been publicly disclosed, they can be released in their entirety without redactions.

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Internal Revenue Service (IRS)
Date: March 31, 1998

Social Security Account Numbers

When referring documents or information to the IRS, it has been requested that, when known, the Social Security Account Number (SSAN) of the FOIPA requester also be furnished. Generally, the SSAN is provided on the initial FOIPA request letter of first party requesters, however, extensive file reviews should not be conducted to ascertain the number. The SSAN assists IRS in locating the original copies of the records referred by the FBI.

Investigations Conducted by the FBI

status of the case. These same procedures should be used in FCI organizational files. In certain instances it might also be appropriate to follow these procedures in closed organization files where a relationship might exist between the organization which was the subject of the closed case and another organization presently under investigation.

Investigations in Foreign Countries

The presence of an FBI Legat in a foreign country is at the pleasure of the host government. Any disclosure indicating that an investigation was conducted in a foreign country, by or on behalf of the FBI, may jeopardize the continued operation of our Legat in that country.

In processing FBI files, the PLS will ordinarily find documents reporting information from foreign agencies or authorities, however, the PLS may encounter documents which report FBI investigative activities in foreign countries. The latter type information is often classified and in such situations, Exemption (b)(1) should be cited to protect the information. Therefore, disclosure PLSs should be certain that information of this type is reviewed by the Document Classification Unit, keeping in mind this situation may also exist in non-security investigations. If the information does not warrant classification, the PLS should consult the Foreign Government Information Classification Guide (G-1)¹ to determine whether or not the foreign agency requests its information be protected and whether or not the foreign agency wants its relationship with the FBI made public. Some foreign agencies or authorities request that their information be protected; however, they do not object to their relationship with the FBI being made public. In those situations, the PLS would protect the foreign agency information pursuant to Exemption (b)(7)(D), but would release the identity of the foreign agency. Other foreign agencies request that both the information and their identity remain protected, and thus, all information would be redacted pursuant to (b)(7)(D).

Documents which often report foreign agency or authority information usually originate from an FBI Legat. It is important to note that even the AFrom@ line in a Legat-authored communication can be sensitive information because it specifically identifies the host country and when combined with the details of the communication, reveals the fact that the host country has furnished information to the FBI. Situations do arise wherein the AFrom@ line of a Legat communication is properly classified ASecret,@ which is possible even in criminal cases. If the document has been classified ASecret@ in its entirety that classification covers the AFrom@ line. If the document is not classified in its entirety the AFrom@ line is not classified unless there is a

¹The G-1 Guide provides instructions on the classification of national security information pertaining to foreign government information.

FOIPA Numbered Memo 60

Page 3

Investigations Conducted by the FBI

classification marking opposite that line. In all cases where the document is not classified in its entirety and there is no classification marking by the AFrom@ line, the same procedures should be followed as above in utilizing the G-1 guide. If there are any questions concerning the classification of the AFrom@ line, the PLS should contact the DCU PLS who reviewed the document for classification even if the case is of a criminal nature.

If the PLS has any questions concerning the application of exemptions to Legat/foreign government information and/or the Legat=s activities in a foreign country, the matter should be discussed with the Team Captain and/or Unit Chief. If a disclosure is still contemplated after that point, the matter should be discussed with personnel from the International Relations Unit.

Multiple Subject Investigations

If the Team Captain and/or PLS determines that the requester is carried in a multiple subject investigation, it may be appropriate to check the other names with RTSS to determine if the file has been previously processed for another requester. It is recognized that privacy interests will dictate how much information will be provided other requesters; however, the possible use of Exemptions (b)(6) and/or (b)(7)(C) may depend on whether the information was withheld or disclosed in a prior release.

Since these multiple subject cases vary in their makeup, a hard and fast rule that other subjects= names should be checked for prior processing in every instance is not necessary. However, the advantages of uniformity in processing and the time saving factors should be carefully considered, resolving any doubts in favor of checking the indices.

FOIPA

MANUAL

MEMO 61

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Iran-Contra / Front Door Material
Date: March 31, 1998

Iran-Contra Investigation; Front Door Files

FRONT DOOR is the code word for the investigation conducted by the Office of Independent Counsel (OIC) relating to the Iran-Contra. **Information pertaining to the Iran-Contra is filed in FBIHQ files 58-11887 and HQ 211-26.**

If either of the above file numbers appear on a search slip, **DO NOT call the files and DO NOT PROCESS the files.** The Special File Room (SFR) controlled access to HQ 58-11887, but the SFR has released HQ 211-26 for review. If you should receive either of the above files, contact PLS immediately.

b6

The Office of the Independent Counsel on Iran-Contra has been disbanded and all of their material has been transferred to National Archives pursuant to Title 28, U.S.C., Section 594(k). Material indexed into 58-11887 or 211-26 will no longer be reviewed or processed by FBI PLSs and, where appropriate, the following paragraphs should be used for response to requesters:

A.) First Party Request Which Results in Cross-references

AA search of the indices to our Central Records System files at FBI Headquarters revealed material that **may or may not** be identical to you in files concerning the sale of arms to Iran and the possible diversion of proceeds from those sales to Nicaraguan AContras. This material is located at the Office of National Archives. If you have further interest in AIran-Contra related material, you may wish to correspond directly with the Office of National Archives.

B.) Request for the Entire Investigation

ARefrence is made to your request for material relating to the AIran-Contra investigation which concerns the sale of arms to Iran and the possible diversion of proceeds from those sales to Nicaraguan AContras. This material is located at the Office of National Archives. If you have further interest in AIran-Contra related material, you may wish to

FOIPA Numbered Memo 43

Page 2

Iran-Contra / Front Door Material

correspond directly with the National Archives. @

FOIPA

MANUAL

MEMO 63

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Legal Attache
Date: March 31, 1998

Search Procedures for Legal Attache (Legat) Files

When a request is made for a search to be conducted of the Legat files, the LT or PLS should complete and submit a search slip to the Special File Room, Room [] to the attention of []. Indicate on the search slip that the scope of the search is for the "Automated" Data Base only, unless the FOIPA request letter specifically asks for the "Manual" indices to be searched or if the information being requested would in itself only be found in the manual index.

Also, indicate that the type of search requested is "Legat Indices," specifying which Legat is to be searched (See sample attached). If an initial FOIPA request is received in RMU for a specific Legat, the search should be completed and the copies of the file(s) obtained prior to assignment of the request to a Disclosure Unit.

b6
b7E

Storage of and Obtaining Legat Files

On May 23, 1984, the Legat Micrographics Program was initiated to enhance security because of the potential hazardous environment of an overseas post and to relieve overcrowded file storage conditions in the Legats.

When an investigation has been closed in the Legat for 90 days, the raw file is sent to FBIHQ to be stored or placed on microfiche. A copy of the microfiche is furnished to the Legat and a copy is maintained at FBIHQ in the Micrographics Unit, Room 1B301, extension 3413. The 1A and Bulky Exhibits are not microfiched, only the covers to this material. If copies of the 1A or Bulky enclosures are needed, they can be retrieved from either Pickett Street or Boyers, Pennsylvania. If a copy of the file will suffice, the Microfiche can be duplicated and sent to the LT or PLS. If the raw material is needed, it will be retrieved by the Micrographics Unit and forwarded to the LT or PLS.

