

**THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

**REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS**

Plaintiff,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 19-2847 (TFH)

DECLARATION OF ADAM A. MARSHALL

I, Adam A. Marshall, declare as follows:

1. I am a staff attorney at the Reporters Committee for Freedom of the Press (“RCFP” or “Reporters Committee”), an unincorporated nonprofit association located in Washington, D.C. I have held this position since September 2016. Prior to becoming an RCFP staff attorney, I was its Jack Nelson/Dow Jones Foundation Legal Fellow; I held that position from September 2014 through August 2016. I am an attorney and co-counsel for Plaintiff in this matter.

2. I make this declaration in support of Plaintiff’s Cross-Motion for Partial Summary Judgment and in Opposition to Defendants’ Motion for Summary Judgment. I have personal knowledge of the matters stated in this declaration.

3. Since September 2014, when I joined the Reporters Committee, my legal practice has focused largely on access to public records under state public records laws and under the federal Freedom of Information Act (“FOIA”). My responsibilities include writing and submitting federal FOIA requests for RCFP. I submitted the FOIA requests at issue in the above-captioned case on behalf of the Reporters Committee.

4. On or about June 21, 2019, I submitted a FOIA request on behalf of RCFP to the Criminal Division of the Department of Justice (“Criminal Division”) via email, a true and correct copy of which is attached hereto as **Exhibit 1** (without attachment).

5. On or about June 21, 2019, I submitted a FOIA request on behalf of RCFP to the Executive Office for United States Attorneys (“EOUSA”) via email, a true and correct copy of which is attached hereto as **Exhibit 2** (without attachment).

6. On or about June 21, 2019, I submitted a FOIA request on behalf of RCFP to the Federal Bureau of Investigation (“FBI”) via fax, a true and correct copy of which is attached hereto as **Exhibit 3** (without attachment).

7. Each of RCFP’s requests at issue in this case included a signed privacy waiver/DOJ-361 form from Bryan Carmody.

8. Following submission of RCFP’s FOIA requests at issue in this case, EOUSA and the Criminal Division did not to provide a determination within the statutory timeframe.

9. On or around December 10, 2019, the EOUSA informed RCFP that the EOUSA had located no records responsive to RCFP’s request.

10. On or around December 16, 2019 the Criminal Division informed RCFP that the Criminal Division had located no records responsive to RCFP’s request.

11. On or around December 11, 2019, the FBI produced one partially redacted record to RCFP, a true and correct copy of which with redactions of a birth date made pursuant to Fed. R. Civ. P. 5.2(a) is attached hereto as **Exhibit 4**.

12. On or about March 4, 2020, I submitted a California Public Records Act request on behalf of RCFP to the San Francisco Police Department (“SFPD”) via online portal, a true and correct copy of which is attached hereto as **Exhibit 5**.

13. Attached hereto as **Exhibit 6** is a true and correct copy of a record produced by the SFPD to RCFP in response to RCFP's California Public Records Act request.

14. Attached hereto as **Exhibit 7** is a true and correct copy of portions of a record produced by the SFPD to RCFP in response to RCFP's California Public Records Act request.

15. Attached hereto as **Exhibit 8** is a true and correct copy of a June 11, 2019 CNN article titled "San Francisco police seize equipment of freelance journalist who refused to identify a source."

16. Attached hereto as **Exhibit 9** is a true and correct copy of the FBI's Records Management Policy Guide as published by the FBI at <https://vault.fbi.gov/records-management-policy-guide-0769pg-part-01-of-01/Records%20Management%20Policy%20Guide%200769PG%20Part%2001%20of%2001/view>.

17. Attached hereto as **Exhibit 10** is a true and correct copy of the DOJ's News Media Policy, 28 C.F.R. § 50.10, as published at https://www.ecfr.gov/cgi-bin/text-idx?SID=f1d3a7753bf1b4c6dc9f0aee72d3d0f6&mc=true&node=se28.2.50_110&rgn=div8.

18. Attached hereto as **Exhibit 11** is a true and correct copy of Section 9-13.400 of the United States Attorneys' Manual as published at <https://www.justice.gov/jm/jm-9-13000-obtaining-evidence#9-13.400>.

19. Attached hereto as **Exhibit 12** is a true and correct copy of a declaration from David Hardy that was filed in *Reporters Committee for Freedom of the Press, et al., v. FBI, et al.*, No. 1:15-cv-01392 (RJL).

20. Attached hereto as **Exhibit 13** is a true and correct copy of a record produced to the Reporters Committee from the FBI in *Reporters Committee for Freedom of the Press, et al., v. FBI, et al.*, No. 1:15-cv-01392 (RJL).

21. Attached hereto as **Exhibit 14** is a true and correct copy of a June 7, 2014 AP article titled “FBI: San Francisco Bomb Suspect Sought Toxins.”

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 1st day of July 2020 in Washington, D.C.

/s/ Adam A. Marshall

Adam A. Marshall

EXHIBIT 1

REPORTERS COMMITTEE

FOR FREEDOM OF THE PRESS

1156 15th Street, NW, Suite 1020
Washington, DC 20005
(202) 795-9300
www.rcfp.org
Bruce D. Brown
Executive Director
bbrown@rcfp.org
(202) 795-9301

STEERING COMMITTEE

STEPHEN J. ADLER
Reuters

J. SCOTT APPLEWHITE
The Associated Press
WOLF BLITZER
CNN

DAVID BOARDMAN
Temple University

MASSIMO CALABRESI
Time Magazine

MANNY GARCIA
USA Today Network

EMILIO GARCIA-RUIZ
The Washington Post

JOSH GERSTEIN
Politico

ALEX GIBNEY
Jigsaw Productions

SUSAN GOLDBERG
National Geographic

JAMES GRIMALDI
The Wall Street Journal

LAURA HANDMAN
Davis Wright Tremaine

DIEGO IBARGÜEN
Hearst

KAREN KAISER
The Associated Press

DAVID LAUTER
Los Angeles Times

DAHLIA LITHWICK
Slate

MARGARET LOW
The Atlantic

JANE MAYER
The New Yorker

MAGGIE MULVIHILL
Boston University

JAMES NEFF
Philadelphia Media Network

CAROL ROSENBERG
The New York Times

THOMAS C. RUBIN
Quinn Emmanuel

CHARLIE SAVAGE
The New York Times

BEN SMITH
BuzzFeed

JENNIFER SONDAG
Bloomberg News

PIERRE THOMAS
ABC News

SAUNDRA TORRY
Freelance

VICKIE WALTON-JAMES
NPR

JUDY WOODRUFF
PBS/The NewsHour

SENIOR ADVISORS

CHIP BOK
Creators Syndicate

JOHN C. HENRY
Freelance

TONY MAURO
National Law Journal

ANDREA MITCHELL
NBC News

PAUL STEIGER
ProPublica

*Affiliations appear only
for purposes of identification*

Adam A. Marshall
Reporters Committee for Freedom of the Press
1156 15th St. NW, Suite 1020
Washington, DC 20005
amarshall@rcfp.org

Department of Justice
Criminal Division
Chief, FOIA/PA Unit
Suite 1127, Keeney Building
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
Email: crm.foia@usdoj.gov

June 21, 2019

VIA EMAIL

RE: Freedom of Information Act Request

This letter constitutes a request under the federal Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”), and is submitted on behalf of the Reporters Committee for Freedom of the Press (“Reporters Committee” or “RCFP”) to the Criminal Division of the Department of Justice (“DOJ”). The Reporters Committee is a nonprofit association dedicated to protecting First Amendment freedoms and the newsgathering rights of journalists.¹

I. Background

For nearly three decades, Bryan Carmody has worked in the Bay Area as a journalist and videographer.² On May 10, 2019, San Francisco police raided Mr. Carmody’s home and office, taking a sledgehammer to the gate of his house and seizing his computers, phones and other devices.³ A spokesman for the San Francisco Police Department said that a search warrant was granted by a judge and executed as part of an inquiry into the release of the “Adachi police report.”⁴

¹ See generally www.rcfp.org.

² Amir Vera and Keith Allen, *San Francisco police seize equipment of freelance journalist who refused to identify a source* (June 11, 2019), <https://www.cnn.com/2019/05/14/media/california-journalist-equipment-seized/index.html>.

³ Laurel Wamsley, *San Francisco Police Raid Journalist's Home After He Refuses To Name Source* (May 13, 2019), <https://www.npr.org/2019/05/13/722745266/san-francisco-police-raid-journalists-home-after-he-refuses-to-name-source>.

⁴ *Id.*

The “Adachi police report” is the police report concerning the death of San Francisco public defender Jeff Adachi in February, who died at age 59.

Mr. Carmody has said that two inspectors with the San Francisco Police Department’s Internal Affairs Bureau initially asked for his source on the Adachi report in April 2019, but he declined to reveal the person’s name.⁵ Mr. Carmody has further stated that during the May 2019 search of his home, two men who identified themselves as FBI agents tried to interview him, but he declined to speak with them and asked for a lawyer.⁶

Please note the additional background information which is provided to facilitate the location of records responsive to this request:

- In January 2015, the Attorney General issued an updated policy, codified at 28 C.F.R. 50.10, regarding obtaining information from and questioning members of the news media (the “News Media Policy”). The News Media Policy mandates robust review and evaluation by the DOJ Criminal Division of requests for authorization to use covered law enforcement tools to question and obtain information from members of the news media, and requires oversight by senior DOJ officials. Under the News Media Policy, Attorney General approval is required before members of the DOJ can question or execute a search warrant against a member of the news media based on conduct related to newsgathering activities, among other things.
- Section 9-13.400 of the United States Attorneys’ Manual and the News Media Policy require members of the DOJ to submit a memorandum to the Policy and Statutory Enforcement Unit (“PSEU”) describing the relevant facts and considerations required to determine whether the DOJ may obtain information from, or records of, members of the news media, question or arrest members of the news media, or execute a search warrant against members of the news media. Submission of this memorandum is part of the mandatory consultation requirement wherein the Attorney General can evaluate whether law enforcement tools may be used with respect to members of the news media.
- Additionally, § 9-13.400 of the United States Attorneys’ Manual states that when there is a question regarding whether an individual or entity is a member of the news media, “members of the Department must consult with the PSEU before employing the use of a covered law enforcement tool. Members of the Department must also consult with the PSEU regarding whether the conduct at issue of the affected member of the news media constitutes or relates to ‘newsgathering activities.’”
- The Privacy Protection Act (“PPA”), codified at 42 U.S.C. § 2000aa *et seq.*, protects journalists from the search or seizure by law enforcement of any work product and documentary materials before dissemination to the public.

⁵ Evan Sernoffsky, *SF police raid journalist’s home in probe over leaked Adachi report* (May 10, 2019), <https://www.sfchronicle.com/crime/article/SF-police-raid-journalist-s-home-in-probe-over-13837363.php?psid=4xXNM>.

⁶ *Id.*

- The California Shield Law—found in California, Article I, § 2(b) of the California Constitution, California Evidence Code § 1070, and California Penal Code § 1524(g)—provides immunity from being held in contempt to reporters, editors, publishers, and other people connected with or employed by newspapers, magazines, press associations and wire services, as well as radio or TV news reporters. California Penal Code § 1524(g) states that no warrant shall issue for any item or items described in §1070 of the California Evidence Code. The California Shield Law applies to both the source of information (“confidential sources”) and to “unpublished information” such as notes, out-takes, unpublished photographs and tapes.

II. Requested Records

Pursuant to the FOIA, I, on behalf of the Reporters Committee, request access to and copies of the following records:

1. All records mentioning or referring to Bryan Carmody. A signed DOJ-361 form from Mr. Carmody is attached hereto.
2. All records, including email correspondence, text messages, and other electronic messages, that include the term “Carmody” (case insensitive) and any of the following keywords (case insensitive):
 - a. Shield
 - b. Privacy Protection Act
 - c. PPA
 - d. Leak
 - e. Leaks
 - f. Subpoena
 - g. Newsgathering
 - h. Question
 - i. Questions
 - j. Questioning
 - k. Media
 - l. Warrant
 - m. Search
 - n. Seize
 - o. Seizure;
3. All communications, including email correspondence, text messages, and other electronic messages between any individual at the Department of Justice and
 - a. the San Francisco Police Department
 - b. the District Attorney’s Office for the City and County of San Francisco
 - c. the San Francisco Sheriff’s Department
 - d. the California Bureau of Investigation
 - e. the California Office of the Governor, and/or
 - f. the California Highway Patrolthat mention, refer to, or discuss Bryan Carmody;

4. All records mentioning, referring to, or constituting the memorandum sent from the United States Attorney's Office for the Northern District of California seeking approval for questioning, arresting, or charging Bryan Carmody.

Please note that email correspondence, as referred to in this request, includes the entire email chain in which the DOJ is a sender or recipient (including a "cc" or "bcc") of one or more emails in the chain. This request also includes any email attachments. This request also includes official communications sent or received using any non-governmental email account or other electronic messaging account.

III. Fees and Fee Categorization

As a representative of the news media, the Reporters Committee is only required to pay for the direct cost of duplication after the first 100 pages. 5 U.S.C. § 552(a)(4)(A)(ii)(II). This information is being sought on behalf of the Reporters Committee for *inter alia*, analysis and free dissemination to the general public through multiple avenues, including RCFP's website,⁷ social media accounts,⁸ and email newsletter.⁹

In the event that there are duplication fees for responding to this request, the Reporters Committee is willing to pay up to \$50. Please let me know in advance if fees for responding to this request will exceed that amount before proceeding.

IV. Conclusion

If this request is denied in whole or part, please justify all such denials by reference to specific exemptions and explain why DOJ "reasonably foresees that disclosure would harm an interest" protected by that exemption or why "disclosure is prohibited by law[.]" 5 U.S.C. § 552(a)(8). Please also ensure that all segregable portions of otherwise exempt material are released.

If you have any questions regarding this request, please feel free to contact me at (202) 795-9308. Thank you in advance for your assistance.

Sincerely,
Adam A. Marshall
Knight Foundation Litigation Attorney
Reporters Committee for Freedom of the Press
amarshall@rcfp.org

⁷ <https://www.rcfp.org/>.

⁸ See, e.g., <https://twitter.com/rcfp> (~16.3 thousand followers as of May 14, 2019); <https://www.facebook.com/ReportersCommittee/> (8,148 "likes" as of May 14, 2019).

⁹ <https://rcfp.us15.list-manage.com/subscribe?u=682100887bbcff066b451132&id=8f701b284f>.

EXHIBIT 2

REPORTERS COMMITTEE

FOR FREEDOM OF THE PRESS

1156 15th Street, NW, Suite 1020
Washington, DC 20005
(202) 795-9300
www.rcfp.org
Bruce D. Brown
Executive Director
bbrown@rcfp.org
(202) 795-9301

STEERING COMMITTEE

STEPHEN J. ADLER
Reuters

J. SCOTT APPLEWHITE
The Associated Press
WOLF BLITZER
CNN

DAVID BOARDMAN
Temple University
MASSIMO CALABRESI
Time Magazine

MANNY GARCIA
USA Today Network
EMILIO GARCIA-RUIZ
The Washington Post
JOSH GERSTEIN
Politico

ALEX GIBNEY
Jigsaw Productions
SUSAN GOLDBERG
National Geographic

JAMES GRIMALDI
The Wall Street Journal

LAURA HANDMAN
Davis Wright Tremaine
DIEGO IBARGÜEN
Hearst

KAREN KAISER
The Associated Press
DAVID LAUTER
Los Angeles Times

DAHLIA LITHWICK
Slate

MARGARET LOW
The Atlantic

JANE MAYER
The New Yorker

MAGGIE MULVIHILL
Boston University

JAMES NEFF
Philadelphia Media Network

CAROL ROSENBERG
The New York Times

THOMAS C. RUBIN
Quinn Emmanuel

CHARLIE SAVAGE
The New York Times

BEN SMITH
BuzzFeed

JENNIFER SONDAG
Bloomberg News

PIERRE THOMAS
ABC News

SAUNDRA TORRY
Freelance

VICKIE WALTON-JAMES
NPR

JUDY WOODRUFF
PBS/The NewsHour

SENIOR ADVISORS

CHIP BOK
Creators Syndicate

JOHN C. HENRY
Freelance

TONY MAURO
National Law Journal

ANDREA MITCHELL
NBC News

PAUL STEIGER
ProPublica

*Affiliations appear only
for purposes of identification*

Adam A. Marshall
Reporters Committee for Freedom of the Press
1156 15th St. NW, Suite 1020
Washington, DC 20005
amarshall@rcfp.org

Department of Justice
Executive Office for United States Attorneys
FOIA/Privacy Unit
175 N Street, N.E.
Suite 5.400
Washington, DC 20530-0001
USAEFOIA.REQUESTS@usdoj.gov

June 21, 2019

VIA EMAIL

RE: Freedom of Information Act Request

This letter constitutes a request under the federal Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”), and is submitted on behalf of the Reporters Committee for Freedom of the Press (“Reporters Committee” or “RCFP”) to the Executive Office for United States Attorneys (“EOUSA”) for records maintained by the United States Attorneys’ Office for the Northern District of California (“USAO-NDC”). The Reporters Committee is a nonprofit association dedicated to protecting First Amendment freedoms and the newsgathering rights of journalists.¹

I. Background

For nearly three decades, Bryan Carmody has worked in the Bay Area as a journalist and videographer.² On May 10, 2019, San Francisco police raided Mr. Carmody’s home and office, taking a sledgehammer to the gate of his house and seizing his computers, phones and other devices.³ A spokesman for the San

¹ See generally www.rcfp.org.

² Amir Vera and Keith Allen, *San Francisco police seize equipment of freelance journalist who refused to identify a source* (June 11, 2019), <https://www.cnn.com/2019/05/14/media/california-journalist-equipment-seized/index.html>.

³ Laurel Wamsley, *San Francisco Police Raid Journalist's Home After He Refuses To Name Source* (May 13, 2019), <https://www.npr.org/2019/05/13/722745266/san-francisco-police-raid-journalists-home-after-he-refuses-to-name-source>.

San Francisco Police Department said that a search warrant was granted by a judge and executed as part of an inquiry into the release of the “Adachi police report.”⁴ The “Adachi police report” is the police report concerning the death of San Francisco public defender Jeff Adachi in February, who died at age 59.

Mr. Carmody has said that two inspectors with the San Francisco Police Department’s Internal Affairs Bureau initially asked for his source on the Adachi report in April 2019, but he declined to reveal the person’s name.⁵ Mr. Carmody has further stated that during the May 2019 search of his home, two men who identified themselves as FBI agents tried to interview him, but he declined to speak with them and asked for a lawyer.⁶

Please note the additional background information which is provided to facilitate the location of records responsive to this request:

- In January 2015, the Attorney General issued an updated policy, codified at 28 C.F.R. 50.10, regarding obtaining information from and questioning members of the news media (the “News Media Policy”). The News Media Policy mandates robust review and evaluation by the DOJ Criminal Division of requests for authorization to use covered law enforcement tools to question and obtain information from members of the news media, and requires oversight by senior DOJ officials. Under the News Media Policy, Attorney General approval is required before members of the DOJ can question or execute a search warrant against a member of the news media based on conduct related to newsgathering activities, among other things.
- Section 9-13.400 of the United States Attorneys’ Manual and the News Media Policy require members of the DOJ to submit a memorandum to the Policy and Statutory Enforcement Unit (“PSEU”) describing the relevant facts and considerations required to determine whether the DOJ may obtain information from, or records of, members of the news media, question or arrest members of the news media, or execute a search warrant against members of the news media. Submission of this memorandum is part of the mandatory consultation requirement wherein the Attorney General can evaluate whether law enforcement tools may be used with respect to members of the news media.
- Additionally, § 9-13.400 of the United States Attorneys’ Manual states that when there is a question regarding whether an individual or entity is a member of the news media, “members of the Department must consult with the PSEU before employing the use of a covered law enforcement tool. Members of the Department must also consult with the PSEU regarding whether the conduct at issue of the affected member of the news media constitutes or relates to ‘newsgathering activities.’”

⁴ *Id.*

⁵ Evan Sernoffsky, *SF police raid journalist’s home in probe over leaked Adachi report* (May 10, 2019), <https://www.sfchronicle.com/crime/article/SF-police-raid-journalist-s-home-in-probe-over-13837363.php?psid=4xXNM>.

⁶ *Id.*

- The Privacy Protection Act (“PPA”), codified at 42 U.S.C. § 2000aa *et seq.*, protects journalists from the search or seizure by law enforcement of any work product and documentary materials before dissemination to the public.
- The California Shield Law—found in California, Article I, § 2(b) of the California Constitution, California Evidence Code § 1070, and California Penal Code § 1524(g)—provides immunity from being held in contempt to reporters, editors, publishers, and other people connected with or employed by newspapers, magazines, press associations and wire services, as well as radio or TV news reporters. California Penal Code § 1524(g) states that no warrant shall issue for any item or items described in §1070 of the California Evidence Code. The California Shield Law applies to both the source of information (“confidential sources”) and to “unpublished information” such as notes, out-takes, unpublished photographs and tapes.

II. Requested Records

Pursuant to the FOIA, I, on behalf of the Reporters Committee, request access to and copies of the following records maintained by the USAO-NDC:

1. All records mentioning or referring to Bryan Carmody. A signed DOJ-361 form from Mr. Carmody is attached hereto.
2. All records, including email correspondence, text messages, and other electronic messages, that include the term “Carmody” (case insensitive) and any of the following keywords (case insensitive):
 - a. Shield
 - b. Privacy Protection Act
 - c. PPA
 - d. Leak
 - e. Leaks
 - f. Subpoena
 - g. Newsgathering
 - h. Question
 - i. Questions
 - j. Questioning
 - k. Media
 - l. Warrant
 - m. Search
 - n. Seize
 - o. Seizure;
3. All communications, including email correspondence, text messages, and other electronic messages between any individual at the USAO-NDC and
 - a. the San Francisco Police Department
 - b. the District Attorney’s Office for the City and County of San Francisco
 - c. the San Francisco Sheriff’s Department

- d. the California Bureau of Investigation
 - e. the California Office of the Governor, and/or
 - f. the California Highway Patrol,
- that mention, refer to, or discuss Bryan Carmody;

4. All records mentioning, referring to, or constituting the memorandum sent from the USAO-NDC seeking approval for questioning, arresting, or charging Bryan Carmody.