Legat ELSUR Requests

If a request has been made for a search of a specific Legat=s ELSUR indices, the requester should be advised there are no ELSUR indices in the Legats. The FBI has no authority to conduct ELSUR in foreign countries, therefore an ELSUR indices is not maintained.

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Mail Covers
Date: March 31, 1998

Mail covers are placed with the Postal Service and entail the Postal Service watching for and recording the addressee and addresser of all mail written to a particular individual or organization. The existence of a mail cover is not generally protected under Exemption (b)(7)(E); however, National Security mail covers are often classified and governed by Exemption (b)(1) law.

At times, unique circumstances may exist where information pertaining to a mail cover may need to be protected, such as when the mechanics/details of the mail cover (which are not generally known to the public) are set forth in an FBI record. Should it surface, the PLS may be able to protect those aspects of the mail cover under Exemption (b)(7)(E). In other instances in which mail covers were utilized, the assertion of Exemption (b)(7)(E) should be considered for cases recently closed by administrative means and did not reach a prosecutive status. If the case has the possibility of being reopened or a Aspin-off@ case was involved, the release of the fact a mail cover was utilized could be a detriment to the reopening of the investigation or any related pending investigations. Contact with the field office Case Agent is recommended in these situations in order to determine if there is a "foreseeable harm" in disclosure of the information.

FOIPA

MANUAL

MEMO 65

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Manuals, FBI
Date: March 31, 1998

The following FBI manuals have been processed and are available for release:

- X Manual of Administrative Operations and Procedures (MAOP)
- X Manual of Investigative Operations and Guidelines (MIOG)
- X Foreign Counterintelligence Manual (FCIM)
- X National Crime Information Center (NCIC) Manual
- X Legal Handbook for Special Agents

Inasmuch as these manuals are available for review in the FOIPA Reading Room and they undergo periodic changes, information being considered for release should be coordinated with Team Captain or PLS Unit 3, prior to any disclosure.

b6

FOIPA Numbered Memo 66

Page 2

National Center for the Analysis of Violent Crime

252-2345).

Since April 1992, all opened and closed HQ 252 classifications have been manually maintained at Quantico as a part of the NCAVC record system (JUSTICE/FBI 015). The HQ 252 files generated prior to 1992 are maintained at Picket Street or Quantico. You should also be aware that NCAVC/VICAP manually maintains their equivalent 252 file classification and other file classifications concerning violent crimes investigated by the FBI (such as kidnaping, extortion or crime on government reservation) at Quantico.

The NCAVC is maintaining a control file, 190-IR-C-2246, for FOIPA requests involving 252 files and the other classifications, as described above. If an FOIPA search reveals that a 252 file or other classifications exists, the LT or PLS should:

1. Contact the Rotor Clerk for the NCAVC at 115-1690 or 540-720-4906 or 4926, in order to obtain the file(s) for duplication and processing.
2. EC or FAX a copy of the FOIPA request letter to the attention of the NCAVC/VICAP Unit Chief at (540)-720-4956 and the CIRG, Chief Division Counsel at (703)-640-1162.
3. Provide NCAVC with the requester's 190 file number and the FOIPA computer number.

Data concerning violent crimes is also stored in an automated data base maintained by the NCAVC in a separate FBI record system which is part of the NCAVC (JUSTICE/FBI-015). This data base contains information which is used in the overall VICAP Program. NCAVC/VICAP analyses the information in this data base to identify any common threads which might run through the various cases.

Components of the NCAVC/VICAP data base should not be searched unless the requester specifically asks that it be searched or includes information in his request letter which indicates it should be searched.

The information in the NCAVC/VICAP data base and the 252 VICAP files is exempt from access under the Privacy Act pursuant to exemption (j)(2). When processed under the Freedom of Information Act, the appropriate Exemption 7 provisions should be utilized in addition to any other applicable FOIA exemptions. In addition, contact and coordination should be made with NCAVC/VICAP when processing these cases.

Because of the sensitive nature of the techniques used by all NCAVC components in their development of unknown offender profiles, investigative recommendations, interviews and

FOIPA Numbered Memo 66

Page 3

National Center for the Analysis of Violent Crime

interrogation techniques, prosecutive and trial strategies, threat assessments, overall crime analysis, search warrant affidavits and expert testimony, the NCAVC should be consulted. Upon completion of the processing of the 252 file or other classification, the PLS should:

1. Provide NCAVC with a black-out copy of the proposed release for their review prior to disclosing any material to the requester.
2. Provide NCAVC with a copy of the final disclosure or denial letter. If the case is being closed administratively, notify NCAVC of this action and the reason for closing the case.

If the FBI receives an administrative appeal concerning the material from a 252 file and the DOJ/OIP attorney affirms the appeal, there is no need to advise NCAVC. If, however, the DOJ attorney suggests an amended release, consult with the NCAVC before agreeing to the release of additional material. Then provide NCAVC with copies of:

1. The requester=s appeal letter.
2. The DOJ acknowledgment letter.
3. The DOJ letter advising requester of a remand or an amended release.
4. The FBI letter releasing the additional material.

If the FBI receives an appeal concerning one of the other file classifications, as described above, containing NCAVC material and the DOJ attorney affirms the appeal or the DOJ attorney recommends release of material that does not include the NCAVC material, there is no need to advise NCAVC of the appeal. However, if the DOJ attorney recommends the release of information of interest to NCAVC, consult with NCAVC before agreeing to the release of the additional material. Provide NCAVC with copies of items 1 through 4 above.

Be aware that much of the work done by NCAVC is for other federal (non-FBI), local and state law enforcement agencies, and there will be times when the FBI file is closed and the other federal, state or local investigation is still pending. The (b)(7)(A) exemption of the FOIA should be considered.

When processing a VICAP report, the PLS will release the cover page. For the report itself, the PLS will need to review the report to determine the origin of the information in the report. If the material in the report was furnished by a state or local law enforcement agency, the PLS will deny the report in its entirety citing Exemption (b)(7)(D) and if applicable Exemption

FOIPA Numbered Memo 66

Page 4

National Center for the Analysis of Violent Crime

(b)(7)(C). If the material in the report was furnished by a federal (non-FBI) law enforcement agency, the PLS will consult with the contributing agency.

FOIPA Numbered Memo 67

Page 2

National Crime Information Center (NCIC)

state code, but may end in either a numeric or alphabetic character. They may or may not follow the entry code "ORI". They commonly appear in three places:

- 1) the beginning of a record, representing the agency requesting a record;
- 2) in the body of a record, representing the agency which entered the record; and
- 3) in an III record, following identification of an arrest event, representing the arresting agency.

Due to variances in state and federal system formats, the positions of message keys and ORIs may vary from record to record. In addition, anticipated changes in the NCIC system may create similar codes. (An example is the proposed "CTI" identifier for courts issuing warrants.) The examples provided below are typical of how the codes may appear as discussed above:

1.) 2L0102077MJM .QH.DCFBIWA36.NAM [REDACTED] b6

2.) 7L0102077MJM
DCFBIWA36
THIS NCIC INTERSTATE IDENTIFICATION INDEX RESPONSE IS THE RESULT OF YOUR
INQUIRY ON NAM [REDACTED] SEX/M RAC/W DOB [REDACTED] b6

NAME	FBI NO.	INQUIRY DATE
[REDACTED]	[REDACTED]	10/25/90

SEX	RACE	BIRTHDATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTHPLACE
M	W	[REDACTED]	185	BRO	BRO	[REDACTED]	

FINGERPRINT CLASS
PO PI CO PO PM
PI PM 10 PI 13

ALIAS NAMES
[REDACTED]

IDENTIFICATION DATA UPDATED 10/16/90

THE CRIMINAL HISTORY RECORD IS MAINTAINED AND AVAILABLE FROM THE FOLLOWING:

FBI -FBI [REDACTED]

THE RECORD(S) CAN BE OBTAINED THROUGH THE INTERSTATE IDENTIFICATION INDEX BY USING THE APPROPRIATE NCIC TRANSACTION.
END

FOIPA Numbered Memo 67

Page 3

National Crime Information Center (NCIC)

3). QW.DCFBIWA36.NAM/BADGUY,JOHN T.DOB/010101

DCFBIWA36

NO NCIC WANT DOB/010101 NAM/BADGUY,JOHN T

Stop Index in NCIC

The Bureau Stop Index Program was instituted in April, 1971. Essentially, it was a computerized file included in NCIC for intelligence purposes on individuals against whom warrants were not outstanding. NCIC queries by any NCIC user would result in a ANo NCIC Want@ response to that user, but would generate a special notice to the NCIC Control Room to notify the appropriate Field Office of the inquiry. The Program was discontinued in February, 1974.

NCIC has determined there can be no entry into NCIC except for categories of individuals or records published in the Federal Register pursuant to the Privacy Act. Consequently, language in FBI documents, especially form FD-305, such as AStop Notice Placed with NCIC@ or AStop Notice Placed with the Bureau Stop Index@ is not protectable under (b)(7)(E).

Please take the foregoing into consideration when processing documents pertaining to NCIC Stop Notices.

FOIPA Numbered Memo 69

Page 2

Personnel Files

which warrant classification review noted on OPCA-18 form. The following are examples of information which may be found in personnel files and require DCU review: Special Agent, Radio Maintenance Technician, and Special Employee files which may contain references or notations in the annual performance rating to security informants or the specific nature of FCI investigations handled by the employee; a synopsis of an FCI investigative matter handled by an employee as justification for a letter of commendation; in-service memos detailing the nature of FCI training; or material in the background investigation of the employee which may have been obtained from foreign police agencies.

(5) Prepare an addendum to the FD-488 (Privacy Act Request Form) setting forth the following: the reason for any excisions; number of pages withheld in their entirety, if any; and a description of the last document/serial in the file as of the time of processing. Since a formal disclosure letter is normally not prepared in connection with these reviews/releases, it is recommended that the employee initial the addendum as evidence of his or her understanding of the deletions made.

(6) The proposed disclosure must be reviewed by a Team Captain.

(7) Contact the employee and make an appointment to review the file. If possible, provide an appropriate location where the review can be conducted other than the PLS=s work area. If the employee is not located at FBIHQ and is not in a position to review the material in the FOIPA Section, contact the Field Coordination Team to determine the appropriate procedure for the employee to review the file.

(8) Have the employee sign the lower portion of the FD-488 acknowledging the employee was given appeal rights and the right to obtain copies of reviewed material.

(9) Have copies made of any documents requested. A notation may be added to the addendum identifying documents requested by the employee.

Requests by FOIPA Section employees for access to their own personnel files will be assigned for processing by the Section=s Front Office.

In addition to the OPF, personnel/performance folders are maintained by the rating official on FBI employees. At the time the employee is provided with his or her performance rating, a request may be made by the employee for access to physically review this folder. Should the employee request copies of any material maintained in this folder, he or she should be advised that a FOIPA request must be submitted in order to obtain copies of the material.

There may be particular circumstances which preclude the release of certain performance related information or documentation to the employee. These circumstances may include

FOIPA Numbered Memo 69

Page 3

Personnel Files

information or documentation which is relevant to a pending complaint, charge or internal investigation.

B) FORMER EMPLOYEES

Former employees are generally treated as members of the public. They may not review their files in the FOIPA Section space or have access to classified information. When their files contain information which may require classification, the entire file should be sent to DCU for review.

FOIPA personnel should remain alert for information located in personnel records which may require classification. This includes, but is not limited to, such items as: references to the SSG (Special Support Group); language training for certain vice training classes; various Bureau codes and systems data; some security clearance forms; and information concerning the duties or responsibilities of Radio Maintenance Technicians.

C) MEDICAL RECORDS

Employee medical records may be located in the following places: 1) the employee's personnel file; 2) the employee's medical folder, which is part of the personnel file but is maintained separately from it; and 3) the employee's clinical file, which is located in the Health Services Unit.

Medical folders were first established for agents in 1986 and for support personnel in 1988. Prior to the establishment of those folders, all medical records were filed in the employee's personnel file. Since the records in a personnel file were not removed and placed in a newly opened medical folder, an employee's medical record can be located in all three places mentioned above. Existence of a medical folder will be indicated by the stamp "Medical Records Filed Separately" on the personnel file. Medical folders are requested by calling the Personnel Records Unit (Ext. 4857).

Clinical files, which were first established on 1/13/86, contain the original EOD physical examination report of a current employee hired after that date and various other records. After employment ends, the documents in the clinical file are placed in the medical folder. Clinical files should be requested by calling the Supervisory Occupational Health Nurse (SOHN). If records are obtained from the clinical file for processing, an FOIPA Section employee must annotate the FD-488 Privacy Act Request to show which records were retrieved and included in the processed package.

The Unit Chief of the Employee Assistance Program (EAP) has advised that if the release of medical records pursuant to a Privacy Act request may cause harm to the requester or another person, they would review the documents and respond to us as to whether or not the information

FOIPA Numbered Memo 69

Page 4

Personnel Files

may indeed cause harm. In those rare instances, when EAP indicates harm, we could cite (b)(7)(D) and/or (b)(7)(F) to protect the material. The documents are to be sent to EAP, Room 10190, telephone number 324-5244.