Please note that email correspondence, as referred to in this request, includes the entire email chain in which the USAO-NDC is a sender or recipient (including a “cc” or “bcc”) of one or more emails in the chain. This request also includes any email attachments. This request also includes official communications sent or received using any non-governmental email account or other electronic messaging account.

III. Fees and Fee Categorization

As a representative of the news media, the Reporters Committee is only required to pay for the direct cost of duplication after the first 100 pages. 5 U.S.C. § 552(a)(4)(A)(ii)(II). This information is being sought on behalf of the Reporters Committee for *inter alia*, analysis and free dissemination to the general public through multiple avenues, including RCFP’s website,⁷ social media accounts,⁸ and email newsletter.⁹

In the event that there are duplication fees for responding to this request, the Reporters Committee is willing to pay up to \$50. Please let me know in advance if fees for responding to this request will exceed that amount before proceeding.

IV. Conclusion

If this request is denied in whole or part, please justify all such denials by reference to specific exemptions and explain why EOUSA “reasonably foresees that disclosure would harm an interest” protected by that exemption or why “disclosure is prohibited by law[.]” 5 U.S.C. § 552(a)(8). Please also ensure that all segregable portions of otherwise exempt material are released.

If you have any questions regarding this request, please feel free to contact me at (202) 795-9308. Thank you in advance for your assistance.

Sincerely,
Adam A. Marshall
Knight Foundation Litigation Attorney
Reporters Committee for Freedom of the Press
amarshall@rcfp.org

⁷ <https://www.rcfp.org/>.

⁸ See, e.g., <https://twitter.com/rcfp> (~16.3 thousand followers as of May 14, 2019); <https://www.facebook.com/ReportersCommittee/> (8,148 “likes” as of May 14, 2019).

⁹ <https://rcfp.us15.list-manage.com/subscribe?u=682100887bbcff066b451132&id=8f701b284f>.

EXHIBIT 3

Fax Transmission

To: Federal Bureau of Investigation

Fax: 15408684391

RE: FOIA Request

From: Reporters Committee for Freedom of the

Date: 6/21/2019 7:04:47 AM PDT

Pages: 6

Comments:

To whom it may concern:

Please see the attached request under the Freedom of Information Act, 5 U.S.C. 552, from the Reporters Committee for Freedom of the Press.

Sincerely,

Adam A. Marshall

REPORTERS COMMITTEE

FOR FREEDOM OF THE PRESS

1156 15th Street, NW, Suite 1020
Washington, DC 20005
(202) 795-9300
www.rcfp.org
Bruce D. Brown
Executive Director
bbrown@rcfp.org
(202) 795-9301

STEERING COMMITTEE

STEPHEN J. ADLER
Reuters

J. SCOTT APPLEWHITE
The Associated Press
WOLF BLITZER
CNN

DAVID BOARDMAN
Temple University
MASSIMO CALABRESI
Time Magazine

MANNY GARCIA
USA Today Network
EMILIO GARCIA-RUIZ
The Washington Post

JOSH GERSTEIN
Politico

ALEX GIBNEY
Jigsaw Productions

SUSAN GOLDBERG
National Geographic

JAMES GRIMALDI
The Wall Street Journal

LAURA HANDMAN
Davis Wright Tremaine

DIEGO IBARGÜEN
Hearst

KAREN KAISER
The Associated Press

DAVID LAUTER
Los Angeles Times

DAHLIA LITHWICK
Slate

MARGARET LOW
The Atlantic

JANE MAYER
The New Yorker

MAGGIE MULVIHILL
Boston University

JAMES NEFF
Philadelphia Media Network

CAROL ROSENBERG
The New York Times

THOMAS C. RUBIN
Quinn Emmanuel

CHARLIE SAVAGE
The New York Times

BEN SMITH
BuzzFeed

JENNIFER SONDAG
Bloomberg News

PIERRE THOMAS
ABC News

SAUNDRA TORRY
Freelance

VICKIE WALTON-JAMES
NPR

JUDY WOODRUFF
PBS/The NewsHour

SENIOR ADVISORS

CHIP BOK
Creators Syndicate

JOHN C. HENRY
Freelance

TONY MAURO
National Law Journal

ANDREA MITCHELL
NBC News

PAUL STEIGER
ProPublica

*Affiliations appear only
for purposes of identification*

Adam A. Marshall
Reporters Committee for Freedom of the Press
1156 15th St. NW, Suite 1020
Washington, DC 20005
amarshall@rcfp.org

Federal Bureau of Investigation (FBI)
Record/Information Dissemination Section (RIDS)
170 Marcel Drive
Winchester, VA 22602-4843
Fax: 540-868-4391

June 21, 2019

VIA FAX

RE: Freedom of Information Act/Privacy Act Request

This letter constitutes a request under the federal Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”) and is submitted on behalf of the Reporters Committee for Freedom of the Press (“Reporters Committee” or “RCFP”) to the Federal Bureau of Investigation (“FBI”). The Reporters Committee is a nonprofit association dedicated to protecting First Amendment freedoms and the newsgathering rights of journalists.¹

I. Background

For nearly three decades, Bryan Carmody has worked in the Bay Area as a journalist and videographer.² On May 10, 2019, San Francisco police raided Mr. Carmody’s home and office, taking a sledgehammer to the gate of his house and seizing his computers, phones and other devices.³ A spokesman for the San Francisco Police Department said that a search warrant was granted by a judge and executed as part of an inquiry into the release of the “Adachi police report.”⁴ The “Adachi police report” is the police report concerning the death of San Francisco public defender Jeff Adachi in February, who died at age 59.

¹ See generally www.rcfp.org.

² Amir Vera and Keith Allen, *San Francisco police seize equipment of freelance journalist who refused to identify a source* (June 11, 2019), <https://www.cnn.com/2019/05/14/media/california-journalist-equipment-seized/index.html>.

³ Laurel Wamsley, *San Francisco Police Raid Journalist's Home After He Refuses To Name Source* (May 13, 2019), <https://www.npr.org/2019/05/13/722745266/san-francisco-police-raid-journalists-home-after-he-refuses-to-name-source>.

⁴ *Id.*

Mr. Carmody has said that two inspectors with the San Francisco Police Department's Internal Affairs Bureau initially asked for his source on the Adachi report in April 2019, but he declined to reveal the person's name.⁵ Mr. Carmody has further stated that during the May 2019 search of his home, two men who identified themselves as FBI agents tried to interview him, but he declined to speak with them and asked for a lawyer.⁶

Please note the additional background information which is provided to facilitate the location of records responsive to this request:

- In January 2015, the Attorney General issued an updated policy, codified at 28 C.F.R. 50.10, regarding obtaining information from and questioning members of the news media (the "News Media Policy"). The News Media Policy mandates robust review and evaluation by the DOJ Criminal Division of requests for authorization to use covered law enforcement tools to question and obtain information from members of the news media, and requires oversight by senior DOJ officials. Under the News Media Policy, Attorney General approval is required before members of the DOJ can question or execute a search warrant against a member of the news media based on conduct related to newsgathering activities, among other things.
- Section 9-13.400 of the United States Attorneys' Manual and the News Media Policy require members of the DOJ to submit a memorandum to the Policy and Statutory Enforcement Unit ("PSEU") describing the relevant facts and considerations required to determine whether the DOJ may obtain information from, or records of, members of the news media, question or arrest members of the news media, or execute a search warrant against members of the news media. Submission of this memorandum is part of the mandatory consultation requirement wherein the Attorney General can evaluate whether law enforcement tools may be used with respect to members of the news media.
- Additionally, § 9-13.400 of the United States Attorneys' Manual states that when there is a question regarding whether an individual or entity is a member of the news media, "members of the Department must consult with the PSEU before employing the use of a covered law enforcement tool. Members of the Department must also consult with the PSEU regarding whether the conduct at issue of the affected member of the news media constitutes or relates to 'newsgathering activities.'"
- The Privacy Protection Act ("PPA"), codified at 42 U.S.C. § 2000aa *et seq.*, protects journalists from the search or seizure by law enforcement of any work product and documentary materials before dissemination to the public.
- The California Shield Law—found in California, Article I, § 2(b) of the California Constitution, California Evidence Code § 1070, and California Penal Code § 1524(g)—provides immunity from being held in contempt to reporters, editors, publishers, and other

⁵ Evan Sernoffsky, *SF police raid journalist's home in probe over leaked Adachi report* (May 10, 2019), <https://www.sfchronicle.com/crime/article/SF-police-raid-journalist-s-home-in-probe-over-13837363.php?psid=4xXNM>.

⁶ *Id.*

people connected with or employed by newspapers, magazines, press associations and wire services, as well as radio or TV news reporters. California Penal Code § 1524(g) states that no warrant shall issue for any item or items described in §1070 of the California Evidence Code. The California Shield Law applies to both the source of information (“confidential sources”) and to “unpublished information” such as notes, out-takes, unpublished photographs and tapes.

II. Requested Records

Pursuant to the FOIA, I, on behalf of the Reporters Committee, request access to and copies of the following records:

1. All records mentioning or referring to Bryan Carmody. A signed DOJ-361 form from Mr. Carmody is attached hereto.
2. All records, including email correspondence, text messages, and other electronic messages, that include the term “Carmody” (case insensitive) and any of the following keywords (case insensitive):
 - a. Shield
 - b. Privacy Protection Act
 - c. PPA
 - d. Leak
 - e. Leaks
 - f. Subpoena
 - g. Newsgathering
 - h. Question
 - i. Questions
 - j. Questioning
 - k. Media
 - l. Warrant
 - m. Search
 - n. Seize
 - o. Seizure;
3. All communications, including email correspondence, text messages, and other electronic messages between any individual at the FBI and
 - a. the San Francisco Police Department
 - b. the District Attorney’s Office for the City and County of San Francisco
 - c. the San Francisco Sheriff’s Department
 - d. the California Bureau of Investigation
 - e. the California Office of the Governor, and/or
 - f. the California Highway Patrol,that mention, refer to, or discuss Bryan Carmody;

4. All records mentioning, referring to, or constituting the memorandum sent from the United States Attorney's Office for the Northern District of California seeking approval for questioning, arresting, or charging Bryan Carmody.

RCFP requests that the FBI's San Francisco Field Office be searched in responding to this request, in addition to all other locations likely to contain responsive records.

Please note that email correspondence, as referred to in this request, includes the entire email chain in which the FBI is a sender or recipient (including a "cc" or "bcc") of one or more emails in the chain. This request also includes any email attachments. This request also includes official communications sent or received using any non-governmental email account or other electronic messaging account.

III. Fees and Fee Categorization

As a representative of the news media, the Reporters Committee is only required to pay for the direct cost of duplication after the first 100 pages. 5 U.S.C. § 552(a)(4)(A)(ii)(II). This information is being sought on behalf of the Reporters Committee for *inter alia*, analysis and free dissemination to the general public through multiple avenues, including RCFP's website,⁷ social media accounts,⁸ and email newsletter.⁹

In the event that there are duplication fees for responding to this request, the Reporters Committee is willing to pay up to \$50. Please let me know in advance if fees for responding to this request will exceed that amount before proceeding.

IV. Conclusion

If this request is denied in whole or part, please justify all such denials by reference to specific exemptions and explain why the FBI "reasonably foresees that disclosure would harm an interest" protected by that exemption or why "disclosure is prohibited by law[.]" 5 U.S.C. § 552(a)(8). Please also ensure that all segregable portions of otherwise exempt material are released.

If you have any questions regarding this request, please feel free to contact me at (202) 795-9308. Thank you in advance for your assistance.

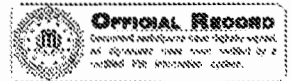
Sincerely,
Adam A. Marshall
Knight Foundation Litigation Attorney
Reporters Committee for Freedom of the Press
amarshall@rcfp.org

⁷ <https://www.rcfp.org/>.

⁸ See, e.g., <https://twitter.com/rcfp> (~16.3 thousand followers as of May 14, 2019); <https://www.facebook.com/ReportersCommittee/> (8,148 "likes" as of May 14, 2019).

⁹ <https://rcfp.us15.list-manage.com/subscribe?u=682100887bbcff066b451132&id=8f701b284f>.

EXHIBIT 4



FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/10/2019b6 -1
b7C -1

On May 10, 2019 at approximately 8:30am Special Agents (SAs) [redacted] [redacted] interviewed Bryan Carmody, date of birth (DOB) Fed. R. Civ. P. 5.2, at his residence, 794 45th Ave, San Francisco, California. The interview was conducted while San Francisco Police officers were conducting a search warrant at the residence. Carmody was detained/hand cuffed during the interview. Agents helped Carmody get clothes on prior to the interview. After being advised of the identity of the interviewing Agent and the nature of the interview Carmody provided the following information:

Carmody stated he wanted to speak with his lawyer before answering any questions. (*Agent note: Agents provided some background on the investigation and reasons why cooperation would be beneficial.*) Carmody stated that law enforcement was raiding the home of a reporter and that it would be national news. Carmody repeated that he wanted to speak with his lawyer and make phone calls.

The interview concluded at approximately 8:40am.

Investigation on 05/10/2019 at San Francisco, California, United States (In Person)
File # [redacted] Date drafted 05/10/2019
by [redacted]

b7A -1

b6 -1
b7C -1

EXHIBIT 5

REPORTERS COMMITTEE

FOR FREEDOM OF THE PRESS

1156 15th Street NW, Suite 1020
Washington, DC 20005
(202) 795-9300 | www.rcfp.org
Bruce D. Brown, Executive Director

STEERING COMMITTEE

STEPHEN J. ADLER

Reuters

J. SCOTT APPLEWHITE

The Associated Press

WOLF BLITZER

CNN

DAVID BOARDMAN

Temple University

MASSIMO CALABRESI

Time Magazine

MANNY GARCIA

USA Today Network

EMILIO GARCIA-RUIZ

The Washington Post

JOSH GERSTEIN

Politico

ALEX GIBNEY

Jigsaw Productions

SUSAN GOLDBERG

National Geographic

JAMES GRIMALDI

The Wall Street Journal

LAURA HANDMAN

Davis Wright Tremaine

DIEGO IBARGÜEN

Hearst

KAREN KAISER

The Associated Press

DAVID LAUTER

Los Angeles Times

DAHLIA LITHWICK

Slate

MARGARET LOW

The Atlantic

JANE MAYER

The New Yorker

COLLEEN MCCAIN NELSON

The McClatchy Company

MAGGIE MULVIHILL

Boston University

JAMES NEFF

The Philadelphia Inquirer

NORMAN PEARLSTINE

The Los Angeles Times

CAROL ROSENBERG

The New York Times

THOMAS C. RUBIN

Quinn Emmanuel

CHARLIE SAVAGE

The New York Times

BEN SMITH

BuzzFeed

JENNIFER SONDAG

Bloomberg News

ADAM SYMSON

The E.W. Scripps Company

PIERRE THOMAS

ABC News

SAUNDRA TORRY

Freelance

VICKIE WALTON-JAMES

NPR

JUDY WOODRUFF

PBS/The NewsHour

SENIOR ADVISORS

CHIP BOK

Creators Syndicate

JOHN C. HENRY

Freelance

TONY MAURO

National Law Journal, ret.

ANDREA MITCHELL

NBC News

PAUL STEIGER

ProPublica

Adam A. Marshall

Reporters Committee for Freedom of the Press

1156 15th St. NW, Suite 1020

Washington, DC 20005

amarshall@rcfp.org

San Francisco Police Department

Records Management

1245 3rd Street

San Francisco, CA 94158

VIA ONLINE PORTAL

March 4, 2020

RE: California Public Records Act and San Francisco Sunshine Ordinance Request

This letter constitutes a request under the San Francisco Sunshine Ordinance, Administrative Code § 67.1 *et. seq* and the California Public Records Act, § 6250 *et seq.*, and is submitted on behalf of the Reporters Committee for Freedom of the Press (“Reporters Committee” or “RCFP”) to the San Francisco Police Department (“SFPD”). The Reporters Committee is a nonprofit association dedicated to protecting First Amendment freedoms and the newsgathering rights of journalists.¹

I. Background

For nearly three decades, Bryan Carmody has worked in the bay Area as a journalist and videographer.² On May 10, 2019, San Francisco police searched Mr. Carmody’s home and office.³ A spokesman for the San Francisco Police Department said that a search warrant was granted by a judge and executed as part of an inquiry into the release of the “Adachi police report.”⁴ The “Adachi police report” is the police report concerning the death of San Francisco public defender Jeff Adachi earlier that year. During the search of Mr. Carmody’s home, two men who identified themselves as FBI agents tried to interview him.⁵

II. Requested Records

Pursuant to the San Francisco Sunshine Ordinance and the California Public Records Act, I, on behalf of the Reporters Committee, request access to and copies of all emails that were sent or received between May 11, 2019 and December 31, 2019 and that contain both “Carmody” and “FBI”.

¹ See generally www.rcfp.org.

² Amir Vera and Keith Allen, *San Francisco police seize equipment of freelance journalist who refused to identify a source*, CNN (June 11, 2019), <https://www.cnn.com/2019/05/14/media/california-journalist-equipment-seized/index.html>.

Laurel Wamsley, *San Francisco Police Raid Journalist's Home After He Refuses To Name Source*, NPR (May 13, 2019), <https://www.npr.org/2019/05/13/722745266/san-francisco-police-raid-journalists-home-after-he-refuses-to-name-source>.

⁴ *Id.*

⁵ *Id.*

III. Fees and Fee Categorization

As a representative of the news media, the Reporters Committee asks that fees associated with the processing of this records request be waived or reduced. *See N. Cty. Parents Org. v Dep't of Ed.*, 23 Cal. App. 4th 144, 148, 28 Cal. Rptr. 2d 359 (1994) (where court held agency had discretionary authority under the act to reduce or waive fee for public records).

This information is being sought on behalf of the Reporters Committee for *inter alia*, analysis and free dissemination to the general public through multiple avenues, including RCFP's website,⁶ social media accounts,⁷ and email newsletter.⁸

In the event that there are duplication fees for responding to this request, the Reporters Committee is willing to pay up to \$50. Please let me know in advance if fees for responding to this request will exceed that amount before proceeding.

IV. Conclusion

If this request is denied in whole or part, please justify all such denials by reference to specific exemptions. *See, e.g., Long Beach Police Officers Ass'n v. City of Long Beach*, 59 Cal. 4th 59, 67 (2014) (stating that exemptions are to be narrowly construed and public agencies bear the burden of proving that an exemption applies). Please also ensure that all segregable portions of otherwise exempt material are released per Cal. Gov't Code § 6253(a).

If you have any questions regarding this request, please feel free to contact me at (202) 795-9308. Thank you in advance for your assistance.

Sincerely,
Adam A. Marshall
Knight Foundation Litigation Attorney
Reporters Committee for Freedom of the Press
amarshall@rcfp.org

⁶ <https://www.rcfp.org/>.

⁷ *See, e.g.*, <https://twitter.com/rcfp> (~18.2 thousand followers as of Feb. 13, 2020); <https://www.facebook.com/ReportersCommittee/> (8,724 "likes" as of Feb. 13, 2020).

⁸ <https://rcfp.us15.list-manage.com/subscribe?u=682100887bbcff066b451132&id=8f701b284f>.

EXHIBIT 6

Fw: Warrant Service

Torres, Pilar (POL) <Pilar.Torres@sfgov.org>

Thu 12/19/2019 5:59 PM

To: Andraychak, Michael (POL) <michael.andraychak@sfgov.org>

Per your request,

This one appears to reference the quashed search warrant?

Lieutenant Pilar E. Torres #597
San Francisco Police Department
Southern Station
1251 3rd Street
San Francisco, Ca. 94158
Office- 415.575.6090
Cell- [REDACTED] 3/11

From: Eldridge, Michael P. (SF) (FBI) <mpeldridge@fbi.gov>

Sent: Friday, May 10, 2019 6:54 PM

To: Torres, Pilar (POL) <Pilar.Torres@sfgov.org>

Subject: Re: Warrant Service

Great to hear, thanks for the update Pilar. Sorry we weren't able to get a better result for you on our end, but thanks for letting us take a shot. I spoke with Joe a little earlier, but if you guys are all right with it, we were going to try to follow up with his attorney early next week.

If you need anything else from us, please let us know. We'll send over the report from today once it's finalized in our system.

Regards,

Mike

Michael Eldridge
Special Agent
FBI San Francisco
450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102

[REDACTED] 3/11

On May 10, 2019 5:24 PM, "Torres, Pilar (POL)" <Pilar.Torres@sfgov.org> wrote:
Mike,

We ended up at a secondary location where we met with success! He still would not give any additional information but we still have the digital media to scrub.

Thank you for you help!

Lieutenant Pilar E. Torres #597
San Francisco Police Department
Investigative Services Detail
1245 3rd Street
San Francisco, Ca. 94158
Desk- 415.882.8425
Cell- [REDACTED] 3/11

From: Eldridge, Michael P. (SF) (FBI) <mpeldridge@fbi.gov>
Sent: Thursday, May 9, 2019 6:57:10 PM
To: Torres, Pilar (POL)
Subject: Re: Warrant Service

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Got it, thanks Pilar. We'll see you tomorrow morning.

Regards,

Mike

Michael Eldridge
Special Agent
FBI San Francisco
450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102

[REDACTED] 3/11

On May 9, 2019 6:53 PM, "Torres, Pilar (POL)" <Pilar.Torres@sfgov.org> wrote:
Mike,

Please see the attached information.

[REDACTED]

Lieutenant Pilar E. Torres #597
San Francisco Police Department
Investigative Services Detail
1245 3rd Street
San Francisco, Ca. 94158
Desk- 415.882.8425



3/11

EXHIBIT 7

Fw: 190149152 / Carmody / SVRCFL Lab # SV-19-0033

Obidi, Joseph (POL)

Wed 12/4/2019 11:38 AM

To: Andraychak, Michael (POL) <michael.andraychak@sfgov.org>

Sgt. Joseph Obidi #2328
San Francisco Police Department
Investigations Bureau
850 Bryant Street, Room 525
San Francisco Ca 94103
415- [REDACTED]

This email is meant for only the intended recipient(s) of the transmission, and may be a communication privileged by law. If you have received this e-mail in error, any review, use, dissemination, distribution, or copying of this e-mail is strictly prohibited. Please notify us immediately of the error by return e-mail and please delete this message from your system. Thank you in advance for your cooperation.

From: Brian Rodriguez <brodriguez@rcfl.gov>

Sent: Monday, June 10, 2019 2:27 PM

To: Torres, Pilar (POL) <Pilar.Torres@sfgov.org>

Cc: Kwok, Sherman (SF) (FBI) <skwok2@fbi.gov>; Penni Price <pprice@fbi.gov>; Obidi, Joseph (POL) <Joseph.A.Obidi@sfgov.org>

Subject: Re: 190149152 / Carmody / SVRCFL Lab # SV-19-0033

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Hello Lt. Torres-

I'm touching base on this case again. I know you had some questions a week or two back regarding the disposition of the forensic images and our documentation. We are at a point where we must close this case if the exam is not going to continue or if no new legal authority will be supplied.

Do you want us to destroy the forensic images (copies) we have of the laptops, OR would you like us to close our case and give you the archive tape containing the images for a later disposition? Either way, it will be documented in a written report.

I am currently out of state, but SVRCFL Lab Director Sherman Kwok (CC'd) will be facilitating the closure of the case. If you have any questions, contact the lab main number at 650-289-3000.

Thanks for an expedited response on this!

-Brian

On May 28, 2019, at 12:29 PM, Brian Rodriguez <brodriguez@rcfl.gov> wrote:

Hi Joe-

In light of all the stuff going on with this case, we have not gone any further with this first request with the two laptops. All that happened here is that I forensically imaged both laptops and Penni prepared to process them. We stopped once we heard the evidence was being picked up. As you know, all submitted evidence was returned to SFPD on 5/20/19. Nothing at all was done on the second request (SV-19-0033-2) with the tower PC and loose HDDs - a written report is forthcoming detailing that.

I do have a question on this first request (with the two laptops)...since I forensically imaged both laptops, we have a couple of options:

- 1) Close our exam (which hasn't really started) and return the master copy tape (containing the forensic images of the laptops) along with a written report in case you/someone wants to examine these laptops for evidence at a later date.
- 2) Close our exam (which hasn't really started) and DESTROY the master copy tape (containing the forensic images of the laptops), which means the laptops can never be examined unless they are seized from the subject again.
- 3) Hold - since we have forensic images of the two laptops (only) and wait for further instruction to possibly examine them.

Please advise!

Thanks!

B-Rod

Sgt. Brian Rodriguez # 4075
San Francisco Police Department
Deputy Director / TFO - Silicon Valley Regional Computer Forensics Laboratory
Desk Phone (650) [REDACTED] / Cell Phone (415) [REDACTED]
brodriguez@rcfl.gov / brian.rodriquez@sfgov.org / brodriguez@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

EXHIBIT 8



LIVE TV



San Francisco police seize equipment of freelance journalist who refused to identify a source

By [Amir Vera](#) and [Keith Allen](#), CNN

Updated 10:15 AM ET, Tue June 11, 2019

(CNN) — Bryan Carmody was sleeping Friday when he woke to the sound of San Francisco police officers breaking down his security gate with a sledgehammer.

The northern California-based freelance journalist told CNN Monday the group of officers produced a search warrant to enter his residence.

For the next seven hours, Carmody said, he was handcuffed as officers seized his computers, cameras, phones and notebooks. Officers also searched Carmody's office away from his home. While he wasn't arrested, Carmody said officers gave him no indication of when his equipment would be returned.

"They took every digital photo I've ever taken, even family photos," Carmody said. "Basically, at this point, I'm out of business."

Carmody said in his 29 years of being a journalist, nothing like this has ever happened to him.

The raid of Carmody's home came after an April 11 conversation with officers in which Carmody refused to tell authorities how he obtained a confidential police report that included information about the February death of prominent San Francisco public defender Jeff Adachi, according to Carmody's attorney Thomas R. Burke. Carmody told officers he could not divulge his source, he said Monday.

Adachi, 59, was known for his dogged criticism of the police department, according to [CNN affiliate KPIX-TV](#). The coroner's office, KPIX reported, said Adachi died from a mix of alcohol consumption and cocaine.

Police refused to release the report or details behind Adachi's death, CNN affiliate KPIX reported. Police said releasing such details would "endanger the safety of a witness or other person involved in the investigation, or ... endanger the successful completion of the investigation or a related investigation."

Despite the police department's reluctance to release investigation information, details were leaked and made their way into news reports.

"The notion that I was running around hawking this (confidential police) document is wrong," Carmody told CNN. "The documents were part of a story, I sold a story. I give stations a heads up, that's how our agreement works."

Carmody also said that his reporting and distribution of the story did not arise out of any political agenda or a

grudge against the city of San Francisco or its police department.

His attorney demanded in a statement Monday that police return "these improperly seized materials, or, at a minimum, not review any materials."

"There is no conceivable basis here for the SFPD to claim any 'exigency' exception to bypass these well-established protections for journalists like Mr. Carmody," Burke said.

Burke said he spoke with a San Francisco officer twice Friday and to the department's spokesperson Saturday. He says he hasn't received a response from the department concerning the return of his client's possessions. He did, however, reach out to the city's district attorney's office and was told the city's top prosecutor had not reviewed any search warrants executed at Carmody's home or office, he said.

Burke said if the department doesn't return Carmody's possessions by Tuesday, then he'll "seek relief from the court."

Police: 'We are committed to maintaining the public's trust'

The San Francisco Police Department issued a statement Monday saying the search warrant was granted by a judge and done as part of a criminal investigation into the "illegal release of the confidential Adachi police report and subsequent sale to members of the media."

"The citizens and leaders of the City of San Francisco have demanded a complete and thorough investigation into this leak, and this action represents a step in the process of investigating a potential case of obstruction of justice along with the illegal distribution of confidential police material," the statement read. "We are committed to maintaining the public's trust, investigating any allegations of misconduct and holding those responsible for such acts accountable."

The Electronic Frontier Foundation, a nonprofit that advocates for civil liberties in the digital age and is based in San Francisco, also released a statement through David Greene, the organization's civil liberties director and senior staff attorney. Greene said the police department's statement fails to address the illegality of its search warrant.

"California law has an absolute ban on the use of a search warrant to obtain materials in possession of a journalist," Greene said. "So when a warrant is used to obtain materials from a journalist, our first thought is that is against the law."

Greene added there are no exceptions no matter the investigation.

"That a judge signed the search warrant means either the judge made an error or maybe the police did not inform the court that the person was a journalist," he said.

Journalism organizations condemn raid

The [Society of Professional Journalists Northern California](#) chapter (SPJ NorCal) and the [Committee to Protect Journalists](#), an independent, nonprofit organization that promotes press freedom worldwide, both released statements condemning Friday's raid.

"California's Shield Law protects journalists from being held in contempt for refusing to disclose their sources' identities and other unpublished/unaired information obtained during the news gathering process," SPJ NorCal said. "That this search was carried out weeks after Carmody declined a request from San Francisco police to divulge his sources shows an alarming disregard for the right to gather and report on information."

SPJ NorCal's statement also said that while there may be questions around the reporting of Adachi's death, "the seizure of any journalist's notes or other reporting materials sets a dangerous precedent."

"An attack on the rights of one journalist is an attack on the rights of all journalists," the statement read. "San Francisco's wrongful actions against Carmody threaten fundamental journalistic freedoms which are vital to a functioning democracy."

The Committee to Protect Journalists "called on authorities to immediately return electronic devices, documents, and other seized property."

Carmody on Monday expressed his gratitude to his supporters.

"The outpouring of support that I've gotten from friends and colleagues and people I don't know -- big reporters that I would never cross paths with," he said. "It's just really nice to have these people reaching out and supporting me and its helping me get through this."

CNN's Augie Martin and Chris Boyette contributed to this report.



- US
- World
- Politics
- Business
- Opinion
- Health
- Entertainment
- Tech
- Style
- Tennis

Travel

Sports

Videos

Coupons

More

Weather



FOLLOW CNN BUSINESS



Most stock quote data provided by BATS. Market indices are shown in real time, except for the DJIA, which is delayed by two minutes. All times are ET. Disclaimer. Morningstar: Copyright 2018 Morningstar, Inc. All Rights Reserved. Factset: FactSet Research Systems Inc. 2018. All rights reserved. Chicago Mercantile Association: Certain market data is the property of Chicago Mercantile Exchange Inc. and its licensors. All rights reserved. Dow Jones: The Dow Jones branded indices are proprietary to and are calculated, distributed and marketed by DJI Opco, a subsidiary of S&P Dow Jones Indices LLC and have been licensed for use to S&P Opco, LLC and CNN. Standard & Poor's and S&P are registered trademarks of Standard & Poor's Financial Services LLC and Dow Jones is a registered trademark of Dow Jones Trademark Holdings LLC. All content of the Dow Jones branded indices Copyright S&P Dow Jones Indices LLC 2018 and/or its affiliates.

[Terms of Use](#) [Privacy Policy](#) [Do Not Sell My Personal Information](#) [AdChoices](#) [About Us](#) [CNN Studio Tours](#)

[CNN Store](#) [Newsletters](#) [Transcripts](#) [License Footage](#) [CNN Newsource](#) [Sitemap](#)

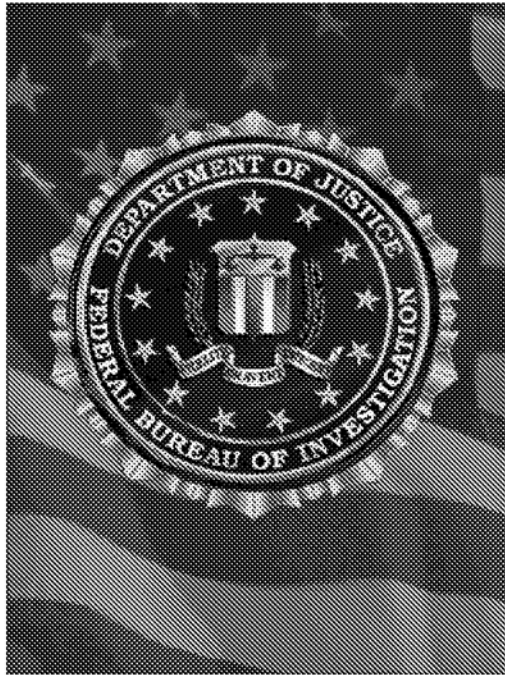
© 2020 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.
CNN Sans ™ & © 2016 Cable News Network.

EXHIBIT 9

UNCLASSIFIED
Records Management Policy Guide

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-29-2015 BY J89J28T90 NSICG

Records Management Policy Guide



Federal Bureau of Investigation

Records Management Division

0769PG

June 04, 2015

Revised: 07/01/2015

UNCLASSIFIED

UNCLASSIFIED
Records Management Policy Guide

General Information

Questions or comments pertaining to this policy guide can be directed to:
Federal Bureau of Investigation Headquarters (FBIHQ), Records Management Division (RMD)
Records Policy and Administration Section (RPAS), Policy, Analysis, and Compliance Unit
(PACU)

Supersession Information

See Appendix E of this policy guide for supersession information.

This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit or individual(s) listed above in the general information section of this policy guide.

UNCLASSIFIED

Records Management Policy Guide

Table of Contents

1. Introduction.....	1
1.1. Overview	1
1.2. Recordkeeping Requirements Policy	1
1.3. Purpose of Records Management.....	1
1.4. Benefits of Good Recordkeeping	2
1.5. Intended Audience.....	2
2. Roles and Responsibilities	3
2.1. Director's Office	3
2.1.1. The Director	3
2.2. Records Management Division	3
2.2.1. Assistant Director.....	3
2.2.2. RMD Front Office.....	3
2.2.3. Records Policy and Administration Section (RPAS).....	4
2.2.4. Records Automation Section	4
2.2.5. Record/Information Dissemination Section (RIDS).....	5
2.2.6. National Name Check Program Section (NNCP).....	5
2.3. Office of the General Counsel.....	5
2.3.1. Employment Law Units	5
2.3.2. Discovery Coordination and Policy Unit	5
2.4. Information and Technology Branch	6
2.5. Inspection Division (INSD)	6
2.6. Criminal Justice Information Services (CJIS) Division.....	6
2.7. All FBIHQ Divisions/Field Offices/Legal Attaché (Legat) Offices	6
2.7.1. Assistant Directors, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), Chief Division Counsels (CDC), and other Supervisory Personnel	6
2.7.2. Records Liaison	6
2.8. All FBI Personnel.....	7
3. Policies.....	9
4. Procedures and Processes.....	10
4.1. Overview	10

UNCLASSIFIED

Records Management Policy Guide

4.2.	Definition of a Record	10
4.2.1.	Questions to Ask in Determining Record Status	10
4.3.	Nontransitory Record (Needed for More Than 180 Days)	11
4.4.	Transitory Record (Needed For 180 Days or Less)	11
4.5.	Nonrecord	12
4.6.	Personal Papers	12
4.7.	Records Creation and Receipt (Phase 1: Records Life Cycle)	12
4.7.1.	Records Created by the FBI	12
4.7.2.	Supervisory Approval of Administrative Records	13
4.7.3.	Records Received from Non-FBI Personnel or Organizations	13
4.8.	Records Maintenance and Use (Phase 2: Records Life Cycle)	13
4.8.1.	Records Requirements	13
4.8.2.	Records Systems	14
4.8.3.	Central Recordkeeping System–Sentinel	14
4.8.4.	Indexing Records	14
4.8.5.	Case Management	16
4.8.6.	Managing Administrative Records	16
4.8.7.	Storing Paper Records	17
4.8.8.	Transferring Records	18
4.8.9.	Retrieving Records	18
4.8.10.	Retrieving Information from Records	19
4.8.11.	Electronic Recordkeeping Certification (ERKC) Program	20
4.8.12.	Metadata	21
4.8.13.	Data Backup Retention	21
4.8.14.	Capturing and Preserving Electronic Records	22
4.8.15.	Electronic Mail	22
4.8.16.	Nontransitory Record E-mails (Needed for More Than 180 Days)	23
4.8.17.	Filing Nontransitory Record E-Mails in Sentinel	24
4.8.18.	Transitory Record E-Mails (Needed 180 Days or Less)	24
4.8.19.	Nonrecord E-Mails	25
4.8.20.	Web Sites	26
4.8.21.	Electronic Information Sharing Technologies	26

UNCLASSIFIED

Records Management Policy Guide

4.8.22.	Imaged Records and Standards for Scanned Documents.....	26
4.8.23.	Standards for Photographic Records	27
4.8.24.	Restrictions on FBI Records	27
4.9.	Records Disposition (Phase 3: Records Life Cycle)	28
4.9.1.	Modification and Destruction of Records.....	28
4.9.2.	Records Retention Plan.....	28
4.9.3.	Purpose of Record Retention Plan	28
4.9.4.	Records Not Included in the Records Retention Plan.....	29
4.9.5.	Applying the Records Retention Plan.....	29
4.9.6.	Preservation of Nontransitory Records with Permanent Retention	29
4.9.7.	Disposition of Nontransitory Records with Temporary Retention	29
4.9.8.	Disposition of Transitory Records	30
4.9.9.	Disposition of Investigative and Intelligence Records	30
4.9.10.	Disposition of Records Pertaining to Evidence.....	30
4.9.11.	Disposition of Administrative Records: Classifications 319 and 67Q	30
4.9.12.	Disposition of Personnel-Related Records.....	30
4.9.13.	Disposition of Draft Documents	31
4.9.14.	Disposition of Personal Files	31
4.9.15.	Disposition of Nonrecord Materials	31
4.10.	Orphaned Records	31
4.11.	Reporting Missing Files and Serials.....	32
4.11.1.	Reporting Missing Files and Serials Subject to Legal Hold	32
4.12.	Expungement of FBI Records	32
4.12.1.	Court-Ordered Expungements.....	32
4.12.2.	Privacy Act Expungements	32
4.13.	Unauthorized Destruction of FBI Records	32
4.14.	Damage to FBI Records	33
4.15.	RMD Records Disaster Team.....	33
4.16.	Vital Records	33
5.	Summary of Legal Authorities	34

UNCLASSIFIED

Records Management Policy Guide

List of Appendices

Appendix A: Final Approvals A-1
Appendix B: Sources of Additional Information B-1
Appendix C: Acronyms C-1
Appendix D: Contact Information D-1
Appendix E: Supersessions E-1

UNCLASSIFIED
Records Management Policy Guide

1. Introduction

1.1. Overview

All Federal Bureau of Investigation (FBI) personnel create, maintain, and use FBI records. It is therefore critical that FBI personnel understand the policies and procedures governing the FBI's Records Management Program.

1.2. Recordkeeping Requirements Policy

The FBI is required by law (Title 44 United States Code [U.S.C.] Chapter 31) to establish and implement agencywide programs to identify, develop, issue, and periodically review recordkeeping requirements for records of all agency activities at all levels and locations and across all media.

Recordkeeping requirements provide the regulatory means to implement adequate and proper documentation requirements. They provide specific instructions developed by subject matter experts for the collection of information or the maintenance of documents for FBI functions or programs. Recordkeeping requirements can range from broad, governmentwide guidance found in statutes and regulations to office-specific instructions on the preparation of a certain report. Each FBI Headquarters (FBIHQ) division, field office (FO), and legal attaché (Legat) office must, with the assistance of the Records Management Division (RMD), incorporate applicable laws, regulations, or other requirements pertinent to the organization's program responsibilities into recordkeeping requirements for the documentation of its programs.

1.3. Purpose of Records Management

The RMD's mission is to ensure that the right records are created, made available to the right people at the right time and for the right reasons, and disposed of, according to the disposition authorities approved in the FBI Records Retention Plan.

FBI records must be adequate, authentic, legally sufficient, and secure to ensure all FBI legal, fiscal, administrative, and business needs are met. Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, effectively perform its critical missions, or efficiently conduct its day-to-day business.

The FBI is committed to ensuring its Records Management Program:

- Supports law enforcement and national security operations.
- Facilitates documentation of official decisions, policies, activities, and transactions.
- Facilitates timely retrieval and sharing of needed information.
- Ensures business continuity.
- Controls the creation and growth of FBI records.

UNCLASSIFIED

Records Management Policy Guide

- Reduces operating costs by managing records according to the FBI's business needs and by encouraging appropriate disposition practices pursuant to the FBI Records Retention Plan.
- Improves efficiency and productivity through effective records storage and retrieval methods.
- Ensures compliance with applicable laws and regulations.
- Safeguards the FBI's mission-critical information.
- Preserves the FBI's history.
- Implements technology to support records management activities.

1.4. Benefits of Good Recordkeeping

Adequate and proper recordkeeping ensures that information is available to safeguard the legal and financial rights of the federal government, the FBI, and persons directly affected by the FBI's activities. It ensures the accountability of the FBI to the President of the United States, the United States Congress, the United States courts, and the American people. Additionally, it supports the administration of justice and effective law enforcement and national security operations throughout the FBI's worldwide operations.

Conversely, deficiencies in the management of FBI records impair the FBI's ability to carry out its essential functions and may result in inquiries and investigations by oversight bodies, as well as adverse public perceptions of the FBI's efficiency, accountability, and management. Records mismanagement can also result in adverse judicial rulings during the discovery process.

1.5. Intended Audience

This policy guide (PG) applies to all FBI personnel. The term "FBI personnel" includes any individual employed by, detailed to, or assigned to the FBI, including members of the armed forces; experts or consultants to the FBI; industrial or commercial contractors, licensees, certificate holders, or grantees of the FBI, including all subcontractors; personal service contractors of the FBI; or any other category or person who acts for, or on behalf of, the FBI, as determined by the FBI Director.

UNCLASSIFIED
Records Management Policy Guide

2. Roles and Responsibilities

2.1. Director's Office

2.1.1. The Director

The Director of the FBI:

- Ensures that records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions are created and preserved.
- Has delegated records management authority to the assistant director (AD) of RMD.

2.2. Records Management Division

2.2.1. Assistant Director

The AD of RMD will:

- Serve as the FBI records officer, establishing and overseeing a comprehensive FBI-wide Records Management Program.
- Oversee the management of FBI records throughout their life cycles, including records creation, maintenance and use, and disposition of recorded information in all formats.
- Appoint an FBI-wide vital records officer who oversees the FBI's Vital Records Program, in accordance with the *Vital Records Policy Guide (0794PG)*.

2.2.2. RMD Front Office

2.2.2.1. Training Services Unit (TSU)

TSU will:

- Provide records management training and guidance to all FBIHQ divisions, FOs, Legats, groups, and organizations throughout the FBI.
- Ensure all FBIHQ divisions, FOs, and Legats are informed of, and trained in, their responsibilities related to the creation, maintenance, and disposition of FBI records.
- Provide guidance and training to FBI personnel on storing and securing records to reduce the risk of damage and loss of information.
- Provide guidance and training to FBI personnel on saving or mitigating the loss of information in records and restoring original records to a useful condition, if possible.