D) SENDING PROCESSED MATERIAL TO FILE

When a Privacy Act request involves processing of material from a 62 {Administrative Inquiry (AI)}, 67 or 263 file classification, the pages containing deletions should be forwarded to the Personnel Records Section for filing into the respective 62 (AI), 67 or 263 file along with the original FD-488 and/or OPCA-16 form (Disclosure letter). Please note those documents from the 67 Sub M and/or the Sub S which contain redactions are to be filed in the 67 Sub M and/or Sub S, along with a copy of the FD-488 or the OPCA-16 form, and not in the main 67 file. When processing a 280 file, the FOIPA correspondence and redouts are to be placed in a messenger envelope and sent to the Equal Employment Opportunity (EEO) Unit, Room 7901, telephone number 202-324-4128. If processing also involves additional file classifications, then a 190 file should be opened and the processed documents from the other file classifications should be filed in the 190 file along with a copy of the FD-488 and/or OPCA-16 form. The 190 file number should be recorded in the AMiscellaneous@ block on the computer sheet.

Personnel Type Records Maintained at the FBI Academy, Quantico, Virginia

Presently, there are two administrative units at the FBI Academy which maintain separate folders containing records identifiable with Special Agent (SA) personnel. The New Agents Unit maintains folders containing information compiled during New Agent=s training. The Personnel Assessment Unit maintains similar folders containing information on those SA Personnel who attend the Management Aptitude Program (MAP) training sessions at the Academy.

In order to bring these records within the FBI Central Records System, a memorandum is inserted in each employee=s personnel file at Headquarters at the time they go through either the New Agents or the MAP training program. This procedure was implemented in approximately November 1981.

As a result of discussion with the MAP Assessment Unit, FBI Academy, it was determined that much of the material maintained in the MAP folder is exempt from access pursuant to Exemption (k)(6) of the Privacy Act (PA) and (b)(2) of the Freedom of Information Act (FOIA), as disclosure would compromise the evaluation process.

In order to facilitate the processing of MAP materials, and to eliminate the need for the unnecessary transfer of documents from the FBI Academy to the FOIPA Section, all requests for

FOIPA Numbered Memo 69

Page 5

Personnel Files

MAP documents will be reviewed personally by the Unit Chief of the Personnel Assessment Unit. The Unit Chief will remove all MAP documents previously determined to be exempt from disclosure pursuant to Exemptions (k)(6) and (b)(2). Any remaining documents will be forwarded by routing slip to the FOIPA Section for processing, setting forth the number of pages withheld pursuant to Exemption (k)(6)/(b)(2).

In the event the request for MAP documents reaches the litigation stage, the Unit Chief of the Personnel Assessment Unit will provide justification for withholding exempt material.

Documents forwarded to the FOIPA Section for processing will include, but are not limited to, the cover page of the MAP report, biographical statements filled out by the MAP candidate, the assessor rating sheets, and the post MAP documents.

The MAP report, which the MAP candidate reviews and initials upon completion of the assessment or shortly thereafter, is exempt pursuant to Exemptions (k)(6)/(b)(2). If the FOIPA requester desires a second review of this MAP report, they should be advised to contact the Unit Chief of the Personnel Assessment Unit at Quantico.

CIA Name Checks in Suitability/Applicant Type Files

Forms used for CIA name checks in suitability applicant files do not have to be referred to CIA if the form indicates "No Record", "No information," or "No Trace." For further information concerning the handling of these forms if any other type of response was noted, see the FOIPA Numbered Memo 8 pertaining to CIA.

Credit Bureau Reports Contained in Personnel Files

PLSs will often encounter credit bureau reports in personnel files. These reports are often denoted as Aconfidential@; however, this designation does not mean the report is classified and per discussion with personnel of Credit Bureau Reports, Incorporated, it does not denote the manner in which the reports were furnished to the FBI. Therefore, it is the policy of the FBI's FOIPA Section to release these credit bureau reports to first party requesters as well as third party requesters with proper notarized authorization to receive such information.

Access to Career Board Minutes

In July 1989, a 67 control file was established to maintain all information pertaining to Career Board Minutes. This file contains agenda which outlines all of the positions considered on a listing, and each agenda item is addressed separately, setting forth the position considered, the person selected and why, and all persons whose qualifications were considered. **Due to the sensitivity and personal nature of the material, access to the Career Board Minutes is limited to PLS [] Unit 1.**

b6

When a request is made for Career Board Minutes pursuant to a FOIPA request, it will be assigned to PLS [] for processing of any or all Career Board tape recordings, accompanying minutes and/or agenda. Documents that are physically contained in a personnel file which pertain to Career Board activities or information will, in most instances, be processed by the PLS to whom the case is assigned. However, the PLS should contact PLS [] in order to verify that he does not need to process the documents.

b6

Informal Access Review of Personnel Files

(The request for an Informal Access review is not processed through or by the FOIPA Section or its employees. Employees have been designated from each field office and FBIHQ Division to handle these requests. This is a request only to review the personnel file and no copies of any documents are made available to the employee through the Informal Access procedures.)

In the Settlement Agreement reached in Emanuel Johnson, et. al. V. Stuart M. Gerson, Acting Attorney General, the FBI agreed to establish procedures whereby all FBI employees could access their personnel files without submitting a Privacy Act request.

With the exception of Legats, all offices including FBIHQ Divisions and offices, will be responsible for handling requests for informal access to personnel files from employees assigned to their offices. (Legats will forward requests from employees assigned to their offices to FBIHQ for handling.) Field offices will also be responsible for handling requests from employees assigned to Resident Agencies within that office=s territory.

FBIHQ employees may make an informal access request by executing a request form and submitting their request to the Assistant Director (AD) or office head of their assigned division. Field office employees may execute a request form and submit their request to the Special Agent in Charge (SAC) or the Assistant Director in Charge (ADIC). The request will then be forwarded to the designated employee handling these requests for processing.

FOIPA Numbered Memo 69

Page 7

Personnel Files

Fifteen and 45 day periods have been established as a time frame in which the employee's file will be available for review. This 15 and 45 day period will begin upon receipt of the employee's request by the SAC, ADIC, AD or office head.

Upon review of the file, an employee will be afforded an opportunity to submit to the respective SAC, ADIC, AD or office head a response or rebuttal to any information in their personnel file for inclusion in that file.

FOIPA Numbered Memo 70

Page 2

Photograph Albums, FBI

and Exclusions (c)(1) and (c)(3), should also be considered. The use of Exemption (b)(7)(E) should be considered to protect the criteria used to determine when a subject is of sufficient interest to be shown in a Photograph Album.

Processing under the Privacy Act

Information from Photograph Albums will generally be protected from disclosure under Exemptions (j)((2) or (k)(1).

Polygraph Examinations

- 4) **Polygraph Zone Comparison Numerical Analysis Data Sheet (FD-524)**
Polygraph Review Modified General Question Test Numerical Evaluation (FD-525)

The numerical ratings on these two forms (See Attachments 4 and 5) may be released entirely to first party requesters, however, the examiner=s name should be protected pursuant to exemption (b)(7)(C).

When encountering **polygraph examinations conducted on third party individuals** in FBI investigatory files, who are assumed or known to be living, they should be withheld entirely applying the above exemptions as indicated in addition to exemption (b)(7)(C).

NOTE: The same Polygraph information should be protected as outlined above when processing an applicant/background investigation or personnel type files. The appropriate Privacy Act and FOIA exemptions should be asserted for this information.