UNCLASSIFIED

Records Management Policy Guide

2.2.3. Records Policy and Administration Section (RPAS)

RPAS will:

- Collaborate with the Records Automation Section (RAS) in the development of records management policies for electronic media.
- Work with the Information and Technology Branch (ITB) and RAS to manage and maintain a policy-compliant records management application (RMA) as part of the FBI's enterprise architecture.
- Establish and disseminate policies and procedures governing the creation, organization, maintenance, use, preservation, disposition, and transfer of all FBI records, regardless of medium or format.
- Conduct periodic FBI records reviews and evaluations to ensure compliance with records management policies and procedures.
- Develop and maintain a network of records liaisons in all FBIHQ divisions, FOs, and Legats, and ensure they receive adequate training to carry out their responsibilities.
- Manage and regularly update the FBI Records Retention Plan and coordinate requests for, and receipt of, all disposition authorities with the National Archives and Records Administration (NARA).
- Manage the storage and maintenance of records.
- Manage the transfer of permanent records to NARA and the destruction of temporary records that have met their retention periods.
- Implement legal holds received from the Office of the General Counsel (OGC).
- Process records modification, permanent charge outs, and expungement requests.
- Conduct and manage FBI-wide record inventories.
- Oversee the storage and maintenance of records in FBIHQ storage areas and advise FBI personnel regarding their records storage and maintenance activities.

2.2.4. Records Automation Section

RAS will:

- Collaborate with RPAS in the development of records management policies for electronic media.
- Provide document conversion services (both imaging and optical character recognition) through the Document Conversion Laboratory (DocLab).
- Conduct electronic recordkeeping certification (ERKC) reviews of all information systems used in the conduct of FBI activities.
- Work with the ITB and RPAS to manage and maintain a policy-compliant RMA as part of the FBI's enterprise architecture.

UNCLASSIFIED

Records Management Policy Guide

- Plan and assist with the development, management, and maintenance of the enterprise RMA, in coordination with information technology (IT) divisions, offices, and groups.
- Ensure proper records management requirements are incorporated into the design and deployment of new information and knowledge management systems, which include monitoring system compliance with records management requirements.
- Coordinate and guide the incorporation of electronic recordkeeping (ERK) requirements into IT system development.
- Coordinate and guide the incorporation of recordkeeping requirements into the enterprise RMA file plan as records disposition schedules are updated or added.

2.2.5. Record/Information Dissemination Section (RIDS)

RIDS will:

- Plan, develop, direct, and manage responses to requests for FBI information in accordance with the requirements of the Freedom of Information Act (FOIA) (5 U.S.C. Section [§] 552); the Privacy Act of 1974 (5 U.S.C. § 552a); [FOIA] Executive Order (EO) 13392, *Improving Agency Disclosure of Information*; EO 13526, *Classified National Security Information*; and other applicable Presidential, Attorney General, and FBI policies, procedures, and other mandates, judicial decisions, and Congressional directives.
- Coordinate with OGC's Discovery Coordination and Policy Unit (DCPU) regarding specific FOIA requests.
- Manage the prepublication review program.

2.2.6. National Name Check Program Section (NNCP)

The NNCP will research, analyze, and disseminate information from FBI records, according to the requirements of the NNCP, in order to respond to requests from customer agencies (EO 10450).

2.3. Office of the General Counsel

2.3.1. Employment Law Units

The Employment Law Units will assist with the expungement of information from employee personnel records.

2.3.2. Discovery Coordination and Policy Unit

DCPU will:

- Set the scope, duration, and other characteristics of legal holds.
- Notify FBI personnel of their legal hold obligations.
- Notify FBI personnel of legal hold rescissions.

UNCLASSIFIED

Records Management Policy Guide

- Assist FBI personnel with the adjudication and dissemination of record information.

2.4. Information and Technology Branch

The ITB will work with RMD, in coordination with the OGC, to plan and deploy a legally compliant RMA as part of the FBI's enterprise architecture.

2.5. Inspection Division (INSD)

INSD will:

- Monitor records management compliance in FBI FOs, using records review results provided by RMD's RPAS.
- Coordinate with RPAS's Policy, Analysis, and Compliance Unit (PACU) to conduct focused records reviews, as appropriate.

2.6. Criminal Justice Information Services (CJIS) Division

CJIS will send record modifications and expungement requests to the RMD's RPAS.

2.7. All FBIHQ Divisions/Field Offices/Legal Attaché Offices

2.7.1. Assistant Directors, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), Chief Division Counsels (CDC), and other Supervisory Personnel

ADs, SACs, ADICs, CDCs, and other supervisory personnel will:

- Appoint records liaisons to assist RMD in the development and implementation of records management policies and procedures.
- Ensure their respective FBIHQ divisions, FOs, and Legats comply with the RMD's policies by creating, approving, and maintaining adequate and proper documentation of all official programs and activities, including properly indexing in Sentinel or other electronic recordkeeping systems when appropriate.
- Provide resources and time to enable FBIHQ division, FO, and Legat personnel to participate in and complete records management requirements and training.
- Appoint FBIHQ division/FO/Legat vital records officers to work with the FBI-wide vital records officer to identify vital records, in accordance with the Vital Records Policy Guide (0794PG).

2.7.2. Records Liaison

The records liaison will:

- Represent an FBIHQ division, an FO, or a Legat by coordinating with RMD on all records management policies, procedures, and programs.
- Understand records management concepts and federal records management laws and regulations.

UNCLASSIFIED

Records Management Policy Guide

- Review proposed records management policies within an FBIHQ division, an FO, or a Legat, and provide coordinated review responses to the RMD.
- Oversee the creation and maintenance of records in FBIHQ divisions, FOs, or Legats, and advise FBI personnel in their respective divisions, FOs, and Legats on FBI recordkeeping requirements.
- Monitor records destruction and records transfers to ensure compliance, in coordination with RPAS's Records Disposition Unit (RDU), with any legal holds issued by OGC.
- Provide training on records management policies and procedures, in coordination with RMD's TSU.
- Coordinate with RMD to assist with the resolution of issues involving FBIHQ division, FO, and Legat files.
- Oversee continued inventory of paper records.
- Conduct periodic records audits and inventories, in coordination with RPAS.
- Report promptly to the program manager, Records Protection and Recovery Program, about damage to records.
- Report missing hard-copy case files and serials promptly to RPAS's RDU and for classified material, to the division and/or chief security officer (CSO) via the Security Incident Reporting System (SIRS).
- Report missing hard-copy case files and serials that are subject to legal hold promptly to OGC's DCPU. Report missing classified material to the division and/or CSO via SIRS system owners.

Systems owners will coordinate with RAS to ensure the ERKC process is complete and all documentation is accurate and accessible.

2.8. All FBI Personnel

All FBI personnel will:

- Create and maintain adequate, complete, accurate, and proper documentation of FBI programs, investigations, activities, decisions, and transactions.
- Ensure the records they create and/or maintain are filed appropriately in an approved central recordkeeping system, such as Sentinel, and are properly indexed when appropriate.
- Ensure all records made or received while in the FBI's service have been properly recorded or properly and legally disposed of prior to separation from FBI service, in accordance with approved retention schedules.
- Cooperate with FBIHQ division, FO, and Legat records liaisons in the creation, maintenance, and disposition of FBI records.

UNCLASSIFIED

Records Management Policy Guide

- Ensure all deletion, destruction, or removal of FBI records complies with policies and procedures established by RMD.
- Comply with legal hold obligations and rescissions.

UNCLASSIFIED

Records Management Policy Guide

3. Policies

RMD establishes the requirements, procedures, and policies necessary to ensure FBI personnel manage records effectively to meet the FBI's business needs and to comply with applicable laws and regulations. This PG sets forth those requirements and procedures.

All FBI personnel must comply with the policies and procedures contained in this PG.

UNCLASSIFIED
Records Management Policy Guide

4. Procedures and Processes

4.1. Overview

Records management policies and procedures apply to each phase of a record's life cycle:

- Phase 1: Creation and/or receipt (see subsection 4.7.)
- Phase 2: Maintenance and use (see subsection 4.8.)
- Phase 3: Disposition (see subsection 4.9.)

In order to determine what policies and procedures apply to each phase of a record's life cycle, it must first be determined what kind of information is at issue: a record (nontransitory or transitory), a nonrecord, or a personal paper. The *Records Management User Manual* (RM User Manual) provides detailed information and guidance about specific records management procedures to supplement the policies and procedures outlined in this section.

4.2. Definition of a Record

The Federal Records Act of 1950 (see 44 U.S.C. § 3301), as amended, defines records as:

All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. Records do not include library or museum material made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved for convenience. Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

Specific mediums, platforms, and technologies change over time; however, the determination about what constitutes a record remains the same: it is based on content, not form. Communications using advanced electronic tools and media may be records, depending on their content. This PG applies to all records, regardless of physical form or characteristics.

FBI recordkeeping has evolved from paper-intensive records and information management systems to paperless records and electronic information management systems. Today, the FBI's official recordkeeping system is Sentinel, an electronic information management system. All electronic information management systems within the FBI containing records must comply with the policies and procedures governing the management of FBI records.

4.2.1. Questions to Ask in Determining Record Status

A document, regardless of medium, is considered a record if it contains information and is:

- Required to be documented by law, regulation, policy, or an established business practice applicable to the FBI.

UNCLASSIFIED

Records Management Policy Guide

- Pertinent to an FBI investigation (including assessments) or intelligence-gathering activities.
- Reasonably necessary to protect the rights of the government or of an individual affected by government action.
- Reasonably necessary to document or explain the basis for a significant action or decision involving the exercise of government authority.
- Needed to conduct government business effectively.
- Necessary to document other significant operations or administrative matters. Examples include changes in the FBI's organizational structure, changes in FBI-wide or FBIHQ division policies, accomplishment of an FBI mission responsibility, an expenditure of funds, a disposition of FBI property, and compliance or noncompliance with a legal obligation.

4.3. Nontransitory Record (Needed for More Than 180 Days)

A nontransitory record is a record needed for more than 180 days that has one or more of the following characteristics: (1) it provides substantive documentation of the FBI's policies and actions, (2) it contains important and/or valuable evidentiary information, and/or (3) it is required to be maintained by law or regulation. A nontransitory record may have a permanent or temporary retention requirement.

A nontransitory record with a permanent retention period is a record appraised by NARA as having sufficient historical or other value to warrant continued preservation beyond the time the record is needed for an agency's administrative, legal, or fiscal purpose. A permanent, nontransitory record will be transferred to, and preserved as part of, the National Archives of the United States after its usefulness to the FBI has ceased.

Examples of permanent, nontransitory records include policy files, exceptional case files, and files pertaining to the FBI's "Ten Most Wanted Fugitives." Exceptional case files document the FBI's investigation of significant individuals, events, organizations, precedent-setting programs, unusual investigative methods, and landmark legal cases involving FBI investigations. Additional information about permanent, nontransitory records is available on [RDU's](#) Intranet page.

A nontransitory record with a temporary retention period is a record that NARA has determined to be disposable after a specified period of time or after a specific event has occurred. This period may be for one year, or it could span decades. A temporary, nontransitory record has no continuing value after its usefulness to the FBI has ceased.

4.4. Transitory Record (Needed For 180 Days or Less)

A transitory record is a record that has only minimal documentary or evidentiary value and is needed for 180 days or less. Transitory records may include:

- Routine information or publications, working drafts, routine office management documentation, suspense and tickler file notices, and other records that do not serve as the basis for official actions, such as notices of holidays, charitable events, and the like.

UNCLASSIFIED**Records Management Policy Guide**

- Originating office copies of letters of transmittal that do not add any information already contained in the transmitted material.
- Records documenting routine activities and containing no substantive information, such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling-related activities.
- Routine communications, such as reminders of existing policies, work-related guidance, and meeting notices.
- Drafts of, or comments on, proposed policies or actions that are not considered or submitted for consideration by the approving authorities.
- “To-do” lists.

4.5. Nonrecord

A nonrecord is any material that does not meet the statutory definition of a record. As set forth in 44 U.S.C. § 3301, examples of nonrecord materials include:

- Library materials made or acquired and preserved solely for reference or exhibition purposes.
- Stocks of publications or unprocessed blank forms.
- Extra copies of documents preserved only for convenience of reference.

Note: Not all copies are nonrecord material. Copies of records may be used for different purposes within the FBI, and they may take on record status. For example, copies of other government agency (OGA) records may be maintained by the FBI as records. A nonrecord copy may also become a transitory record or a nontransitory record if substantive notes or comments are added to the document.

4.6. Personal Papers

Personal papers are materials that belong to an individual and are not used to conduct FBI business. They are primarily personal in nature and may be in any format or medium. An example of personal papers includes an employee’s copy of his or her Standard Form (SF)-50 (“Notification of Personnel Action”). It is important to note that if a document contains both record and personal information, the document must be treated as a record.

4.7. Records Creation and Receipt (Phase 1: Records Life Cycle)

Under the Federal Records Act, every federal agency is required to make and preserve records containing adequate and proper documentation of its organization, functions, policies, procedures, and essential transactions. See 44 U.S.C. Chapters 29, 31, and 33.

4.7.1. Records Created by the FBI

Every employee, FBIHQ division, FO, and Legat has the responsibility to adequately document activities, decisions, policies, and transactions conducted to further the FBI’s mission and to do so according to FBI policies. Documentary materials created in accordance with this responsibility are records.

UNCLASSIFIED

Records Management Policy Guide

Only FBI employees may approve official Bureau records. Policy Directive (PD) 0115D, *Approval Authority for Official Bureau Records*, contains additional information.

4.7.2. Supervisory Approval of Administrative Records

FBIHQ divisions, FOs, and Legats are responsible for establishing procedures clearly defining what administrative documents require supervisory approval prior to importing and serializing them to administrative case files. Unless specifically designated, supervisory approval is not required for importing and serializing administrative records. When supervisory approval is required, FBIHQ divisions, FOs, and Legats must establish clearly defined procedures for obtaining required signatures that will not impede the timely serialization of records in the administrative case file.

Supervisors are responsible for making sure staff receives training to ensure documentation requirements are followed. Users are responsible for obtaining supervisory approval of division documents that require such approval and for obtaining this approval prior to importing and serializing them in administrative case files.

The only exemption to this procedure is for documents imported through Sentinel's workflow by those individuals who do not have supervisory functionality. In those instances, when adding administrative documents, the creator can make himself or herself the approver and should do so on those administrative-type documents that the creator's particular office has authorized for self-approval.

4.7.3. Records Received from Non-FBI Personnel or Organizations

Documents, databases, and other information received by the FBI that the FBI must or does take action in the course of its routine duties and responsibilities are FBI records, even though non-FBI personnel or other organizations created them. Examples of these types of records include electronic mail (e-mail) or facsimiles (fax).

An exception to the above is non-FBI-generated, evidentiary material seized by the FBI or its law enforcement partners acquired through court order, warrant, federal grand jury or administrative subpoena or voluntarily provided in the course of an investigation of a particular case or intelligence assessment. This material is treated as evidentiary property and is managed under a different set of rules and regulations than those defined in this PG. Note, however, the "Evidence Chain-of-Custody" (FD-1004) form documents the management of evidence, and it is a record. For more information regarding evidence, see the *Field Evidence Management Policy Guide* (0780PG) and the *Domestic Investigations and Operations Guide* (DIOG) (0667DPG).

4.8. Records Maintenance and Use (Phase 2: Records Life Cycle)

In this phase of a record's life cycle, authentic, reliable, and trustworthy records are readily available (useable) for business purposes and are protected (maintained) from unauthorized alteration, deletion, or destruction.

4.8.1. Records Requirements

Federal regulation Title 36 Code of Federal Regulations (CFR) Chapter XII, Subchapter B, requires agencies to take the following actions in this phase:

UNCLASSIFIED**Records Management Policy Guide**

- Establish recordkeeping systems for filing records and separating records from nonrecord and personal materials.
- Specify official file locations and storage media for all record types.
- Provide standards, guides, and instructions for easy reference to records.
- Provide reference services to facilitate access to records by authorized users.
- Periodically review and audit recordkeeping systems and practices.

4.8.2. Records Systems

The FBI utilizes many different databases, electronic information systems, and automated records systems to store case or subject data, and each system has its own unique system documentation and distinct records retention requirements. This PG sets forth recordkeeping policies and provides guidance that applies to the content of each system. Questions regarding individual systems should be directed to the responsible system owner. RAS should be contacted for recordkeeping requirements for system content and documentation, as well as ERKC. Additional information is contained in the ERKC Manual.

4.8.3. Central Recordkeeping System–Sentinel

The FBI uses a central recordkeeping system to maintain its investigative, intelligence, personnel, applicant, administrative, and general files. Records are maintained in the central recordkeeping system using a file classification system. Investigative and intelligence documents relating to specific cases, as well as significant administrative documents appropriate for distribution to other divisions and offices, are serialized in relevant case files.

In July 2012, Sentinel became the FBI's official central recordkeeping system. It is a next generation information and case-management system. It has moved the FBI from a primarily paper-based recordkeeping system to an electronic records management system. The Sentinel Intranet site contains guidance about document management within Sentinel.

4.8.4. Indexing Records

Indexing is a fundamental requirement for the management of all types of FBI records, regardless of format, medium, or origin. The FBI must maintain an automated index of subjects, references, victims, and complainants to support FBI investigative and administrative matters. Indexing is mandatory, and FBIHQ divisions, FOs, and Legats must ensure required indexing is accomplished. See DIOG, Section 3 and Appendix J, for additional information.

Within Sentinel, indexing is accomplished by creating an “entity” record. The Indexing User Manual for Sentinel contains guidelines that must be followed for entering and searching Sentinel entity records for persons, organizations, or events that are subjects, references, victims, or complainants. It is designed to promote standardized entry and search formats resulting in effective management of the administrative and investigative information collected by the FBI in the performance of its day-to-day activities. RMD's

UNCLASSIFIED**Records Management Policy Guide**

PACU will conduct monthly reviews to determine the FBI's compliance with the indexing guidance detailed in the manual referenced above.

4.8.4.1. Records Series and Filing Locations

Records are filed according to content and use, regardless of their medium, and are divided into record groups (or series) of files. There are two general types of content: program and administrative.

The majority of the FBI's program or mission-related records are arranged in case files related to a specific file classification. FBI file classifications pertain to federal violations over which the FBI has investigative jurisdiction. File classifications also have been assigned to intelligence, personnel, and administrative matters.

Administrative records facilitate routine organizational or "housekeeping" activities and are created by all FBIHQ divisions, FOs, and Legat offices. Examples of administrative records include time and attendance, travel vouchers, purchase orders, and budget preparation documents. Classifications 319 and 67Q encompass most administrative records; however, some administrative files belong in file classifications such as 242 (Automation) and 261 (Security). For administrative records, file the record copy in the respective division, FO, or Legat subfile designated for the office of origin (OO). See DIOG Appendix J for additional guidance in determining the OO.

With specific approval from RMD's Records Storage and Maintenance Unit, pre-Sentinel Legat classification 319/67Q files may be sent to RMD's Alexandria Records Center (ARC) for storage. RSMU will give special consideration to Legat offices that may experience higher risk for maintaining administrative files. To obtain approval to submit Legat administrative files for storage at the ARC, prepare a lead in Sentinel, addressed to the RSMU, and include an inventory of the files, a total box count, and the desired date of shipment. The Records Management User Manual (RM User Manual) contains additional instructions on this topic.

4.8.4.2. File Plan

A file plan is a directory of an office's or a program's records. It outlines the main file headings and subdivision headings for each record series and information system in an office. The plan identifies records in all media, including paper, electronic, and audiovisual, that are physically stored in the office; electronic records, whether on a local or remote computer server or on removable media such as compact discs (CD); records on other nonpaper media, such as digital video discs (DVD), audiotapes, and film; and records stored in other office file storage areas. When records are organized in accordance with a file plan, it is easy to periodically move inactive and noncurrent files out of an office area to other storage locations, freeing up needed office and computer space. Section 3 of the RM User Manual contains detailed guidance about file plans, as well as a sample file plan.

The point when files change from pending to closed or inactive is referred to as a file cutoff. File cutoffs identify and control records in manageable blocks, usually organized by fiscal or calendar year. Some files do not have event-driven cutoffs. These files are

UNCLASSIFIED

Records Management Policy Guide

identified and cut off based on their retention. Section 4 of the RM User Manual contains detailed guidance about file cutoffs and their implementation.

4.8.5. Case Management

FBI personnel must create and maintain authentic and reliable records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14 and DIOG Appendix J. Consult Section 5 of the RM User Manual for procedural information and records management guidance for:

- Case files.
- File jackets.
- File types.
- Universal Case File Numbers.
- Serializing.
- Subfiles and subfile designators.
- 1A (FD-340) envelopes.
- Compressed files.
- File consolidation.
- Dual-captioned cases.
- Cover sheets and media labels.
- Records managed by the Executive Secretariat (EXEC SEC).

Procedures for subfiles and subfile designators are set forth in subsection 5.6. of the RM User Manual. ITB and FBI personnel must make sure only dashes, alpha, numeric, and/or blank entries are allowed in the subfile name field of case files.

The use of compressed files is no longer authorized. Compressed files were small paper case files (normally one to ten serials in scope) that were opened in the same file classification and placed together in a single file jacket in order to conserve shelving space. See subsection 5.8. of the RM User Manual for additional information.

4.8.6. Managing Administrative Records

Classifications 319 and 67Q are designated for administrative and personnel-related records. A subfile has been opened for each FBIHQ division, FO and Legat for each of the 319 and 67Q categories. However, not all FOs will need to use all the established case file numbers. Administrative records should be filed under the classification 319 categories rather than under an investigative or an intelligence classification.