Any questions concerning polygraph material should be directed to the Polygraph Unit, Laboratory Division, after consultation with the Team Captain and/or the Unit Chief.

FOIPA

MANUAL

MEMO 73

To: All FBI FOIPA Personnel
From: John M. Kelso, Jr.
Subject: Psychological Services for FBI Employees
Date: May 14, 2001

Psychological Services Provided to the FBI

Doctors [] and []

b6

Doctors [] and [] who are no longer under contract with the FBI, previously provided psychological services to Bureau employees as part of the Bureau's psychological services program. As of March 2001, Dr. [] on behalf of himself and his wife, Dr. [] requested they be given the opportunity to retain confidentiality on a case-by-case basis. Therefore, Dr. [] requested that he or his wife continue to be notified if information provided by them is in a file being processed pursuant to the FOIPA. Doctor [] and [] may be contacted at telephone number [] which is their residential and business number. This notification should be done at the Team Captain level or higher.

b6

Thus, if information provided by the Doctors is located in any document being processed by FOIPA Section employees, the doctors should be notified. Unless advised to the contrary by them, the information should be protected by FOIPA exemptions (k)(5)/(b)(7)(D) in order to protect the confidentiality of both doctors. If the information cannot be protected for some reason such as prior public disclosures, the Doctors should be contacted and notified of that fact.

Metropolitan Psychiatric Group

[] Metropolitan Psychiatric Group (MPG) telephone 202-452-9080, has provided psychological services to FBI employees. Information provided by Dr. [] and/or any member of the MPG should be afforded protection for confidentiality purposes pursuant to FOIPA exemptions (k)(5)/(b)(7)(D). Also, should there be situations where a document being processed contains information provided by the MPG about a third party employee, not the requesting employee, the third party information should be protected in its entirety for privacy rights of the third party and the confidentiality of MPG pursuant to FOIPA exemptions (k)(5), (b)(7)(D), (b)(6), etc.

b6

Any questions concerning the FBI's psychological services program or specific questions concerning particular cases should be directed to the Unit Chief of the Employment Assistance

FOIPA Numbered Memo 73

Page 2

Psychological Services to FBI Employees

Program at 324-5244.

FOIPA Numbered Memo 74

Page 2

Reading Room, FOIPA

describing the material the PLS is forwarding to the Public Reading Room. Attached hereto are two examples of the EC.

If additional information is being released on Reading Room subjects as a result of reprocessing, appeals or litigations, the Reading Room package should be updated through coordination with Reading Room personnel.

Consultation Referrals Returned from Other Government Agencies

When FBI consultation referrals are returned to the FBI following review by the other agency, they sometimes contain changes in classification. Regardless of whether the classification changes, all consultation referrals returned from other government agencies containing classified information must be returned to DCU for annotation of classification markings desired by the other government agency. The returned referral documents are being treated as walk-ups by the DCU, thus eliminating needless administrative requirements and delays.

Credit for Direct Response Referrals

Effective 7/1/95, PLSs will receive credit for reviewing documents originated by other government agencies. Therefore, the pages referred to other agencies for direct response are to be counted as reviewed pages by the PLS.

When referring documents originated by the other agency, refer only one copy of the document with any FBI information which needs protected blacked out except for the following:

1. CIA - Send two copies of the document (1 black out copy and 1 clean copy)
2. DOJ/Civil Rights Division - Send two copies of the document (1 black out copy and 1 clean copy)
3. DOJ/Criminal Division - Highlight or bracket information to be protected and cite exemption (Do not black out)
4. NSA - Coordinate with PLS assigned to the Unit which handles referrals to NSA

FOIPA

MANUAL

MEMO 76

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Selective Service System
Date: March 31, 1998

Draft Board Information

Effective 2/14/91, Mr. Henry Williams, Selective Service System, advised Draft Board information pertaining to an individual of a first party request may be released to that individual. Likewise, Draft Board information concerning a deceased individual may also be released to third party requesters. Therefore, **DO NOT refer** Draft Board information to Selective Service concerning deceased individuals.

FOIPA

MANUAL

MEMO

77

To: All FBI FOIPA Personnel
From: John M. Kelso, Jr.
Subject: **Special Agent and Support Applicant Interview Forms/Testing Material**
Date: July 19, 2000

Special Agent Interview Forms

Effective 7/14/93, there is no longer a need to protect any information in the captioned forms listed below, since they are not being used in the current Special Agent selection system.

FD-190	Special Agent Interview Form
FD-511	Special Agent Dimension Evaluation Work Sheet
FD-510	Special Agent Applicant Interview Board Background Interview Form

Since the implementation of the new Special Agent selection system in August of 1994, no testing material of any kind is being maintained in the applicant=s personnel record (67 classification). This material is securely stored in Personnel Resources Unit (PRU) for a time period of one year, at which time, it is transferred to an off-site location for an additional year. At the end of this two-year period, all testing material on a Special Agent Applicant is destroyed. When processing a personnel file, if it appears that any testing material from the Special Agent selection process is included in the background portion of the file, contact the Unit Chief of the PRU immediately on extension 4991. DO NOT PROCESS OR RELEASE any of this material.

Achecklists@ of the material contained in testing packages are occasionally found in the Special Agent applicant file. One such Achecklist@ is the **Checklist for Health Fraud Written Simulation** and the **Checklist for Bank Loan Fraud Written Exercise** forms. If these check lists are found in the applicant file, the PLS should cite the appropriate exemption for testing material. Other Achecklists@ of testing packages found in the applicant file should be reviewed for disclosure on a case-by-case basis.

PRU, advised the **Special Agent Selection Phase I Applicant Testing Checklist form (FD-831)** and **Special Agent Selection Phase II Applicant Testing Checklist form (FD-849)** are releaseable

b6

FOIPA Numbered Memo 77

Page 2

Special Agent and Support Applicant Interview Forms/Testing Material

The FBI started audio taping the interview process of Special Agent applicants during 1995. The applicant is advised of this before the start of the interview. If the cassette tape is located in the personnel file during processing, contact the Unit Chief of PRU on extension 4991. **DO NOT PROCESS OR RELEASE** this tape.

Support Applicant Interview Forms

If the LT/PLS finds the **Support Applicant Interview Form (FD-190a)** in the background portion of a personnel file with a revision date **prior to 9/4/96**, the form is to be released in its entirety with the exception of any FBI employees names which should be protected pursuant to the appropriate FOIPA exemptions. Currently, **the 9/4/96 revised version** contains specific interview questions, responses and ratings which, if released, would give an unfair advantage to future support employee applicants. Therefore, this information on the current version of the FD-190a should be exempted as testing material. If the current version of this form is found in the personnel file during processing pursuant to an FOIPA request and it is not serialized, the form should be removed and sent to PRU at Room PA-750.