It is not necessary to import each 319 and 67Q document. If a document needs to go through the Sentinel workflow approval process, it should be imported into the appropriate 319 or 67Q file within Sentinel. If the document does not need to go through the Sentinel workflow approval process (e.g., time and attendance records or a

UNCLASSIFIED

Records Management Policy Guide

supervisor's drop files), it does not need to be imported into Sentinel. It may be maintained in a shared drive or a paper folder for the applicable retention period. The disposition of 319 and 67Q matters is discussed in subsection 4.9.11 of this PG.

Performance appraisal reports (PAR) must continue to be maintained in paper format with their original signatures. PARs are maintained by the RMD at the ARC.

Section 6 of the RM User Manual contains additional guidance.

4.8.7. Storing Paper Records

FBI paper records are stored in FBIHQ divisions, the ARC, FOs, off-site locations, and Legats around the world. All locations are required by 36 CFR §§ 1223-1238 to meet minimum standards to properly store and protect federal records. Section 8 of the RM User Manual contains detailed guidance regarding records storage.

4.8.7.1. Files at FBI Headquarters

The RMD's Records Storage and Maintenance Unit (RSMU) is responsible for overseeing the storage and maintenance of records in FBIHQ storage areas and advising FBI personnel concerning records storage and maintenance activities. The ARC is the main facility for storage and maintenance of (1) FBIHQ closed and pending case files, (2) Legat closed files, (3) closed files from inventoried FOs, (4) security and medical subfile of active personnel, and (5) micrographics, all with a classification of SECRET or lower. FBIHQ paper records with a classification higher than SECRET or containing Sensitive Compartmented Information (SCI) or other matters requiring restricted access are stored at FBIHQ in the Special File Room, J. Edgar Hoover Building

b7:

4.8.7.2. Files at Legal Attaché

A Legat maintains its pending files. The Security Division's (SecD) Legat Support Program ensures Legats are in compliance with FBI, Department of State, and other national requirements pertaining to secure areas, closed storage of classified information up to the SECRET collateral level, and, where applicable, areas accredited as Sensitive Compartmented Information Facilities (SCIF). Most closed Legat files are stored at the ARC. Subsection 9.3. of the RM User Manual contains detailed procedures for shipping records to the ARC.

4.8.7.3. Files at a Field Office or a Resident Agency (RA)

The FO headquarters city maintains the FO's pending files. The relevant RA location may maintain its unclassified and classified materials if it is in compliance with the requirements for classified material storage. Detailed guidance regarding classified material storage can be found in the Safeguarding Classified National Security Information Directive and Policy Guide (0632DPG).

4.8.7.4. Secure Storage Location Requirements

SecD is responsible for determining the requirements for all storage locations. The "Open Storage Secure Area Checklist" is a checklist of secure area facility requirements guidelines.

UNCLASSIFIED

Records Management Policy Guide

4.8.7.5. Environmental Storage Policy

All records, regardless of format or medium, must be stored in accordance with 36 CFR Part 1234, which sets forth environmental standards and preservation requirements. Section 8 of the RM User Manual contains detailed guidance regarding the minimum requirements for environmental storage of federal records.

4.8.8. Transferring Records

Detailed guidance on how to transfer records is included in Section 9 of the RM User Manual.

4.8.9. Retrieving Records

FBI employees and authorized personnel may request access to stored, paper files. Case files maintained electronically in the FBI's central recordkeeping system (Sentinel) must not be duplicated in paper and filed. Section 10 of the RM User Manual contains detailed guidance about paper records retrieval.

4.8.9.1. File-Automated Control System

The File Automated Control System (FACS) was a library system that was used to track the checking out, and returning of, all FBIHQ paper files (investigative, administrative, and personnel). As of fall 2014, FACS is no longer in use.

Subsection 10.1. of the RM User Manual contains additional information about this system.

4.8.9.2. File Request Automation Project (FRAP)

FRAP is an electronic system used to request (1) paper files (investigative, administrative, and personnel), (2) closed FO files sent to the ARC for storage as part of RMD's Field Office Inventory Project, and (3) Legat files stored at the ARC. This system has been constructed using SharePoint and InfoPath and is deployed on FBINet (the FBI [classified] Network). Files may be accessed through the FRAP Intranet site by following the instructions for ordering a file. The file is then checked out and either physically or electronically sent to the requester. When physically sent, a copy of the FRAP request form will be attached to the file for easy identification. The FRAP request form must be kept attached to the file.

The FRAP User Guide contains step-by-step guidance and additional information about this system.

4.8.9.3. Maintaining Custody of Files

An individual who checks out a file is responsible for the file until it is returned to the RSMU. In order to maintain security and access control over the information contained within the file, the individual must not give or lend the requested file to other FBI personnel. The file must be returned to RSMU and a new request must be completed.

4.8.9.4. Returning Files

All files must be returned to the RSMU within 90 days of receipt unless the requester requires additional time. To retain a file longer than 90 days, the requester must seek an

UNCLASSIFIED**Records Management Policy Guide**

extension through FRAP. The FRAP request form must be attached to the file when a file ordered through FRAP is returned.

4.8.10. Retrieving Information from Records**4.8.10.1. Outside the FBI****4.8.10.1.1. Freedom of Information and Privacy Acts (FOIPA)**

FBI records can be requested through FOIPA. The Policy Directive (PD) 0481D, *Freedom of Information Act and Privacy Act Requests* establishes actions to be taken by FBIHQ divisions, FOs, and Legats when asked by the RMD for assistance in responding to records requests.

4.8.10.1.2. National Name Check Program

The NNCP disseminates information from FBI files in response to name check requests received from federal agencies and other law enforcement entities, including internal FBI offices; components of the legislative, judicial, and executive branches; and intelligence agencies. The NNCP also conducts name check requests of those persons within arms-reach of the President.

4.8.10.1.3. Mandatory Declassification Review

Mandatory declassification reviews of FBI material are generally requested by NARA, Presidential libraries, and the public. The *Declassification of Classified National Security Information Directive and Policy Guide* (0623DPG) sets forth the policies and procedures for carrying out the declassification requirements articulated in EO 13526.

4.8.10.1.4. Legal Holds

FBI personnel have an obligation to ensure all records and nonrecords relevant to a pending litigation or reasonably anticipated matter in litigation (or other proceeding, including criminal investigations, prosecutions, and appeals) and other inquiries, investigations, and inspections are identified and protected from destruction or deletion, even as an exception to standard records disposition practices and schedules, until all legal and official uses are concluded and personnel receive written confirmation from OGC when the identification and protection of such information is no longer necessary. Identifying such records and marking them for retention is referred to as a “freeze” or “legal hold.” Whenever legal holds are initiated, all regularly scheduled destruction and/or transfer activities are suspended until OGC has notified FBI personnel that the legal hold has been rescinded. The *Legal Hold Policy* (0619D) contains further information concerning when legal holds may be issued and the roles and responsibilities of FBI personnel and others with regard to a legal hold.

4.8.10.1.5. Assistance to Other Agencies

If FBI documents and information are to be disseminated to other domestic and foreign agencies for use in investigative and intelligence programs, the documentation and records retention requirements for this type of dissemination are contained in DIOG subsections 12.6. and 12.7.

UNCLASSIFIED

Records Management Policy Guide

4.8.10.2. Personnel Records**4.8.10.2.1. Electronic Official Personnel Folder (eOPF)**

The FBI's official personnel folders (OPF) are available online for FBI employee access via the eOPF application. Access is only available on a UNet (unclassified network) computer with an FBI Internet Protocol (IP) address.

The eOPF provides electronic, Web-enabled access for all federal agency employees to view and manage employment documents. All employees are able to view their own OPFs through the eOPF application. It also includes security measures that ensure the integrity of the system and employee documents in the system. For more information on accessing an eOPF, see the Human Resources Division's eOPF Information Intranet site.

4.8.10.2.2. Paper Personnel Records

Personnel records include the applicant case file; the OPFs of agent personnel retired or separated prior to August 2012 and professional staff personnel separated less than five years prior to January 2012; the security (S) and medical (M) subfiles of active personnel; financial subfile (Sub-F); and PARs. Previously, personnel records included the other government service subfile (Sub-OGS); however, the sub-OGS is no longer maintained as a separate subfiles, it has been incorporated in the eOPF. FBI personnel may submit a formal request for copies of their personnel records. The procedure to do this is set forth in subsection 7.2. of the RM User Manual.

4.8.11. Electronic Recordkeeping Certification (ERKC) Program

An electronic information system or a knowledge management (KM) system (collectively, system) contains and provides access to computerized FBI records and other information. A system containing records must comply with the policies and procedures governing the management of FBI records. The RMD AD, as the FBI records officer, has the authority to approve, or withhold approval of, any system in use or under development.

The FBI records officer has delegated the review of systems to RMD's Records Management Application Unit (RMAU). No system may be utilized to conduct FBI business and house FBI records without review by the RMAU and final certification by the FBI records officer.

The goal of the ERKC process is to ensure systems comply with recordkeeping requirements, including the proper creation, maintenance, use, and disposition of FBI records. The ERKC process evaluates system compliance with records management criteria. The process is designed to guide systems owners and developers with assessing and incorporating records management criteria into system requirements specifications and ensuring fulfillment through review of documented test results. The ERKC process consists of identifying systems containing records; helping system owners, project managers, and developers understand ERK criteria; ensuring system requirements specifications satisfy ERK criteria; and validating ERK functionality through review of system test results.

UNCLASSIFIED**Records Management Policy Guide**

The FBI's ERKC Manual defines the authorities, roles, responsibilities, processes, and documentation requirements that govern the certification of FBI-owned and FBI-sponsored IT systems and serves as a guide for system developers, system owners, project managers, and certification team members concerning the activities required for an FBI-owned or FBI-sponsored system to achieve ERKC.

4.8.12. Metadata

Metadata is defined as data describing information—in particular, its context, content (including author), structure, and its management through time. It is critical that metadata used is detailed and descriptive to effectively manage electronic records throughout their life cycles.

Metadata requirements for recordkeeping purposes are jointly established by both the originating program office and by RMD. With adequate metadata, records are retrieved effectively and purged when no longer needed, without having to be printed for records disposition purposes. Policy for incorporating metadata tags into electronically stored information is located in PD 0249D, *Metadata Tagging of Electronically Stored Information in FBI Systems*, and the ERKC Manual, Appendix B.

4.8.13. Data Backup Retention

The FBI routinely maintains data backups on computer drives or computer media to protect data from system and server failure or from data corruption. All FBI electronic information systems must be backed up to ensure the authenticity, reliability, and integrity of the information within the systems. A full-data backup of each FBI electronic information system is retained until superseded by the next full-data backup, except for FBINet file/print servers (SECRET enclave). For these, a full-data backup is retained for 90 calendar days. See PD 0076, *Data Backup Retention*, for additional information on this matter.

Legal holds or other special inquiries are the only exceptions to this data backup retention policy. In these instances, backups must be maintained until OGC rescinds the legal hold or other preservation request.

The approved retention period for data backup is formulated as General Records Schedule (GRS) 20, "Electronic Records," Item 8, as specified by NARA, 44 U.S.C. § 3303a(d). The approved retention period for system backups is formulated as GRS 24, "Information Technology Operations and Management Records," Item 4a, as specified by NARA, 44 U.S.C. § 3303a(d). The backup retention plans for mission specific electronic systems are evaluated as part of the development of records retention guidance for the specific system.

IT systems administrators must maintain data backups in accordance with this PG. OGC is responsible for notifying IT systems administrators when there is a need to retain electronic information beyond the standard retention period for a given electronic information system and for notifying the IT administrators when an exception to the approved retention period has expired.

UNCLASSIFIED

Records Management Policy Guide

4.8.14. Capturing and Preserving Electronic Records

All FBI personnel bear responsibility for identifying, capturing, and moving electronic records into a recordkeeping system. To ensure proper preservation, personnel must import electronic communications that are nontransitory records into an ERK system such as Sentinel.

Whenever possible, personnel should import electronic communications in the format in which they were generated, otherwise known as “native format.” If an electronic communication cannot be imported in its native format (such as a voice message), it should be preserved in another format (e.g., FD-302 or electronic communication [EC]) in the appropriate recordkeeping system, such as Sentinel.

4.8.14.1.1. Deletion of Electronic Copies

Copies of documents are often maintained in electronic form, across all enclaves, either on office shared drives, individual workstations, or portable magnetic or optical media (e.g., flash drives, CDs, diskettes, or tapes). Many of these copies are word processing documents and are kept for convenience of reference or reproduction. If these copies are created solely to produce a convenience copy, once it is verified the record is appropriately filed, they should be deleted, unless subject to a legal hold. It is each employee’s responsibility to manage these copies on any FBI information system he or she uses.

4.8.15. Electronic Mail

E-mail is a frequent means of communication within the FBI, and the information contained in e-mails must be managed accordingly. FBI personnel are responsible for managing the e-mails they send and receive.

FBI personnel with access to the FBI’s e-mail systems must determine the record status of e-mails sent from, or received in, their e-mail account(s). An e-mail may be a nontransitory record (needed for more than 180 days), transitory record (needed for 180 days or less) or nonrecord. When doubt exists about whether or not an e-mail is a nontransitory record e-mail, it should be treated as a nontransitory record e-mail and imported into Sentinel or a successor central recordkeeping system.

E-mails (whether record or nonrecord) that are responsive to legal holds, investigations, FOIPA requests, or special inquiries of any kind must be preserved. PD 0619D, Legal Hold Policy, contains further information.

4.8.15.1. UNet E-Mail

Communications received via UNet that contain record material must be uploaded to FBINet to ensure proper records management. UNet e-mails should be copied to FBINet and imported into Sentinel to the relevant FBI case file.

To import these unclassified e-mails into Sentinel, use the “UNet to FBINet File Transfer System” (UNet “Uplift”) to transfer the e-mail to FBINet, where it can be filed into Sentinel. See the RM User Manual for further instructions on using Uplift.

UNCLASSIFIED

Records Management Policy Guide

4.8.16. Nontransitory Record E-mails (Needed for More Than 180 Days)

A nontransitory record e-mail is a record needed for more than 180 days that provides substantive documentation of the FBI's policies and/or actions, contains important and/or valuable evidentiary information, or is required to be maintained by law or regulation. The principal categories of materials to be preserved are records that:

- Document the formulation and/or execution of policies and decisions and the taking of necessary actions.
- Facilitate action by FBI officials and their successors in office.
- Permit Congress or other duly authorized agencies of the government to conduct a proper scrutiny of the FBI.
- Protect the financial, legal, and other rights of the government and of persons directly affected by the government's actions.

Examples include e-mails that document:

- An investigation or an intelligence analysis. Examples of e-mails that fall into this category include:
 - Exchanges between special agents (SA) or OGA personnel discussing case issues.
 - Electronic surveillance (ELSUR) requests.
 - Requests for assistance from other parties.
 - Surveillance reports.
 - Intraoffice records requests and responses that pertain to an investigation or an analysis.
 - Pertinent intelligence analyses received from another agency.
 - Task force requests for additional funding.
- Significant decisions reached at meetings, conferences, or through e-mail exchanges, such as executive decisions creating or modifying an FBI policy.
- Official agreements with entities outside the FBI.
- Quotes from vendors in response to requests for pricing proposals, which are subsequently used as the basis for contract agreements.
- FBI reorganizations.
- On-duty injuries requiring hospitalization.
- Formal assignments of divisional, FO, and Legat roles and responsibilities.
- End of the fiscal year final reports of expenditures, procurement of goods and services, and annual accountability by all FBI personnel for equipment issued to them.

UNCLASSIFIED

Records Management Policy Guide

4.8.17. Filing Nontransitory Record E-Mails in Sentinel

FBI personnel must use the Record Marking Tool (RMT) to import nontransitory record e-mails into the appropriate case file in Sentinel. Subsection 12.1. of the RM User Manual contains additional information about the RMT.

Systems such as Microsoft Outlook, Law Enforcement Online (LEO) mail, and UNet mail are communication systems, not electronic recordkeeping systems. To ensure the retention of nontransitory record e-mails in Sentinel, message creators, recipients, or professional staff personnel must complete the steps necessary to scan and import e-mails into Sentinel or a successor central recordkeeping system. Copies of nontransitory record e-mails must be added to the appropriate case file(s) before the original online e-mail message can be deleted. Attachments, as well as transmission and receipt data about the e-mail, must also be saved as part of the record. Transmission and receipt data include the sender's name, date, subject, recipient(s), and any requested return receipts. See Section 12 of the RM User Manual for instructions.

FBI personnel may not create or send a record (transitory or nontransitory) using nonofficial electronic messaging accounts unless the FBI personnel (1) copy their official electronic messaging accounts in the original creation or transmission of the records, or (2) forward complete copies of the records to their official electronic messaging accounts no later than 20 days after the original creation or transmission of the records.

For nontransitory record e-mails, FBI personnel must also complete the steps necessary to import the e-mail into Sentinel:

If the nontransitory record e-mail does not relate to a specific FBI case, the e-mail message should be filed in the related classification zero (0) file, which serves as a holding file for unsubstantiated allegations. For example, if the e-mail message provides general commentary or guidance on bank robbery matters, but does not contain information related to an actual or specific investigation, the message should be filed in the 91-0 file. If a specific case is later opened or identified, the e-mail message can be transferred from the zero (0) file to the relevant case file.

4.8.18. Transitory Record E-Mails (Needed for 180 Days or Less)

Transitory record e-mails are e-mails of short-term interest (180 days or less) and have minimal documentary or evidentiary value to the FBI. As is the case with nonrecord e-mails (discussed below), transitory record e-mails should not be preserved in an FBI recordkeeping system. Absent a legal hold, when no longer needed, these e-mails should be deleted by the creator/receiver. Examples of transitory record e-mails include:

- Routine requests for information or publications, such as e-mails sent to the Office of Public Affairs requesting copies of the "Ten Most Wanted Fugitives" poster and copies of replies.
- Quasi-official notices, such as announcements of upcoming events from the sending office. For example, transit subsidy requirements and forms and annual holiday party guidance are transitory records of the sending office.

UNCLASSIFIED

Records Management Policy Guide

- Documentation of routine activities, such as meeting notifications, reminders of midyear performance plan reviews, and unit award nominations sent to a division's or an FO's front office.
- Working drafts of proposed policies or documents.
- Routine requests for supplies and similar office management documentation.
- Suspense files and "to-do" lists.
- Confirmation of training registration, conference attendance, or travel plans.
- Messages sent enterprisewide, such as holiday closing notices or Combined Federal Campaign information. While senders may have an obligation to retain messages for a short time, recipients may delete them when no longer needed.

4.8.19. Nonrecord E-Mails

A nonrecord e-mail contains information that does not meet the definition of a federal record. A nonrecord e-mail has no documentary or evidentiary value to the business of the FBI and does not require retention beyond its useful life, as determined by the creator and/or recipient, unless subject to an external request or legal hold, as discussed above. Examples of nonrecord e-mails commonly include e-mails that transmit:

- Copies of records, such as ECs already serialized in Sentinel.
- Copies of FBI publications, such as the DIOG, *The Investigator*, or the *Law Enforcement Bulletin*.
- Informal notes and cover notes that are merely informative in nature and do not include content otherwise warranting preservation as records.
- Copies of PowerPoint training slides from FBI-provided courses.
- Electronic versions of blank forms such as the FD-772, "Report of Foreign Travel."
- Copies of notices received by individuals, such as announcements of upcoming blood drives, seminars, Combined Federal Campaign fundraisers, and similar events.
- FBI personnel anniversary, retirement, and other announcements.
- Discussions between personnel about lunch or other non-work-related activities.
- Other notifications of a personal nature.

FBI personnel with access to the FBI's e-mail systems must determine the record status of e-mails sent from, or received in, their e-mail account(s). Across all enclaves, absent a legal hold, nonrecord e-mails should be deleted from all FBI-managed e-mail systems when no longer needed. Care should be taken by FBI personnel not to commingle record and nonrecord information in e-mails. This ensures nonrecord information is not accidentally transferred or retained in any FBI record repository or system.

UNCLASSIFIED

Records Management Policy Guide

4.8.20. Intranet Sites

The Federal Records Act applies to all federal agency records, including Intranet-based records (e.g., records created on SharePoint sites). The E-Government Act of 2002 (Public Law 107-347) places a number of public site requirements on the Office of Management and Budget (OMB), NARA, and agencies in the areas of enterprise architecture, information access and security, and accessibility to persons with disabilities.

FBI personnel who use electronic communication venues to reach agreements or to transmit messages on substantive matters relating to FBI activities, including investigative and intelligence activities, must treat the exchange as a nontransitory record. The nontransitory record must be entered into Sentinel or a successor central recordkeeping system.

Many FBI Intranet pages contain organizational charts, publications, graphic presentations, interactive programs, and links to information repositories. RDU, in conjunction with the Information Technology Infrastructure Division (ITID), has developed a disposition authority, N1-065-04-6, for the administrative records associated with the FBI's public Web site, www.fbi.gov. RMAU, in conjunction with RDU, also assists program offices with developing disposition authorities for records maintained on internal and external FBI sites.

4.8.21. Electronic Information Sharing Technologies

The FBI encourages the participation of FBI personnel in both internal FBI-sponsored and external United States government (USG)-sponsored electronic information-sharing technologies (EIST) and the use of EIST.

Information exchanged through EIST may constitute record material, even though the EIST may not be an approved FBI recordkeeping system. All information that meets the definition of a federal record, including data and metadata created or received using EIST, must be entered into an authorized FBI recordkeeping system. Records management procedures for FBI-sponsored EIST must be developed in collaboration with RMD and are subject to RMD's approval. RMD's approval must be obtained before FBI personnel establish, configure, and/or operate EIST. See *Social Media and Other Electronic Information Sharing Technologies Directive and Policy Guide* (0579DPG) for additional information.

4.8.22. Imaged Records and Standards for Scanned Documents

Both paper and electronic versions must be managed according to RMD's guidance. See the RM User Manual; PD 0774D, *Records Management Standards for Scanned Documents*; and PD 0671D, *Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format*, for additional guidance.