PRU, advised that the **Applicant Checklist for the Special Agent Position form (FD-869)**, which is a five-page document, can be released in its entirety. However, the signature of the Applicant Coordinator or SA Recruiter, which is located on page 5 of the document must be withheld citing the appropriate FOIPA exemptions.

b6

In addition, any **Clerical Selection Battery (CSB)** interview documents (e.g., **FD-799 and FD-800 and FD-859**) should not be contained in any personnel files since field offices are instructed to send these to the PRU for maintenance and destruction (after two years). However, PRU is aware that the CJIS Division in West Virginia made copies of all their interviews and included them in packages submitted to the Applicant Unit for background investigations. These interviews are removed from the files as detected, but there are of some CSB documents that remain in the personnel files. In the event these documents are found in personnel files when processing pursuant to an FOIPA request and are not serialized, they should be removed and sent to PRU at Room PA-750.

During 1997, the FBI started audio taping the interview process of support applicants. The applicant is advised of this fact before the interview is started. If the cassette tape is located in the personnel file at the time of processing, contact the Unit Chief of PRU on extension 4991. **DO NOT PROCESS OR RELEASE** this tape.

When the FBI receives a Privacy Act request for material related to the Special Agent or

FOIPA Numbered Memo 77

Page 3

Special Agent and Support Applicant Interview Forms/Testing Material

clerical applicant testing and interview process, IPU personnel will place a note in the request folder confirming they advised PRU of the existence of the request. When processing such a request, the PLS should contact either [redacted] Disclosure Unit 1, telephone 220-1106, [redacted] Disclosure Unit 2, telephone 220-1006, [redacted] Disclosure Unit 3, telephone 220-1751 or [redacted] Disclosure Unit 4, telephone 220-1148, who have been designated as liaisons to review this restricted material. These individuals will verify that the material is responsive, provide a page count and advise as to the releasability of the material.

b6

FOIPA Numbered Memo 79

Page 2

Special File Room

(5) If copies are made for processing, **the copies must also be secured overnight in a safe-like cabinet.**

(6) When the PLS closes a case which includes a copy of material from the SFR, the PLS should hand carry **the disclosure letter and all of the processed documents** to the SFR for filing. If the PLS referred a copy of a document(s) maintained in the SFR to another Federal Government agency and is attaching a copy of the referred document(s) to the yellow of the referral form, **the referral with enclosure** must also be sent to the SFR for filing. This also applies to any **referral response enclosing a copy of a document(s) maintained in the SFR.** All other FOIPA mail should be sent to the 190 Processing Subunit in IPU.

(7) **All material from the SFR must be hand carried to and from the SFR.**

Review of Special Compartmentalized Information (SCI) Material

Special security clearances are required to review or handle certain ATop Secret@ files or documents which contain SCI material. If the LT/PLS is notified by the SFR that he/she does not have the appropriate clearance to review the classified material requested, one of the following PLSs should be contacted to conduct the review. It is recommended that the individual contacted be from the same unit as the PLS handling the case.

Disclosure Units:

Unit 1
Unit 4

I. Unit 3

b6

Litigation Unit:

Help Desk:

DCU:

All Team Captains in DCU are afforded SCI clearances. However, should there be any questions concerning classification matters on a case prior to DCU review, the LT or PLS should initially contact the DCU Administrative Team Captain.

RMU:

Currently, there are no RMU employees with an SCI clearance. If an RMU employee has been advised by the SFR that they do not have the proper clearance to review the file material, they should contact one of the Disclosure PLSs listed above.

FOIPA

MANUAL

MEMO 82

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Telephone Application
Date: March 31, 1998

The Telephone Application (TA), formerly known as the Computerized Telephone Number File (CTNF), supports FBI investigative squads in collecting, analyzing and processing telephone data obtained during investigations. [redacted]

b7E

The main value of using the TA is the ability [redacted]

b7E

When processing a FOIPA request that contains information which refers to TA or the former CTNF, the mere mention of these systems should be protected pursuant to Exemption (b)(7)(E) since they are not systems of records and their use is not generally known to the public. In addition, all FBI information or documents that reflect or denote what information or the type of information that has been entered into these systems such as the FD-450 (**Attachment 1**) should be denied from public disclosure pursuant to the same exemption.

Third Party Requests/Third Party Information

Proof of Death

The guidelines concerning the proof needed before processing and releasing records about a subject whom the requester asserts is dead are as follows:

1. The subject of a third party request should be presumed to be alive unless there is a record confirming death. The record of death can be a death certificate, obituary, or recognized reference source (e.g., Who Was Who in America).
2. A mere assertion by a requester that a subject is dead is not sufficient proof of death.
3. Death can be presumed if the requester asserts the subject is dead, and there is proof that the subject is at least 100 years old.
4. If our own records establish death, then that is satisfactory.

Waivers of Privacy

Waivers of privacy require careful analysis, since there is significant potential for an inadvertent violation of the Privacy Act's disclosure prohibitions if a waiver is interpreted inaccurately or if a waiver is insufficient. A waiver does not authorize anything more than what is stated in the waiver itself. The waiver should be compared with the request letter to ensure that a limited waiver is not misquoted by the requester. If any aspect of the waiver is not clear, the request should be brought to the attention of supervisory personnel for additional review.

Waivers of personal privacy must be signed by the person waiving privacy, preferably in the presence of a notary, must specifically identify the person waiving privacy (including full name, date of birth and present address), and must be specifically directed to the FBI, permitting the FBI to release personal information (about the person executing the waiver) from its files. The waiver should be dated within a reasonable time period preceding the request, and the original copy of the waiver must be provided to the FBI.

Third Party Information

Information in FBI files concerning third parties which has **not been provided** by the requester, and which is **not outweighed** by a public interest in disclosure, **should be denied pursuant to Exemption (b)(7)(C)**. An exception to this general standard will involve historical processing, wherein substantive information concerning third parties may be considered for

FOIPA Numbered Memo 83

Page 3

Third Party Requests/Third Party Information

released.

Information in FBI files concerning third parties which has been provided by the first party requester will be processed to protect the identity of the third parties pursuant to Exemption (b)(7)(C). This may require the redaction of the third party's name, or it may require the redaction of significant portions of the substantive information, if an identifiable profile would otherwise be revealed. Although considerable flexibility and judgement will be required to determine how much information can be released without identifying the third party, the standard should be to protect all information which would identify the third party to a member of the public who does not have inside information about the case. The special knowledge of an individual requester should not be considered. This balances the right of a first party requester to know what information a governmental agency may have recorded from his own statements to that agency, while still protecting the privacy interests of persons who have been mentioned in or been the subject of an investigation.

Third party information in government files being processed pursuant to a first or third party request must be weighed between the public's right to know and the individual's right to privacy. In balancing the public interest in disclosure against personal privacy rights of individuals, the reviewer should first determine that a right of privacy exists. Unless the information at issue can significantly contribute to a public understanding of government operations and activities, the privacy interest should prevail and disclosure of more than public source information in widely acknowledged cases would be unwarranted. For additional information concerning the balancing of interests in personal information, see FOIA Update, Vol. X, No. 2, Spring 1989 edition, published by the Office of Information and Privacy, U.S. Department of Justice (**See Attachment 3**).