Divisions considering the destruction of paper records after conversion to digital images must have authorization to do so from RMD.

UNCLASSIFIED

Records Management Policy Guide

4.8.23. Standards for Photographic Records

Photographic records and negatives may have a permanent retention, and many will be maintained for long retention periods. When practical and possible, FBI electronic photographic records that originated in digital format created by using medium- to high-quality resolution settings appropriate for continued preservation must be produced and retained in a manner appropriate to meet recordkeeping standards and requirements. RMD should be consulted for guidance on the standards for the creation, maintenance, and disposition of digital photographic records.

Digital photographic records and negatives generated by the FBI that are evidentiary or documentary in nature and considered FBI records, such as crime scene photographs, must be filed in the related investigative case file and will assume the retention period established for the file.

The *Field Evidence Management Policy Guide* (0780PG) and the DIOG set forth additional guidance regarding the storage and disposition of evidence, as well as the accompanying recordkeeping requirements.

4.8.24. Restrictions on FBI Records

Certain types of information must be protected from disclosure. Three examples are discussed briefly below. This is not an all-inclusive list; specific statutes may impose additional burdens on disclosures. For more guidance, see DIOG Sections 14 and 18.

4.8.24.1. Sensitive and Restricted Information

FBI personnel are required to comply with statutory, regulatory, and FBI policy requirements for the protection of certain sensitive and restricted information. Guidance on the application of national security classifications, caveats, and compartmented access requirements is located on the SecD Intranet site.

4.8.24.1.1. TOP SECRET (TS) Information /Sensitive Compartmented Information

TS/SCI must not be serialized into Sentinel. However, a placeholder, documenting the existence and attributes of the TS/SCI material, must be created and serialized into Sentinel. For details on the serialization of TS/SCI material, please see the following document, which is posted on the "One-Shots" library on the RMD Intranet site.

4.8.24.2. Federal Grand Jury Material

Federal Rules of Criminal Procedure 6(e) generally prohibits disclosing "matters occurring before the grand jury." DIOG subsection 18.6.5. sets forth policies and guidance regarding the receipt, use, disclosure, and storage of grand jury material.

4.8.24.3. Federal Tax Information

FBI personnel must protect information contained in tax returns from disclosure. SecD's FTI program manages policy, training, oversight, and coordination of FBIHQ-level efforts and programs with regard to FTI, in accordance with laws and policies and with direction from the Internal Revenue Service (IRS) and the Department of Justice (DOJ).

UNCLASSIFIED

Records Management Policy Guide

DIOG Appendix N sets out guidance on the acquiring, handling, storing, and disposition of FTI.

4.9. Records Disposition (Phase 3: Records Life Cycle)

RMD is the sole authority for the disposition of FBI records, regardless of location or medium. “Disposition” is a comprehensive term referring to either the permanent transfer of nontransitory records to NARA or the destruction of all other records.

4.9.1. Modification and Destruction of Records

RMD is the sole entity with authority to destroy or delete FBI records and is the sole entity that can authorize the destruction or deletion of FBI records. RMD (or its designee) will modify or destroy records, as authorized or required by law and in accordance with approved retention schedules. RMD is also the sole entity with authority to modify or destroy electronic references or pointers in nonrecord automated systems (i.e., Automated Case Support [ACS]), which serve to point the user to the FBI’s electronic records systems.

All FBIHQ divisions, FOs and Legats must advise RMD of the need to modify or destroy records. In Sentinel, this can be accomplished by setting a lead to DK-RPAS (RMD Records Policy and Administration Section) and requesting a permanent charge-out (PCO) of the relevant material

4.9.2. Records Retention Plan

RDU implements and updates the FBI Records Retention Plan, which governs the retention, disposition, and transfer of all FBI records, regardless of location or format. The FBI Records Retention Plan refers collectively to the GRS as well as the individual disposition schedules (SF-115 “Request for Records Disposition Authority”) the FBI submits to NARA for approval.

Disposition schedules are broken down by records series (i.e., file classification) or by system name. For each records series or system, the disposition schedule includes a brief description of the records, a breakdown of the types of records covered by the records series or system, and disposition instructions for each.

4.9.3. Purpose of Record Retention Plan

The FBI Records Retention Plan:

- Ensures compliance with the law. Federal agencies are required to have retention schedules for their records, regardless of format.
- Reduces the risk that records will be disposed of before they have met their authorized retention periods.
- Ensures records are retained as long as needed for business purposes and disposed of when no longer needed.
- Facilitates discovery during litigation.
- Protects the FBI from litigation resulting from the destruction of unscheduled records.

UNCLASSIFIED**Records Management Policy Guide**

- Frees up costly office and computer space, removing records no longer needed for current business activities.

4.9.4. Records Not Included in the Records Retention Plan

Records that are not included in the FBI Records Retention Plan or the GRSs are not authorized for disposition. These records must be retained; they cannot be deleted or destroyed. Owners and creators of these records should contact RDU for assistance with hard copy paper records and RMAU for assistance with electronic records.

4.9.4.1. Creating a New Series of Records

FBI personnel must contact RDU (paper records) or RMAU (electronic records) if the program, FBIHQ division, FO, or Legat begins creating a new series of records, obtains authorization for a new file classification, creates a new electronic information system, or substantially changes the ways in which records are created and used. RDU and RMAU will work with FBI personnel to analyze retention requirements and develop a retention schedule.

4.9.5. Applying the Records Retention Plan

The FBI Records Retention Plan sets forth specific instructions about the length of time records must be maintained. Section 13 of the RM User Manual contains detailed guidance regarding the disposition of records. The RM User Manual supplements the general policy discussion below and should be consulted as a reference tool. Note: Legal holds supersede any destruction guidance provided in the RM User Manual until such holds have been lifted.

4.9.6. Preservation of Nontransitory Records with Permanent Retention

The FBI Records Retention Plan designates a small percentage of all FBI records for permanent retention and allows for the destruction of the remainder. “Permanent retention” means a file will never be deleted or destroyed. The file will be processed by RDU and transferred to NARA for continuing retention after a specified number of years following the closing of the case. When an electronic case file is transferred to NARA, it will be deleted from the FBI’s electronic system by RDU. NARA will make the file available for researchers studying the FBI’s investigations and activities, when appropriate. See Section 13 of the RM User Manual for additional guidance.

4.9.7. Disposition of Nontransitory Records with Temporary Retention

Temporary records are records deemed by NARA to have no continuing value after their usefulness to the agency has ceased. These records are not transferred to NARA for preservation, but rather are destroyed either after a fixed period or after a specific event has occurred. Their retention periods may range from months to years. Temporary records are disposed of in accordance with a NARA-approved records schedule, unless those records are subject to a legal hold. RMD is the sole entity with authority to destroy or delete FBI records and the sole entity that can authorize the destruction or deletion of the FBI’s temporary records.

UNCLASSIFIED

Records Management Policy Guide

4.9.8. Disposition of Transitory Records

Transitory records do not need to be scanned or imported into Sentinel. They may be deleted by the user/receiver when no longer needed or deleted according to an automated deletion process, unless those records are subject to a legal hold.

4.9.9. Disposition of Investigative and Intelligence Records

RDU (paper records) and RMAU (electronic records) directly manage the disposition of all investigative and intelligence-related records. This ensures that the complex disposition requirements for these records are accurately and consistently applied. Because most of the mission-related activities of the FBI are documented in investigative and intelligence classifications, offices must retain these case files until RDU or RMAU issues specific disposition instructions or directs the transfer of records to FBIHQ for processing. Offices must not initiate disposition actions without prior guidance from RDU or RMAU.

4.9.10. Disposition of Records Pertaining to Evidence

Once a case is closed and all investigative needs have been exhausted, non-FBI-generated evidence is returned to the owner/contributor, destroyed, or forfeited. FBI-generated evidentiary and nonevidentiary items, regardless of size, that are documentary in nature and considered FBI records, such as chain of custody forms, agents' notes, crime scene photographs, and laboratory analyses, should be filed in the related investigative case file and will assume the retention period established for the file, unless modified by a legal hold.

The *Field Evidence Management Policy Guide (0780PG)* sets forth the policy regarding the storage and disposition of evidence, as well as the accompanying recordkeeping requirements.

4.9.11. Disposition of Administrative Records: Classifications 319 and 67Q

All classification 319 and 67Q records must be maintained in Sentinel or in a successor central recordkeeping system.

Most of the FBI's administrative records are temporary records and may be destroyed after their retention periods have expired. This means after a certain period has lapsed, the records can be destroyed with the approval or at the direction of RDU (paper records) or RMAU (electronic records), unless these records are subject to a legal hold. Once the retention period has expired, and authorization has been obtained, eligible classification 319 and 67Q paper serials can be destroyed.

4.9.12. Disposition of Personnel-Related Records

Personnel subfiles are maintained at the ARC, regardless of the location of the FBI personnel. The disposition of subfiles Sub-M, Sub-S, and Sub-F, is determined by the "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration and Addendums 1, 2, and 3" and the FBI Records Retention Plan.

UNCLASSIFIED

Records Management Policy Guide

RDU applies disposition to unsuccessful applicant records in accordance with retention schedules, unless they are subject to a legal hold.

4.9.13. Disposition of Draft Documents

Working files, such as preliminary drafts, notes, and other similar materials, are to be destroyed when the final documents have been approved by the FBI official with authority to do so, unless they:

- Are subject to a legal hold.
- Relate to pending FOIPA requests.
- Contain unique information, such as substantive annotations or comments that add to a proper understanding of the FBI's formulation and execution of basic policies, decisions, actions, or responsibilities and were circulated or made available for approval, comment, action, recommendation, follow-up, or to communicate FBI business.
- Have some other business reason requiring retention for reference purposes.

This guidance applies to all drafts created in any medium.

4.9.14. Disposition of Personal Files

Personal papers are not federal records and are not imported, serialized, indexed, or filed in FBI records management systems. They should be maintained separately from office records and may be disposed of at the owner's discretion, unless subject to a legal hold or FOIA.

4.9.15. Disposition of Nonrecord Materials

Nonrecord material does not need an authorized disposition. It is destroyed when FBI personnel or the responsible office no longer needs it or when the information has served its intended purpose, unless subject to a legal hold or FOIA. As a matter of good recordkeeping practice, FBI personnel should file nonrecord materials separately from records. FBI personnel should review nonrecord materials annually, and materials that are no longer useful should be destroyed.

4.10. Orphaned Records

Orphaned records are records left behind by the creators or owners. Orphaned records are sometimes abandoned in offices after personnel have moved or a reorganization has occurred. FBI personnel should be aware of their responsibilities in ensuring records in their custody are not inadvertently left behind during office moves. Similarly, supervisors should ensure that departing FBI personnel manage records in their possession prior to departure. Anyone finding orphaned records should contact the RMD Help Desk, and RMD will help determine the disposition of those records. See subsection 13.13. of the [RM User Manual](#) for additional guidance.

UNCLASSIFIED

Records Management Policy Guide

4.11. Reporting Missing Files and Serials

Files or serials missing for 30 calendar days or longer must be reported by the records liaison, via EC, to the RDU within 30 calendar days of discovery. Reasonable efforts to locate missing files or serials must be undertaken, and the status of those efforts must be reported to the RDU every 60 days after the initial report is filed. RDU shall report any missing files or serials to NARA that have not been located within six months of the date of the reported loss.

4.11.1. Reporting Missing Files and Serials Subject to Legal Hold

If missing files or serials contain documents subject to a legal hold, OGC's DCPU must be notified immediately.

If missing files or serials contain classified material, this must be reported immediately to the division and/or CSO, who will then report it to the Security Compliance Unit at FBIHQ, as directed by PD 0610D, *Security Incident Program*.

If missing files or serials can be recreated from other sources, the file should be recreated, and the new file must reference that fact. In addition, if a missing file or a serial is recreated from other sources, and the materials are subject to a legal hold, the FBIHQ division or FO must notify DCPU immediately.

The records liaison must contact RDU if, after reporting a missing file or serial, the material is subsequently located.

4.12. Expungement of FBI Records**4.12.1. Court-Ordered Expungements**

RMD's RPAS is responsible for processing court-ordered requests for the expungement of FBI case files. RPAS does this in accordance with PD 0169D, *Expungement of FBI Records*.

RPAS only processes expungement requests received directly from the CJIS Division or from OGC. Should an FBIHQ division or an FO receive an expungement request from a local, state, or federal court, the expungement request must be forwarded to the CJIS Division's Criminal History and Investigative Service Unit for processing.

4.12.2. Privacy Act Expungements

The Privacy Act allows individuals to request expungement of their records. For example, an individual may ask that erroneous information contained in his or her FBI records be expunged. All Privacy Act expungement requests are referred to the RMD's Record/Information Dissemination Section for processing.

4.13. Unauthorized Destruction of FBI Records

All FBI personnel are responsible for preventing the unauthorized destruction, damage, or alienation (removal from FBI custody) of records. The unlawful removal, defacing, alteration, or destruction of federal records may result in penalties, including fines and imprisonment. If files or serials are missing or destroyed due to negligent or willful

UNCLASSIFIED**Records Management Policy Guide**

misconduct of FBI personnel, the Office of Professional Responsibility (OPR), OGC, and RDU must be notified immediately.

RDU must then report the unauthorized destruction of any files or serials to NARA.

4.14. Damage to FBI Records

FBI records can be damaged by natural or manmade events or causes. The extent of damage can vary from minimal to extensive and can occur at any time; therefore, all FBI personnel should understand and be able to implement basic salvage operations to reduce continued deterioration of FBI records.

Information about protecting and recovering records is available on RMD's Records Protection and Recovery Intranet site.

Damaged FBI records must be reported to RMD through an EC (FD-1057), using case file 319O-HQ-A1487624-XX, Records Management Matters (replace XX with the FO's two-letter designator). The incident that damaged the documents and the remediation provided must be described in the EC.

4.15. RMD Records Disaster Team

The RMD Records Disaster Team is a collaborative effort of trained RMD employees who can deploy to any FBI division for predisaster and postdisaster records assistance. Additional information about the Records Disaster Team can be found on RMD's Records Protection and Recovery Intranet site.

4.16. Vital Records

Vital records are records that are essential to the functions of the FBI's operation during and following an emergency. The loss of these records during a disaster can create gaps in vital information, resulting in the disruption of essential services, exposure to unplanned expenses of financial settlements or loss of revenue, increased vulnerability to litigation, and loss of productivity.

Vital records may be maintained on a variety of media including paper, magnetic tape or disc, photographic film, removable hardware, and microfilm. The Vital Records Program (VRP), as defined in 36 CFR § 1236.14, provides resources to identify, use, and protect the essential operating records needed to meet federal responsibilities under national security or disaster emergencies. The Vital Records Policy Guide (0794PG) contains information about the FBI's Vital Records Program.

UNCLASSIFIED

Records Management Policy Guide

5. Summary of Legal Authorities

Several agencies, including NARA, OMB, and the General Services Administration (GSA) share oversight of records management in the federal government. Listed below are citations to the codes, regulations, and authorities most relevant to records management:

- Records Management by the Archivist of the United States and by the Administrator of General Services (44 U.S.C. Chapter 29)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)
- Disposal of Records (44 U.S.C. Chapter 33)
- Coordination of Federal Information Policy (44 U.S.C. Chapter 35)
- Public Money, Property, or Records (18 U.S.C. § 641)
- Criminal Penalties for Unauthorized Disposal of Federal Records (18 U.S.C. § 2071)
- The Freedom of Information Act (5 U.S.C. § 552)
- The Privacy Act of 1974 (5 U.S.C. § 552a)
- Federal Records (36 CFR Chapter 12, Subchapter B)
- Personnel Records (5 CFR Part 293)
- OMB Circular A-130: *Management of Federal Information Resources*
- U.S. Office of Personnel Management (OPM) Manual, *The Guide to Personnel Recordkeeping* (November 2006)
- Department of Justice Order No. 0801 (March 12, 2014) (establishes policy governing the DOJ Records and Information Management (RIM) Program for the creation, capture or receipt, maintenance and use, and disposition of all DOJ records”

UNCLASSIFIED

Records Management Policy Guide

Appendix A: Final Approvals

POLICY TITLE: <i>Records Management Policy Guide</i>	
Primary Strategic Objective	P-1 Streamline administrative and operational processes
Publish Date	2015-06-04
Effective Date	2015-06-04
Review Date	2018-06-04
EXEMPTIONS	
None	
REFERENCES	
See Section 4 and Appendices B and C of this PG.	
APPROVALS	
Sponsoring Executive Approval	Michelle A. Jupina Assistant Director Records Management Division
Final Approval	Kevin L. Perkins Associate Deputy Director

UNCLASSIFIED

Records Management Policy Guide

Appendix B: Sources of Additional Information

- *Declassification of Classified National Security Information Policy Guide* (0623DPG)
- *Domestic Investigations and Operations Guide* (DIOG) (0667DPG)
- *Social Media and Other Electronic Information Sharing Technologies Directive and Policy Guide* (0579DPG)
- *FBI Electronic Recordkeeping Certification Manual*
- *Field Evidence Management Policy Guide* (0780PG)
- *FRAP User Guide for Non-NNCP Users*
- FRAP Intranet site
- PD 0418D, *Freedom of Information Act and Privacy Act Requests*
- PD 0619D, *Legal Hold Policy*
- "Managing Your Federal Records: A Guide for FBI Executives"
- PD 0249, *Metadata Tagging of Electronically Stored Information in FBI Systems*
- Open storage secure area checklist
- *Prepublication Review Policy Guide* (0792PG)
- PD 0423D, *Preservation and Disclosure of Electronic Communications in Federal Criminal Cases*
- Records Management Division Intranet site
- *Records Management User Manual* (RM User Manual)
- RMD Help Desk
- PD 0610D, *Security Incident Program*
- Sentinel Intranet site
- *Indexing User Manual for Sentinel*
- PD 0774D, *Records Management Standards for Scanned Documents*
- PD 0671D, *Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format*
- *Vital Records Policy Guide* (0794PG)
- "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration" and Addendums 1, 2, and 3
- PD 0457D, *RMD Statement of Authorities and Responsibilities*

UNCLASSIFIED

Records Management Policy Guide

Appendix C: Acronyms

ACS	Automated Case Support [system]
AD	assistant director
ADIC	assistant director in charge
ARC	Alexandria Records Center
CD	compact disc
CDC	chief division counsel
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services Division
DCPU	Discovery Coordination and Policy Unit
DIOG	<i>Domestic Investigations and Operations Guide</i>
DK-RPAS	RMD Records Policy and Administration Section
DocLab	Document Conversion Laboratory
DOJ	Department of Justice
DVD	digital video discs
EC	electronic communication
EIST	electronic information sharing technologies
ELSUR	electronic surveillance
e-mail	electronic mail
EO	executive order
eOPF	electronic official personnel file
ERK	electronic recordkeeping
ERKC	electronic recordkeeping certification

UNCLASSIFIED

Records Management Policy Guide

Exec Sec	Executive Secretariat
FACS	file automated control system
fax	facsimile
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FBINet	Federal Bureau of Investigation Network
FO	field office
FOIA	Freedom of Information Act
FOIPA	Freedom of Information and Privacy Acts
FRAP	file request automation report
FTI	federal tax information
GRS	General Records Schedule
GSA	General Services Administration
INSD	Inspection Division
IP	Internet Protocol
IT	information technology
ITB	Information and Technology Branch
ITID	Information Technology Infrastructure Division
JEH	J. Edgar Hoover [Building]
KM	knowledge management
Legat	legal attaché
LEO	Law Enforcement Online

UNCLASSIFIED

Records Management Policy Guide

MAOP	<i>Manual of Administrative Operations and Procedures</i>
NARA	National Archives and Records Administration
NNCP	National Name Check Program
OGA	other government agency
OGC	Office of the General Counsel
OGS	other government service
OMB	Office of Management and Budget
OO	office of origin
OPF	official personnel files
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
PACU	Policy, Analysis, and Compliance Unit
PAR	performance appraisal reports
PCO	permanent charge-out
PD	policy directive
PG	policy guide
RA	resident agency
RAS	Records Automation Section
RDU	Records Disposition Unit
RIDS	Record/Information Dissemination Section
RM	Records Manual
RMA	records management application

UNCLASSIFIED

Records Management Policy Guide

RMAU	Records Management Application Unit
RMD	Records Management Division
RMT	Record Marking Tool
RPAS	Records Policy and Administration Section
RSMU	Records Storage and Maintenance Unit
SA	special agent
SAC	special agent in charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SecD	Security Division
SF	Standard Form
SIRS	Security Incident Reporting System
TS	TOP SECRET
TSU	Training Services Unit
U.S.C.	United States Code
UNet	unclassified network
USG	United States government
VRP	Vital Records Program

UNCLASSIFIED

Records Management Policy Guide

Appendix D: Contact Information

Records Management Division	
RMD Help Desk phone	<input type="text"/>
RMD Help Desk e-mail	<input type="text"/>

b7.

UNCLASSIFIED

Records Management Policy Guide

Appendix E: Supersessions

This PG supersedes:

- *Records Management Manual* (POL05-0001-RMD)
- PD 0106D, *Reporting Missing Files and Serials*
- PD 0108D, *Disposition Authority for FBI Records*
- PD 0291D, *Supervisory Approval of Administrative Records*
- PD 0332D, *Use of Special Characters and Symbols as Subfile Designators*
- PD 0372D, *Non-record E-mail Retention*
- PD 0131D, *Modification and Destruction of Records*
- 66F-HQ-A1358157-POLI serial 2
- 319W-HQ-A1487698 serial 12
- 319W-HQ-A1487698 serial 325
- 319O-HQ-1487624 serial 545
- *Manual of Administrative Operations and Procedures* (MAOP) Part 1 Section 20-4.1. through 20-4.2.
- MAOP Part 2 Section 2-3.5.
- MAOP Part 2 Section 2-3.11.
- MAOP Part 2 Section 2-4.1. through 2-4.3.8.
- MAOP Part 2 Section 2-4.5. through 2-4.5.29.
- MAOP Part 2 Section 2-5.1. through 2-5.3.1.
- MAOP Part 2 Section 11-5.1.
- MAOP Part 2 Section 11-7.3.

EXHIBIT 10

ELECTRONIC CODE OF FEDERAL REGULATIONS

e-CFR data is current as of June 25, 2020

[Title 28](#) → [Chapter I](#) → [Part 50](#) → §50.10

Title 28: Judicial Administration

[PART 50—STATEMENTS OF POLICY](#)

§50.10 Policy regarding obtaining information from, or records of, members of the news media; and regarding questioning, arresting, or charging members of the news media.

(a) *Statement of principles.* (1) Because freedom of the press can be no broader than the freedom of members of the news media to investigate and report the news, the Department's policy is intended to provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering activities. The policy is not intended to extend special protections to members of the news media who are subjects or targets of criminal investigations for conduct not based on, or within the scope of, newsgathering activities.

(2) In determining whether to seek information from, or records of, members of the news media, the approach in every instance must be to strike the proper balance among several vital interests: Protecting national security, ensuring public safety, promoting effective law enforcement and the fair administration of justice, and safeguarding the essential role of the free press in fostering government accountability and an open society.

(3) The Department views the use of certain law enforcement tools, including subpoenas, court orders issued pursuant to 18 U.S.C. 2703(d) or 3123, and search warrants to seek information from, or records of, non-consenting members of the news media as extraordinary measures, not standard investigatory practices. In particular, subpoenas or court orders issued pursuant to 18 U.S.C. 2703(d) or 3123 may be used, after authorization by the Attorney General, or by another senior official in accordance with the exceptions set forth in paragraph (c)(3) of this section, only to obtain information from, or records of, members of the news media when the information sought is essential to a successful investigation, prosecution, or litigation; after all reasonable alternative attempts have been made to obtain the information from alternative sources; and after negotiations with the affected member of the news media have been pursued and appropriate notice to the affected member of the news media has been provided, unless the Attorney General determines that, for compelling reasons, such negotiations or notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm.

(4) When the Attorney General has authorized the use of a subpoena, court order issued pursuant to 18 U.S.C. 2703(d) or 3123, or warrant to obtain from a third party communications records or business records of a member of the news media, the affected member of the news media shall be given reasonable and timely notice of the Attorney General's determination before the use of the subpoena, court order, or warrant, unless the Attorney General determines that, for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm.

(b) *Scope.*—(1) *Covered individuals and entities.* (i) The policy governs the use of certain law enforcement tools to obtain information from, or records of, members of the news media.

(ii) The protections of the policy do not extend to any individual or entity where there are reasonable grounds to believe that the individual or entity is—

(A) A foreign power or agent of a foreign power, as those terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(B) A member or affiliate of a foreign terrorist organization designated under section 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a));

(C) Designated as a Specially Designated Global Terrorist by the Department of the Treasury under Executive Order 13224 of September 23, 2001 (66 FR 49079);

(D) A specially designated terrorist as that term is defined in 31 CFR 595.311 (or any successor thereto);

(E) A terrorist organization as that term is defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi));

(F) Committing or attempting to commit a crime of terrorism, as that offense is described in 18 U.S.C. 2331(5) or 2332b(g)(5);

(G) Committing or attempting the crime of providing material support or resources to terrorists, as that offense is defined in 18 U.S.C. 2339A; or

(H) Aiding, abetting, or conspiring in illegal activity with a person or organization described in paragraphs (b)(1)(ii)(A) through (G) of this section.

(2) *Covered law enforcement tools and records.* (i) The policy governs the use by law enforcement authorities of subpoenas or, in civil matters, other similar compulsory process such as a civil investigative demand (collectively “subpoenas”) to obtain information from members of the news media, including documents, testimony, and other materials; and the use by law enforcement authorities of subpoenas, or court orders issued pursuant to 18 U.S.C. 2703(d) (“2703(d) order”) or 18 U.S.C. 3123 (“3123 order”), to obtain from third parties “communications records” or “business records” of members of the news media.

(ii) The policy also governs applications for warrants to search the premises or property of members of the news media, pursuant to Federal Rule of Criminal Procedure 41; or to obtain from third-party “communication service providers” the communications records or business records of members of the news media, pursuant to 18 U.S.C. 2703(a) and (b).

(3) *Definitions.* (i)(A) “Communications records” include the contents of electronic communications as well as source and destination information associated with communications, such as email transaction logs and local and long distance telephone connection records, stored or transmitted by a third-party communication service provider with which the member of the news media has a contractual relationship.

(B) Communications records do not include information described in 18 U.S.C. 2703(c)(2)(A), (B), (D), (E), and (F).

(ii) A “communication service provider” is a provider of an electronic communication service or remote computing service as defined, respectively, in 18 U.S.C. 2510(15) and 18 U.S.C. 2711(2).

(iii) (A) “Business records” include work product and other documentary materials, and records of the activities, including the financial transactions, of a member of the news media related to the coverage, investigation, or reporting of news. Business records are limited to those generated or maintained by a third party with which the member of the news media has a contractual relationship, and which could provide information about the newsgathering techniques or sources of a member of the news media.

(B) Business records do not include records unrelated to newsgathering activities, such as those related to the purely commercial, financial, administrative, or technical, operations of a news media entity.

(C) Business records do not include records that are created or maintained either by the government or by a contractor on behalf of the government.

(c) *Issuing subpoenas to members of the news media, or using subpoenas or court orders issued pursuant to 18 U.S.C. 2703(d) or 3123 to obtain from third parties communications records or business records of a member of the news media.* (1) Except as set forth in paragraph (c)(3) of this section, members of the Department must obtain the authorization of the Attorney General to issue a subpoena to a member of the news media; or to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party communications records or business records of a member of the news media.

(2) Requests for the authorization of the Attorney General for the issuance of a subpoena to a member of the news media, or to use a subpoena, 2703(d) order, or 3123 order to obtain communications records or business records of a member of the news media, must be personally endorsed by the United States Attorney or Assistant Attorney General responsible for the matter.

(3) *Exceptions to the Attorney General authorization requirement.* (i)(A) A United States Attorney or Assistant Attorney General responsible for the matter may authorize the issuance

of a subpoena to a member of the news media (e.g., for documents, video or audio recordings, testimony, or other materials) if the member of the news media expressly agrees to provide the requested information in response to a subpoena. This exception applies, but is not limited, to both published and unpublished materials and aired and unaired recordings.

(B) In the case of an authorization under paragraph (c)(3)(i)(A) of this section, the United States Attorney or Assistant Attorney General responsible for the matter shall provide notice to the Director of the Criminal Division's Office of Enforcement Operations within 10 business days of the authorization of the issuance of the subpoena.

(ii) In light of the intent of this policy to protect freedom of the press, newsgathering activities, and confidential news media sources, authorization of the Attorney General will not be required of members of the Department in the following circumstances:

(A) To issue subpoenas to news media entities for purely commercial, financial, administrative, technical, or other information unrelated to newsgathering activities; or for information or records relating to personnel not involved in newsgathering activities.

(B) To issue subpoenas to members of the news media for information related to public comments, messages, or postings by readers, viewers, customers, or subscribers, over which the member of the news media does not exercise editorial control prior to publication.

(C) To use subpoenas to obtain information from, or to use subpoenas, 2703(d) orders, or 3123 orders to obtain communications records or business records of, members of the news media who may be perpetrators or victims of, or witnesses to, crimes or other events, when such status (as a perpetrator, victim, or witness) is not based on, or within the scope of, newsgathering activities.

(iii) In the circumstances identified in paragraphs (c)(3)(ii)(A) through (C) of this section, the United States Attorney or Assistant Attorney General responsible for the matter must—

(A) Authorize the use of the subpoena or court order;

(B) Consult with the Criminal Division regarding appropriate review and safeguarding protocols; and

(C) Provide a copy of the subpoena or court order to the Director of the Office of Public Affairs and to the Director of the Criminal Division's Office of Enforcement Operations within 10 business days of the authorization.

(4) *Considerations for the Attorney General in determining whether to authorize the issuance of a subpoena to a member of the news media.* (i) In matters in which a member of the Department determines that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the member of the Department requesting Attorney General authorization to issue a subpoena to a member of the news media shall provide all facts necessary for determinations by the Attorney General regarding both whether the member of the news media is a subject or target of the investigation and whether to authorize the

issuance of such subpoena. If the Attorney General determines that the member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the Attorney General's determination regarding the issuance of the proposed subpoena should take into account the principles reflected in paragraph (a) of this section, but need not take into account the considerations identified in paragraphs (c)(4)(ii) through (viii) of this section.

(ii)(A) In criminal matters, there should be reasonable grounds to believe, based on public information, or information from non-media sources, that a crime has occurred, and that the information sought is essential to a successful investigation or prosecution. The subpoena should not be used to obtain peripheral, nonessential, or speculative information.

(B) In civil matters, there should be reasonable grounds to believe, based on public information or information from non-media sources, that the information sought is essential to the successful completion of the investigation or litigation in a case of substantial importance. The subpoena should not be used to obtain peripheral, nonessential, cumulative, or speculative information.

(iii) The government should have made all reasonable attempts to obtain the information from alternative, non-media sources.

(iv)(A) The government should have pursued negotiations with the affected member of the news media, unless the Attorney General determines that, for compelling reasons, such negotiations would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm. Where the nature of the investigation permits, the government should have explained to the member of the news media the government's needs in a particular investigation or prosecution, as well as its willingness to address the concerns of the member of the news media.

(B) The obligation to pursue negotiations with the affected member of the news media, unless excused by the Attorney General, is not intended to conflict with the requirement that members of the Department secure authorization from the Attorney General to question a member of the news media as required in paragraph (f)(1) of this section. Accordingly, members of the Department do not need to secure authorization from the Attorney General to pursue negotiations.

(v) The proposed subpoena generally should be limited to the verification of published information and to such surrounding circumstances as relate to the accuracy of the published information.

(vi) In investigations or prosecutions of unauthorized disclosures of national defense information or of classified information, where the Director of National Intelligence, after consultation with the relevant Department or agency head(s), certifies to the Attorney General the significance of the harm raised by the unauthorized disclosure and that the information disclosed was properly classified and reaffirms the intelligence community's continued support for the investigation or prosecution, the Attorney General may authorize

members of the Department, in such investigations, to issue subpoenas to members of the news media. The certification, which the Attorney General should take into account along with other considerations identified in paragraphs (c)(4)(ii) through (viii) of this section, will be sought not more than 30 days prior to the submission of the approval request to the Attorney General.

(vii) Requests should be treated with care to avoid interference with newsgathering activities and to avoid claims of harassment.

(viii) The proposed subpoena should be narrowly drawn. It should be directed at material and relevant information regarding a limited subject matter, should cover a reasonably limited period of time, should avoid requiring production of a large volume of material, and should give reasonable and timely notice of the demand.

(5) *Considerations for the Attorney General in determining whether to authorize the use of a subpoena, 2703(d) order, or 3123 order to obtain from third parties the communications records or business records of a member of the news media.* (i) In matters in which a member of the Department determines that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the member of the Department requesting Attorney General authorization to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party the communications records or business records of a member of the news media shall provide all facts necessary for determinations by the Attorney General regarding both whether the member of the news media is a subject or target of the investigation and whether to authorize the use of such subpoena or order. If the Attorney General determines that the member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the Attorney General's determination regarding the use of the proposed subpoena or order should take into account the principles reflected in paragraph (a) of this section, but need not take into account the considerations identified in paragraphs (c)(5)(ii) through (viii) of this section.

(ii)(A) In criminal matters, there should be reasonable grounds to believe, based on public information, or information from non-media sources, that a crime has been committed, and that the information sought is essential to the successful investigation or prosecution of that crime. The subpoena or court order should not be used to obtain peripheral, nonessential, cumulative, or speculative information.

(B) In civil matters, there should be reasonable grounds to believe, based on public information, or information from non-media sources, that the information sought is essential to the successful completion of the investigation or litigation in a case of substantial importance. The subpoena should not be used to obtain peripheral, nonessential, cumulative, or speculative information.

(iii) The use of a subpoena or court order to obtain from a third party communications records or business records of a member of the news media should be pursued only after the government has made all reasonable attempts to obtain the information from alternative sources.

(iv)(A) The government should have pursued negotiations with the affected member of the news media unless the Attorney General determines that, for compelling reasons, such negotiations would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm.

(B) The obligation to pursue negotiations with the affected member of the news media, unless excused by the Attorney General, is not intended to conflict with the requirement that members of the Department secure authorization from the Attorney General to question a member of the news media as set forth in paragraph (f)(1) of this section. Accordingly, members of the Department do not need to secure authorization from the Attorney General to pursue negotiations.

(v) In investigations or prosecutions of unauthorized disclosures of national defense information or of classified information, where the Director of National Intelligence, after consultation with the relevant Department or agency head(s), certifies to the Attorney General the significance of the harm raised by the unauthorized disclosure and that the information disclosed was properly classified and reaffirms the intelligence community's continued support for the investigation or prosecution, the Attorney General may authorize members of the Department, in such investigations, to use subpoenas or court orders issued pursuant to 18 U.S.C. 2703(d) or 3123 to obtain communications records or business records of a member of the news media. The certification, which the Attorney General should take into account along with the other considerations identified in paragraph (c)(5) of this section, will be sought not more than 30 days prior to the submission of the approval request to the Attorney General.

(vi) Requests should be treated with care to avoid interference with newsgathering activities and to avoid claims of harassment.

(vii) The proposed subpoena or court order should be narrowly drawn. It should be directed at material and relevant information regarding a limited subject matter, should cover a reasonably limited period of time, and should avoid requiring production of a large volume of material.

(viii) If appropriate, investigators should propose to use search protocols designed to minimize intrusion into potentially protected materials or newsgathering activities unrelated to the investigation, including but not limited to keyword searches (for electronic searches) and filter teams (reviewing teams separate from the prosecution and investigative teams).

(6) When the Attorney General has authorized the issuance of a subpoena to a member of the news media; or the use of a subpoena, 2703(d) order, or 3123 order to obtain from a third party communications records or business records of a member of the news media, members of the Department must consult with the Criminal Division before moving to compel compliance with any such subpoena or court order.

(d) Applying for warrants to search the premises, property, communications records, or business records of members of the news media. (1) Except as set forth in paragraph (d)(4) of this section, members of the Department must obtain the authorization of the Attorney

General to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media.

(2) All requests for authorization of the Attorney General to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media must be personally endorsed by the United States Attorney or Assistant Attorney General responsible for the matter.

(3) In determining whether to authorize an application for a warrant to search the premises, property, communications records, or business records of a member of the news media, the Attorney General should take into account the considerations identified in paragraph (c)(5) of this section.

(4) Members of the Department may apply for a warrant to obtain work product materials or other documentary materials of a member of the news media pursuant to the “suspect exception” of the Privacy Protection Act (“PPA suspect exception”), 42 U.S.C. 2000aa(a)(1), (b)(1), when the member of the news media is a subject or target of a criminal investigation for conduct not based on, or within the scope of, newsgathering activities. In such instances, members of the Department must secure authorization from a Deputy Assistant Attorney General for the Criminal Division.

(5) Members of the Department should not be authorized to apply for a warrant to obtain work product materials or other documentary materials of a member of the news media under the PPA suspect exception, 42 U.S.C. 2000aa(a)(1), (b)(1), if the sole purpose is to further the investigation of a person other than the member of the news media.

(6) A Deputy Assistant Attorney General for the Criminal Division may authorize, under an applicable PPA exception, an application for a warrant to search the premises, property, communications records, or business records of an individual other than a member of the news media, but who is reasonably believed to have “a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.” 42 U.S.C. 2000aa(a), (b).

(7) In executing a warrant authorized by the Attorney General or by a Deputy Assistant Attorney General for the Criminal Division investigators should use search protocols designed to minimize intrusion into potentially protected materials or newsgathering activities unrelated to the investigation, including but not limited to keyword searches (for electronic searches) and filter teams.

(e) *Notice to affected member of the news media.* (1)(i) In matters in which the Attorney General has both determined that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, and authorized the use of a subpoena, court order, or warrant to obtain from a third party the communications records or business records of a member of the news media pursuant to paragraph (c)(4)(i), (c)(5)(i), or (d)(1) of this section, members of the Department are not required to provide notice of the Attorney General's authorization to the

affected member of the news media. The Attorney General nevertheless may direct that notice be provided.

(ii) If the Attorney General does not direct that notice be provided, the United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Attorney General every 90 days an update regarding the status of the investigation, which update shall include an assessment of any harm to the investigation that would be caused by providing notice to the affected member of the news media. The Attorney General shall consider such update in determining whether to direct that notice be provided.

(2)(i) Except as set forth in paragraph (e)(1) of this section, when the Attorney General has authorized the use of a subpoena, court order, or warrant to obtain from a third party communications records or business records of a member of the news media, the affected member of the news media shall be given reasonable and timely notice of the Attorney General's determination before the use of the subpoena, court order, or warrant, unless the Attorney General determines that, for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm.

(ii) The mere possibility that notice to the affected member of the news media, and potential judicial review, might delay the investigation is not, on its own, a compelling reason to delay notice.

(3) When the Attorney General has authorized the use of a subpoena, court order, or warrant to obtain communications records or business records of a member of the news media, and the affected member of the news media has not been given notice, pursuant to paragraph (e)(2) of this section, of the Attorney General's determination before the use of the subpoena, court order, or warrant, the United States Attorney or Assistant Attorney General responsible for the matter shall provide to the affected member of the news media notice of the order or warrant as soon as it is determined that such notice will no longer pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm. In any event, such notice shall occur within 45 days of the government's receipt of any return made pursuant to the subpoena, court order, or warrant, except that the Attorney General may authorize delay of notice for an additional 45 days if he or she determines that, for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm. No further delays may be sought beyond the 90-day period.

(4) The United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Director of the Office of Public Affairs and to the Director of the Criminal Division's Office of Enforcement Operations a copy of any notice to be provided to a member of the news media whose communications records or business records were sought or obtained at least 10 business days before such notice is provided to the affected member of the news media, and immediately after such notice is, in fact, provided to the affected member of the news media.

(f) *Questioning, arresting, or charging members of the news media.* (1) No member of the Department shall subject a member of the news media to questioning as to any offense that he or she is suspected of having committed in the course of, or arising out of, newsgathering activities without first providing notice to the Director of the Office of Public Affairs and obtaining the express authorization of the Attorney General. The government need not view the member of the news media as a subject or target of an investigation, or have the intent to prosecute the member of the news media, to trigger the requirement that the Attorney General must authorize such questioning.

(2) No member of the Department shall seek a warrant for an arrest, or conduct an arrest, of a member of the news media for any offense that he or she is suspected of having committed in the course of, or arising out of, newsgathering activities without first providing notice to the Director of the Office of Public Affairs and obtaining the express authorization of the Attorney General.

(3) No member of the Department shall present information to a grand jury seeking a bill of indictment, or file an information, against a member of the news media for any offense that he or she is suspected of having committed in the course of, or arising out of newsgathering activities, without first providing notice to the Director of the Office of Public Affairs and obtaining the express authorization of the Attorney General.

(4) In requesting the Attorney General's authorization to question, to seek an arrest warrant for or to arrest, or to present information to a grand jury seeking an indictment or to file an information against, a member of the news media as provided in paragraphs (f)(1) through (3) of this section, members of the Department shall provide all facts necessary for a determination by the Attorney General.

(5) In determining whether to grant a request for authorization to question, to seek an arrest warrant for or to arrest, or to present information to a grand jury seeking an indictment or to file an information against, a member of the news media, the Attorney General should take into account the considerations reflected in the Statement of Principles in paragraph (a) of this section.

(g) *Exigent circumstances.* (1)(i) A Deputy Assistant Attorney General for the Criminal Division may authorize the use of a subpoena or court order, as described in paragraph (c) of this section, or the questioning, arrest, or charging of a member of the news media, as described in paragraph (f) of this section, if he or she determines that the exigent use of such law enforcement tool or technique is necessary to prevent or mitigate an act of terrorism; other acts that are reasonably likely to cause significant and articulable harm to national security; death; kidnapping; substantial bodily harm; conduct that constitutes a specified offense against a minor (for example, as those terms are defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006, 42 U.S.C. 16911), or an attempt or conspiracy to commit such a criminal offense; or incapacitation or destruction of critical infrastructure (for example, as defined in section 1016(e) of the USA PATRIOT Act, 42 U.S.C. 5195c(e)).

(ii) A Deputy Assistant Attorney General for the Criminal Division may authorize an application for a warrant, as described in paragraph (d) of this section, if there is reason to believe that the immediate seizure of the materials at issue is necessary to prevent the death of, or serious bodily injury to, a human being, as provided in 42 U.S.C. 2000aa(a)(2) and (b) (2).

(2) Within 10 business days of the approval by a Deputy Assistant Attorney General for the Criminal Division of a request under paragraph (g) of this section, the United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Attorney General and to the Director of the Office of Public Affairs a statement containing the information that would have been provided in a request for prior authorization.

(h) *Safeguarding.* Any information or records obtained from members of the news media or from third parties pursuant to this policy shall be closely held so as to prevent disclosure of the information to unauthorized persons or for improper purposes. Members of the Department should consult the United States Attorneys' Manual for specific guidance regarding the safeguarding of information or records obtained from members of the news media or from third parties pursuant to this policy.

(i) *Failure to comply with policy.* Failure to obtain the prior approval of the Attorney General, as required by this policy, may constitute grounds for an administrative reprimand or other appropriate disciplinary action.