FOIPA

MANUAL

MEMO

84

To: All FBI FOIPA Personnel
From: John M. Kelso, Jr.
Subject: Undercover Operations
Date: March 19, 2001

The recording of an undercover contact is usually made on an FD-302 by the office responsible for the undercover operation and since the targets/subjects may reside or work anywhere in the country, copies of the FD-302 may appear in substantive files of other field offices. The contact with the subject may have been productive or unproductive; prosecution may have ensued or the investigation of the individual may have been closed. The undercover operation which generated the contact, however, could still be operative.

The FD-302 may be prefaced in the following manner: "On (date) SA (Name) , using the undercover name (Name) , contacted (Subject) at (Address) , etc." References to the contact, however, could appear in any format or communication.

[Redacted]

b7E

An unintentional disclosure of information regarding the contact to the subject could jeopardize an ongoing operation and the agents who are in contact with other individuals known to the subject of the closed case.

[Redacted]

b7E

To prevent this possibility, **the Undercover and Sensitive Operations Unit, Division 6, as well as the office responsible for the undercover operation, should be contacted to determine if the operation is still functional and if disclosure of the document in question would jeopardize the operation.**

[Redacted]

b7E

[Redacted]

FOIPA Numbered Memo 84
Page 2
Undercover Operations



b7E

FOIPA Numbered Memo 86

Page 2

White House Referrals and Consultations

In coordination with the Office of the Counsel to the President, the Department of Justice has determined that agencies should implement the following FOIA procedures regarding all White House related records or information found in their files. Please note that these procedures prescribe >consultations,= which do not involve a transfer of administrative responsibility for responding to a FOIA request, as distinct from complete record >referrals.=²

In all instances involving White House records or information, your agency will be responsible for responding directly to the FOIA requester once the process of consultation is completed.@

A1. Records originating with any part of the >White House Office=³ should be forwarded to the Office of the Counsel to the President for any recommendation or comment it may wish to make, including any assertion of privilege, prior to your response to the FOIA requester. Please be sure to advise the White House Counsel=s Office of any sensitivity that these records have from the perspective of your agency and whether you believe any FOIA exemption applies. If after considering the possibility of discretionary disclosure in accordance with the Attorney General=s FOIA Memorandum of October 4, 1993, you believe that a FOIA exemption applies, you should mark each record accordingly to facilitate review by the Counsel=s Office of your proposed response.@

All such consultation communications should be forwarded to the White House Counsel=s Office at the following address:

Office of the Counsel to the President
The White House

²"See FOIA Update, Summer 191, at 3-4 (>OIP Guidance: Referral and Consultation Procedures=) (further discussing differences between these two procedures).

³"The >White House Office= includes, among other components, the Offices of the President, Cabinet Affairs, Chief of Staff, Communications, First Lady, Counsel to the President, Intergovernmental Affairs, Legislative Affairs, Management and Administration, Operations, Political Affairs, Presidential Personnel, Public Liaison, Scheduling and Advance, Staff Secretary, Correspondence, Visitors, Policy Development, Domestic Policy Council, Environmental Policy, Council of Economic Advisors, National Economic Council, Assistant to the President for National Security Affairs and Deputy Assistant to the President for National Security Affairs, Assistant to the President for Science and Technology, and the Presidents Foreign Intelligence Advisory Board. The White House Office also includes task forces and working groups created by the President or an official in the White House, and reporting to the President or an official in the White House, including, for instance, the National Performance Review.@

FOIPA Numbered Memo 86

Page 3

White House Referrals and Consultations

1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

APlease note that many records originating with the White House Press Office, such as APress Briefings@ and AWhite House Talking Points@ (unless they are marked as, or appear to be drafts), are in the public domain and thus **may be disclosed without consultation.**

Questions concerning records likely to be in the public domain should be referred to the White House Counsel=s Office as well.@

Alt is possible that a record originating in the White House Office (or in the Office of the Vice President--see below) will be one over which the White House Office (or the Office of the Vice President) has retained control, in which case it will not be an >agency record= subject to the FOIA even though it is located by a federal agency in response to a FOIA request. Accord, e.g., Goland v. CIA, 6707 F.2d 339, 345-48 (D.C. Cir 1978) (honoring >retention of control= by non-FOIA entity), cert. denied, 445 U.S. 927 (1980; see also Paisley v. CIA, 712 F.2d 686, 692-94 (D.C. Cir. 1983); Holy spirit Ass=n v. CIA, 636 F.2d 838, 840-042 (D.C. Cir. 1981). Any such records should be identified for special handling.@

A2. Any record originating with the Office of the Vice President or any of its component offices, offices which likewise are not subject to the FOIA, should be forwarded for consultation purposes to the Office of the Counsel to the Vice President, Old Executive Office Building, Room 269, Washington, D.C. 20501.@

A3. All records originating with other offices within the Executive Office of the President (EOP--including the Office of Administration; the Office of Management and Budget; the Office of Science, Technology and Space Policy; the Office of the U.S. Trade Representative; the Council on Environmental Quality; and the Office of National Drug Control Policy--should be forwarded to the FOIA officers of the relevant individual EOP offices. This, again, is for consultation purposes only; agencies remain responsible for responding directly to the FOIA requester once these EOP consultations have been completed. For your convenience, a contact list for these EOP offices is attached.@

A4. Responses to FOIA requests for any classified White House records or records originating with the National Security Council should be coordinated with Ms. Nancy V. Menan of the National Security Council at the following address:

Director of Information Disclosure
Office of Information Disclosure
National Security Council
Old Executive Office Building, Room 392
Washington, D.C. 20506

FOIPA Numbered Memo 86

Page 4

White House Referrals and Consultations

Records originating with the Assistant to the President for National Security Affairs or his deputy should continue to be treated as records originating in the White House Office (see footnote 3 above).@

If any question arises regarding these procedures, either generally or in any particular case, please do not hesitate to contact Margaret Ann Irving, Acting Deputy Director of the Justice Department=s Office of Information and Privacy, at (202) 514-4251.@

Executive Office of the President--Agencies Subject to the FOIA@

Council on Environmental Quality
Deputy General Counsel
722 Jackson Place, N.W., Room 31
Washington, D.C. 20006

Office of Administration
Director, Administrative Services Division
Old Executive Office Building, Room 350
Washington, D.C. 20500

Office of Management and Budget
Deputy Assistant Director for Administration
New Executive Office Building, Room 9026*
Washington, D.C. 20503

Office of National Drug Control Policy
FOIA Officer
750 17th Street, N.W., 8th Floor
Washington, D.C. 20500

Office of Science, Technology and Space Policy
Executive Director
726 Jackson Place, N.W., Room 5013
Washington, D.C. 20500

Office of the U.S. Trade Representative
FOIA Officer
600 17th Street, N.W., Room 222
Washington, D.C. 20506

* OMB requests that records be forwarded to the attention of Darrell A. Johnson at this address.

FOIPA Numbered Memo 87

Page 2

Witnesses - Protection of Information

accord Lesar v. United States Department of Justice, 636 F.2d 472 (D.C. Cir. 1980). However, there can be a waiver of confidentiality, either explicit or implicit, by the source. DOJ policy at this time is that a waiver will be found as to information which is given in testimony in open court. Once again, though, if FBI records do not include a trial transcript, Exemption (b)(7)(D) may apply because there is no way to determine from FBI records which information is in the public record.

Another point which needs to be made is that Exemption (b)(7)(D) does not depend on a balancing test or on the information provided: AExemption (b)(7)(D) differs from other FOIA exemptions in that its applicability depends not on the specific factual contents of a particular document; instead, the pertinent question is whether the information at issue was furnished by a >confidential source= during the course of a legitimate criminal law enforcement investigation.@ Once this question has been answered in the affirmative, it must be determined if it was provided under an expressed or implied promise of confidentiality and reviewed as such for any discretionary disclosure of information.

Finally, PLSs should be aware that under certain circumstances, Exemption (b)(7)(F) may be used even though (b)(7)(C) and (D) are inapplicable.

FOIPA Numbered Memo 88

Page 2

World War II Censorship Documents

(a) Information concerning communications intelligence or cryptography and their related activities.

(b) Information concerning the intelligence method of secret writing, microphotography and their detection.

(c) Information concerning foreign governmental censorship activities as disclosed by U.S. liaison with foreign censorship agencies and not previously declassified and released.

3. Unclassified and declassified information in censorship intercepts and similar documents: Information in censored communications and related documents covered by this guideline that clearly identifies living individuals or organizations will normally be exempted from release in those cases where its disclosure would constitute a clearly unwarranted invasion of personal privacy [cf. 5 U.S.C. 552 (b)(6) and/or (b)(7)(C)]. Reviewers of documents covered by this portion of the guideline should determine whether the document contains information about a living individual which reveals details of a highly personal nature which the individual could reasonably assert a claim to withhold from the public to avoid a clearly unwarranted invasion of privacy. Such information may be disclosed, however, to the individuals who were parties to the communication or their authorized representatives. Further, segregated portions of a record document requested under the Freedom of Information Act shall be provided to any person requesting such record after deletion of the portions which are exempt under this guideline. Information which may be exempted from such release may be further defined as:

(a) Information clearly identifying living individuals or organizations whose communications were intercepted, were the object of surveillance or were of particular interest to the intelligence agencies of the United States or its Allies, including the following:

- (1) Originals, photocopies, transcripts or extracts from intercepted communications;
- (2) Daily reports (also known as ADayreps®) which were Office of Censorship messages to stations providing background information on persons and organizations of interest to the Office of Censorship;
- (3) Special watch instructions (also known as SWIs) which were instructions or supplemental information on particular persons, addresses, organizations, etc., whose communications are to be intercepted;
- (4) Watch lists/flash lists which are lists of persons, organizations, addresses, etc., with indicator of subject interest, whose communications are to be intercepted, including proposed entries and deletions;

FOIPA Numbered Memo 88

Page 3

World War II Censorship Documents

(5) White lists which are names of persons whose communications were to be bypassed without examination including entries and deletions;

(6) Border watch/flash lists which includes names of persons whose communications across the U.S. borders were of particular interest to a local censorship station, including entries and deletions thereto.

(b) Information clearly identifying living individuals or organizations involved in either complaints or recommendations arising out of such complaints about carrying out the specific provisions of the Code of Wartime Practices for the American Press and Broadcasters and not previously wholly releasable.

FOIPA Numbered Memo 89

Page 2

COINTELPRO (Counter-Intelligence Program)

Communist Party	Bufile:	100-3-104
Socialist Workers Party	Bufile:	100-436291
White Hate	Bufile:	157-9
Black Nationalist	Bufile:	100-448006
New Left	Bufile:	100-449698
Special Operations	Bufile:	105-174254
Soviet-Bloc	Bufile:	65-69260
Border Coverage	Bufile:	100-434445
Yugoslav	Bufile:	105-190290
Cuban	Bufile:	105-99938
Puerto Rican	Bufile:	105-93124
Hoodwink	Bufile:	100-446533

If a "no record" response is going to be given to a requester who has indicated he may have been the target of a COINTELPRO action, the following language should be used:

AA review of the appropriate records pertaining to COINTELPRO actions was conducted and no indication that you were ever the target of a COINTELPRO action was located.@

NOTE: If FBI records indicate a COINTELPRO action was not reviewed in accordance with the Attorney General's notification program regarding COINTELPRO activities, then notice should be sent to the attention of the Counsel, Office of Professional Responsibility, Room 4304 - MJB at the Department of Justice.

CLASSIFICATION MATTERS CONCERNING
COINTELPRO MATERIAL

During a review of previously processed material located in the FBI FOIPA Reading Room, it was determined that there were some instances where the Reading Room copy and the original file copy were marked differently as to classification.

In order to ensure that COINTELPRO material processed under FOIPA, litigation or any other purpose, is consistent with material previously released and currently located in the FBI FOIPA Reading Room, a memorandum is being placed as a "ATop Serial," not to be serialized, in each of those original COINTELPRO files. PLSs processing material from these files are placed on notice that the Reading Room copy must also be reviewed to insure both are marked in a consistent manner. When such a review is completed, a notation must be made on the original that it has been compared to the Reading Room copy.

To: All FBI FOIPA Personnel
From: J. Kevin O'Brien
Subject: Department of the Army
Date: March 31, 1998

Army Intelligence Agency (AIA)

This following instructions set forth procedures for the handling of referrals to the Army Intelligence Agency (AIA) in which classified information is involved.

(1) If documents classified ATop Secret@ or ASecret@ are to be referred to the AIA, receipts should be attached indicating among other required information the name and telephone number of the FBI employee involved. Receipt forms are maintained by the Document Classification Unit (DCU).

(2) Regarding Army documents in FBI files referred to the Army for handling and direct response to the requester, the PLS should specifically request in the referral letter that the FBI be notified of any classification changes. Upon receipt of the Army=s notice of a classification change, the material should be forwarded to DCU where the changes will be noted on the FBI file copies of the Army documents. After those changes are noted, the photocopied material furnished by the Army should be destroyed.

FOIPA Numbered Memo 91

Page 2

File Classification "280"

elected to provide information in confidence. Release of information can be made in an open investigation; however, any proposed release should be coordinated with the Complaint Processing Unit of OEEOA prior to disclosure.

In addition to releases dealing with EEO investigations, proposed releases of all other 280 file matters should also be coordinated with OEEOA.

Red-outs should not be placed in 190 files. The pages containing deletions should be forwarded to OEEOA for filing into respective 280 file along with the OPCA-16 form (Disclosure letter).

FOIPA Numbered Memo 92

Page 2

Extradition Material

procedures as court proceedings in the United States. Court documents from foreign governments such as complaints, affidavits and arrest warrants in extradition matters should be denied in their entirety pursuant to exemption (b)(1) or (b)(7)(D) when applicable.

Be aware that there may be circumstances when it will be necessary to consult with the Criminal Investigative Division, International Relations Section, at FBIHQ or to refer the documents to the Office of International Affairs (OIA), Criminal Division, U.S. Department of Justice for further assistance.