(j) *General provision.* This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

[AG Order No. 3486-2015, 80 FR 2820, Jan. 21, 2015]

[Need assistance?](#)

EXHIBIT 11

[added December 2017]

9-13.200 - Communications with Represented Persons

Department attorneys are governed in criminal and civil law enforcement investigations and proceedings by the relevant rule of professional conduct that deals with communications with represented persons. 28 U.S.C. Section 530B. In determining which rule of professional conduct is relevant, Department attorneys should be guided by 28 C.F.R. Part 77 (1999). Department attorneys are strongly encouraged to consult with their Professional Responsibility Officers or supervisors—and, if appropriate, the Professional Responsibility Advisory Office—when there is a question regarding which is the relevant rule or the interpretation or application of the relevant rule.

[updated January 2020]

9-13.300 - Polygraphs—Department Policy

The Department opposes all attempts by defense counsel to admit polygraph evidence or to have an examiner appointed by the court to conduct a polygraph test. Government attorneys should refrain from seeking the admission of favorable examinations that may have been conducted during the investigatory stage for the following reasons.

Though certain physiological reactions such as a fast heartbeat, muscle contraction, and sweaty palms are believed to be associated with deception attempts, they do not, by themselves, indicate deceit. Anger, fear, anxiety, surprise, shame, embarrassment, and resentment can also produce these same physiological reactions. S. Rep. No. 284, 100th Cong., 2d Sess. 3-5 (1988). Moreover, an individual is less likely to produce these physiological reactions if he is assured that the results of the examination will not be disclosed without his approval. Given the present theoretical and practical deficiencies of polygraphs, the government takes the position that polygraph results should not be introduced into evidence at trial. On the other hand, in respect to its use as an investigatory tool, the Department recognizes that in certain situations, as in testing the reliability of an informer, a polygraph can be of some value. Department policy therefore supports the limited use of the polygraph during investigations. This limited use should be effectuated by using the trained examiners of the federal investigative agencies, primarily the FBI, in accordance with internal procedures formulated by the agencies. *E.g.*, R. Ferguson, Polygraph Policy Model for Law Enforcement, *FBI Law Enforcement Bulletin*, pages 6-20 (June 1987). The case agent or prosecutor should make clear to the possible defendant or witness the limited purpose for which results are used and that the test results will be only one factor in making a prosecutive decision. If the subject is in custody, the test should be preceded by Miranda warnings. Subsequent admissions or confessions will then be admissible if the trial court determines that the statements were voluntary. *Wyrick v. Fields*, 459 U.S. 42 (1982); *Keiper v. Cupp*, 509 F.2d 238 (9th Cir. 1975).

[updated January 2020]

9-13.400 Obtaining Information From, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media.

In January 2015, the Attorney General issued an updated policy, reflected in 28 C.F.R. 50.10, regarding obtaining information from, or records of, members of the news media; and regarding questioning, arresting, or charging members of the news media. The updated policy is intended to ensure that, in determining whether to seek information from, or records of, members of the news media, the Department strikes the proper balance among

several vital interests: protecting national security, ensuring public safety, promoting effective law enforcement and the fair administration of justice, and safeguarding the essential role of the free press in fostering government accountability and an open society. See Memorandum from the Attorney General to All Department Employees (Jan. 14, 2015); Memorandum from the Attorney General to All Department Employees (Feb. 21, 2014); Report on Review of News Media Policies (July 2013). To achieve this balance, the policy mandates robust review and evaluation by the Criminal Division of requests for authorization to use covered law enforcement tools, and oversight by senior Department officials.

This section provides guidance regarding the interpretation and application of the policy reflected in 28 C.F.R. 50.10; instruction regarding the process for securing the necessary approvals; and information regarding the **mandatory consultation requirements** that are noted where applicable throughout this section and summarized in subsection M herein. See Memorandum from the Attorney General to All Department Employees (Jan. 14, 2015). To satisfy the mandatory consultation requirement, members of the Department must submit to the Policy and Statutory Enforcement Unit (PSEU) at pseu@usdoj.gov (link sends e-mail) a memorandum describing the relevant facts and addressing the relevant considerations. In addition to the PSEU email address, members of the Department may contact PSEU for any questions by calling (202) 305-4023. Members of the Department **may not employ** the use of the investigative tool at issue until the Criminal Division has responded in writing.

Because obtaining information from, or records of, members of the news media; and questioning, arresting, or charging members of the news media, requires balancing critical law enforcement and free press-related interests, obtaining the Attorney General's authorization to use the law enforcement tools covered by this policy (or consulting with the Criminal Division, as required) often is time intensive. Accordingly, to ensure appropriate consideration, **members of the Department should submit requests for authorization or consultation pursuant to this policy at least 30 days before the anticipated use of the covered law enforcement tool.**

A. Statement of Principles.

1. The Department's policy is intended to provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering. The policy is not intended to extend special protections to members of the news media who are the subject or targets of criminal investigations for conduct not based on, or within the scope of, newsgathering activities. 28 C.F.R. 50.10(a)(1). The policy also is not intended to inhibit the ability of law enforcement authorities to engage with members of the news media for the purpose of seeking the voluntary (i.e., without compulsion) production or disclosure of records, materials, or information; or to question or interview members of the news media on a voluntary basis when such questioning does not concern criminal conduct the member of the news media is suspected of having committed in the course of, or arising out of, newsgathering activities.

The policy does not define "member of the news media." Rather, whether an individual or an entity is a member of the news media is a fact-specific inquiry, and should be determined on a case-by-case basis. The policy also does not define "newsgathering activities," which determination affects whether the Attorney General, as opposed to the United States Attorney or the Assistant Attorney General responsible for the matter, must authorize the use of a particular law enforcement tool. See 28 C.F.R. 50.10(c)(3)(ii) and (d)(4).

When there is a question regarding whether an individual or entity is a member of the news media, members of the Department must consult with the PSEU before employing the use of a covered law enforcement tool. Members of the Department must also consult with the PSEU

regarding whether the conduct at issue of the affected member of the news media constitutes or relates to "newsgathering activities."

2. In determining whether to seek information from, or records of, members of the news media, the approach in every instance must be to strike the proper balance between several vital interests: protecting national security, ensuring public safety, promoting effective law enforcement and the fair administration of justice, and safeguarding the essential role of the free press in fostering government accountability and an open society. 28 C.F.R. 50.10(a)(2).
3. The Department views the use of certain law enforcement tools, including subpoenas, court orders issued pursuant to 18 U.S.C. 2703(d) or 3123, and search warrants to seek information from, or records of, non-consenting members of the news media as extraordinary measures, not standard investigatory practices. 28 C.F.R. 50.10(a)(3).
4. When the Attorney General has authorized the use of a subpoena, court order issued pursuant to 18 U.S.C. 2703(d) or 3123, or warrant to obtain from a third party the communications records or business records of a member of the news media, the affected member of the news media shall be given reasonable and timely notice of the Attorney General's determination before the use of the subpoena, court order, or warrant, unless the Attorney General determines that, for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm. 28 C.F.R. 50.10(a)(4); *see also* 28 C.F.R. 50.10(e).

B. Scope.

1. Covered Individuals and Entities

- i. The policy governs the use of certain law enforcement tools to obtain information from, or records of, members of the news media; and the questioning, arresting, or charging of members of the news media.
- ii. The protections of the policy do not extend to any individual or entity where there are reasonable grounds to believe that the individual or entity is a foreign power or an agent of a foreign power; a member or an affiliate of a foreign terrorist organization; designated a specially designated global terrorist; a specially designated terrorist; a terrorist organization; committing or attempting to commit a crime of terrorism; committing or attempting to commit the crime of providing material support or resources to a terrorist organization; or aiding, abetting, or conspiring in illegal activity with such individuals or entities. 28 C.F.R. 50.10(b)(1)(ii).

Members of the Department must consult with the PSEU regarding whether an individual or entity is not covered by, and therefore not entitled to the protections of, the policy, pursuant to 28 C.F.R. 50.10(b)(1)(ii). The Criminal Division will consult with the National Security Division, as appropriate.

2. Covered Law Enforcement Tools and Records

- i. The policy governs the use by law enforcement authorities of subpoenas to obtain information from members of the news media, including documents, testimony, and other materials; and the use by law enforcement authorities of subpoenas, or court orders issued pursuant to 18

U.S.C. 2703(d) (2703(d) order) or 18 U.S.C. 3123 (3123 order), to obtain from third parties "communications records" or "business records" of members of the news media, as those terms are defined in 28 C.F.R. 50.10(b)(3). 28 C.F.R. 50.10(b). **Members of the Department shall consult with the PSEU regarding whether particular records sought constitute communications records or business records as defined by this policy.**

- ii. The policy governs applications for warrants to search the premises or property of members of the news media, pursuant to Federal Rule of Criminal Procedure 41; or to obtain from third-party "communication service providers" the communications records or business records of members of the news media, pursuant to 28 U.S.C. 2703(a) and (b). *Id.*
 - iii. The policy governs questioning members of the news media about, arresting members of the news media for, or charging members of the news media with criminal conduct they are suspected of having committed in the course of, or arising out of, newsgathering activities.
3. *Subpoenas or Court Orders Issued or Obtained by Other Executive Branch Departments or Agencies.* Although not expressly addressed in 28 C.F.R. 50.10, members of the Department must consult with the Criminal Division before taking steps to enforce subpoenas issued to member of the news media, or to compel compliance with subpoenas or court orders issued to third parties for communications records or business records of member of the news media, which subpoenas were issued or court orders obtained in the first instance by other Executive Branch departments or agencies. To satisfy the consultation requirement, members of the Department shall submit to the PSEU a memorandum describing the factual and legal background of the matter. Members of the Department may not proceed with any efforts to enforce or compel compliance with any subpoenas or court orders until the Criminal Division has responded in writing to the request for consultation.

C. Issuing Subpoenas to Members of the News Media, or Using Subpoenas or Court Orders Issued Pursuant to 18 U.S.C. 2703 or 3123 to Obtain From Third Parties Communications Records or Business Records of Members of the News Media.

1. Except as set forth in 28 C.F.R. 50.10(c)(3), members of the Department must obtain the authorization of the Attorney General to issue a subpoena to a member of the news media; or to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party communications records or business records of a member of the news media. 28 C.F.R. 50.10(c)(1).
2. Requests for the authorization of the Attorney General for the issuance of a subpoena to a member of the news media; or to use a subpoena, 2703(d) order, or 3123 order to obtain communications records or business records of a member of the news media, must be personally endorsed by the United States Attorney or Assistant Attorney General responsible for the matter. 28 C.F.R. 50.10(c)(2).
3. *Exceptions to the Attorney General Authorization Requirement*
 - i. **Consent of Member of the News Media.** The United States Attorney or Assistant Attorney General responsible for the matter may authorize the issuance of a subpoena to a member of the news media, if the member of the news media expressly agrees to provide the requested information in response to a subpoena. 28 C.F.R. 50.10(c)(3)(i). In such circumstances, the United States Attorney or Assistant Attorney General responsible for a matter shall provide

notice to the Director of the Criminal Division's Office of Enforcement Operations within 10 business days of the authorization of the issuance of the subpoena. *Id.*

ii. **Information Sought Not Related to Newsgathering Activities**

- a. The United States Attorney or Assistant Attorney General responsible for the matter may authorize the issuance of a subpoena to a member of the news media for purely commercial, financial, administrative, technical, or other information unrelated to newsgathering activities; or for information or records relating to personnel not involved in newsgathering activities. 28 C.F.R. 50.10(c)(3)(ii)(A). **Before issuing a subpoena to a member of the news media pursuant to this provision, members of the Department must consult with the PSEU.**
 - b. The United States Attorney or Assistant Attorney General responsible for the matter may authorize the issuance of a subpoena to a member of the news media for information related to public comments, messages, or postings by readers, viewers, customers, or subscribers, over which the member of the news media does not exercise editorial control prior to publication. 28 C.F.R. 50.10(c)(3)(ii)(B). **Before issuing a subpoena to a member of the news media pursuant to this provision, members of the Department must consult with the PSEU.**
 - c. The United States Attorney or Assistant Attorney General responsible for the matter may authorize the use of subpoenas to obtain information from, or the use of subpoenas, 2703(d) orders, or 3123 orders to obtain communications records or business records of, members of the news media who may be perpetrators or victims of, or witnesses to, crimes or other events, when such status (as a perpetrator, victim, or witness) is not based on, or within the scope of, newsgathering activities. 28 C.F.R. 50.10(c)(3)(ii)(C). **Before issuing a subpoena or applying for a court order pursuant to this provision, members of the Department must consult with the PSEU.**
 - d. **Criminal Division Consultation and Notice.** In the circumstances identified in 28 C.F.R. 50.10(c)(3)(ii), the United States Attorney or Assistant Attorney General responsible for the matter must consult with the Criminal Division regarding appropriate review and safeguarding protocols; and provide a copy of the subpoena or court order to the Director of the Office of Public Affairs and to the Director of the Criminal Division's Office of Enforcement Operations within 10 business days of the authorization. 28 C.F.R. 50.10(c)(3)(iii).
4. In seeking the authorization of the Attorney General to issue a subpoena to a member of the news media, members of the Department shall address the considerations identified in 28 C.F.R. 50.10(c)(4).
- i. **Member of the news media as subject or target.** In matters in which a member of the Department determines that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the member of the Department requesting Attorney General authorization to issue a

subpoena to a member of the news media shall provide all facts necessary to a determination by the Attorney General regarding both whether the member of the news media is a subject or target of the investigation and whether to authorize the issuance of such subpoena. 28 C.F.R. 50.10(c)(4)(i). If the Attorney General determines that the member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the Attorney General's determination should take into account the principles reflected in 28 C.F.R. 50.10(a), but need not take into account the considerations identified in 28 C.F.R. 50.10(c)(4)(ii) – (viii). *Id.* **Members of the Department must consult with the PSEU regarding whether a member of the news media is a subject or target of an investigation related to an offense committed in the course of, or arising out of, newsgathering activities.**

- ii. **Director of National Intelligence Certification.** In investigations or prosecutions of unauthorized disclosures of national defense information or classified information, the member of the Department requesting Attorney General authorization to issue a subpoena to a member of the news media shall obtain from the Director of National Intelligence (DNI) a document certifying (1) the significance of the harm raised by the unauthorized disclosure, (2) that the information disclosed was properly classified, and (3) re-affirmance of the intelligence community's support for the investigation or prosecution. 28 C.F.R. 50.10(c)(4)(vi). **Because securing the necessary certification from the DNI may take considerable time, members of the Department are encouraged to initiate the process at least 30 days in advance of seeking the Attorney General's authorization, and must coordinate with the National Security Division in seeking the DNI certification.**

- 5. In seeking the authorization of the Attorney General to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party the communications records or business records of a member of the news media, members of the Department shall address the considerations identified in 28 C.F.R. 50.10(c)(5).

- i. **Member of the news media as subject or target.** In matters in which a member of the Department determines that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the member of the Department requesting Attorney General authorization to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party the communications records or business records of a member of the news media shall provide all facts necessary to a determination by the Attorney General regarding both whether the member of the news media is a subject or target of the investigation and whether to authorize the use of such subpoena or court order. 28 C.F.R. 50.10(c)(5)(i). If the Attorney General determines that the member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the Attorney General's determination should take into account the principles reflected in 28 C.F.R. 50.10(a), but need not take into account the considerations identified in 28 C.F.R. 50.10(c)(5)(ii) – (viii). *Id.* **Members of the Department must consult with the PSEU regarding whether a member of the news media is a subject or target of an investigation related to an offense committed in the course of, or arising out of, newsgathering activities.**

- ii. **Director of National Intelligence Certification.** In investigations or prosecutions of

unauthorized disclosures of national defense information or classified information, the member of the Department requesting Attorney General authorization to use a subpoena, 2703(d) order, or 3123 order to obtain from a third party the communications records or business records of a member of the news media shall obtain from the Director of National Intelligence a document certifying (1) the significance of the harm raised by the unauthorized disclosure, (2) that the information disclosed was properly classified, and (3) re-affirmance of the intelligence community's support for the investigation or prosecution. 28 C.F.R. 50.10(c)(5)(v). **Because securing the necessary certification from the DNI may take considerable time, members of the Department are encouraged to initiate the process at least 30 days in advance of seeking the Attorney General's authorization, and must coordinate with the National Security Division in seeking the DNI certification.**

6. Consultation with Criminal Division before Moving to Compel.

- i. When the Attorney General has authorized the issuance of a subpoena to a member of the news media; or the use of a subpoena, 2703(d) order, or 3123 order to obtain from a third party communications records or business records of a member of the news media, members of the Department shall consult with the Criminal Division *before moving to compel compliance with any such subpoena or court order.* 28 C.F.R. 50.10(c)(6). To satisfy the consultation requirement, members of the Department shall submit to the PSEU a memorandum (2) describing the facts, including communications with the affected member of the news media and other events, that transpired since the Attorney General's authorization; and (2) explaining why compulsion is necessary.
- ii. Although not expressly addressed in 28 C.F.R. 50.10, members of the Department must consult with the Criminal Division before taking steps to enforce subpoenas issued to member of the news media, or to compel compliance with subpoenas or court orders issued to third parties for communications records or business records of member of the news media, which subpoenas were issued or court orders obtained in the first instance by other Executive Branch departments or agencies. To satisfy the consultation requirement, members of the Department shall submit to the PSEU a memorandum describing the factual and legal background of the matter. Members of the Department may not proceed with any efforts to enforce or compel compliance with any subpoenas or court orders until the Criminal Division has responded in writing to the request for consultation.

7. Non-Disclosure Orders Directed to News Media Entities or Third-Party Communication Service Providers

- i. In seeking authorization of the Attorney General, pursuant to 28 C.F.R.50.10(c), or a Deputy Assistant Attorney General for the Criminal Division, pursuant to 28 C.F.R. 50.10(g), to issue a subpoena to a news media entity; or to use of a subpoena, 2703(d) order, or 3123 order to obtain from a third party communications records or business records of a member of the news media, members of the Department must indicate whether they intend to seek an order directing the recipient of the subpoena or court order, if authorized, not to disclose the existence of the subpoena or court order to any other person or entity, and shall articulate the need for such non-disclosure order. Any authorization must expressly indicate whether a non-disclosure order may be sought.

- ii. **Consultation with Criminal Division before Seeking Non-Disclosure Orders Directed to News Media Entity when US Attorney or Assistant Attorney General Authorizes Issuance of Subpoena.** If an Assistant Attorney General or a United States Attorney authorizes the issuance of a subpoena to a news media entity pursuant to 28 C.F.R. 50.10(c)(3), before seeking an order directing the recipient of the subpoena not to disclose the existence of the subpoena to any other person or entity, the responsible Assistant Attorney General or United States Attorney must consult with the Criminal Division regarding the need for such order, and may not seek the non-disclosure order until or unless expressly authorized to do so in writing by the Attorney General, the Deputy Attorney General, the Assistant Attorney General for the Criminal Division, or a Deputy Assistant Attorney General for the Criminal Division.

8. **Notice to Criminal Division of Factual or Legal Developments.** When the Attorney General, an Assistant Attorney General, or a United States Attorney has authorized the use of a covered law enforcement tool to obtain information from, or records of, a member of the news media, members of the Department who requested and obtained such authorization shall immediately apprise the Criminal Division of any subsequent changes to or developments in the facts or circumstances relevant to the decision making process (e.g., considerations identified in 28 C.F.R. 50.10(c)(4), (c)(5), (d)(3), or (f)). When such disclosure of changed facts or circumstances is made, the member of the Department may not issue the subpoena or move to compel compliance with the same unless expressly authorized to do so in writing by the Attorney General, the Deputy Attorney General, the Assistant Attorney General for the Criminal Division, or a Deputy Assistant Attorney General for the Criminal Division.

D. Applying for Warrants to Search the Premises, Property, Communications Records, or Business Records of Members of the News Media. 1

1. Except as set forth in 28 C.F.R. 50.10(d)(4), members of the Department must obtain the authorization of the Attorney General to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media. 28 C.F.R. 50.10(d)(1).
2. All requests for the authorization of the Attorney General to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media must personally be endorsed by the United States Attorney or Assistant Attorney General responsible for the matter. 28 C.F.R. 50.10(d)(2).
3. In seeking the authorization of the Attorney General to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media, members of the Department should address both the requirements of the Privacy Protection Act (PPA), 42 U.S.C. 2000aa – 2000aa- 7, and the considerations identified in 28 C.F.R. 50.10(c)(5). 28 C.F.R. 50.10(d)(3).
 - i. **Member of the news media as subject or target.** In matters in which a member of the Department determines that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the member of the Department requesting Attorney General authorization to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media shall provide all facts necessary to a determination by the Attorney

General regarding both whether the member of the news media is a subject or target of the investigation and whether to authorize the application for the warrant. See 28 C.F.R. 50.10(c)(5)(i). If the Attorney General determines that the member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, the Attorney General's determination should take into account both the requirements of the PPA and the principles reflected in 28 C.F.R. 50.10(a), but need not take into account the considerations identified in 28 C.F.R. 50.10(c)(5)(ii) – (viii). *Id.* **Members of the Department must consult with the PSEU regarding whether a member of the news media is a subject or target of an investigation related to an offense committed in the course of, or arising out of, newsgathering activities.**

- ii. **Director of National Intelligence Certification.** In investigations or prosecutions of unauthorized disclosures of national defense information or classified information, the member of the Department requesting Attorney General authorization to apply for a warrant to search the premises, property, communications records, or business records of a member of the news media shall obtain from the Director of National Intelligence a document certifying (1) the significance of the harm raised by the unauthorized disclosure, (2) that the information disclosed was properly classified, and (3) re-affirmance of the intelligence community's support for the investigation or prosecution. 28 C.F.R. 50.10(c)(5)(v). **Because securing the necessary certification from the DNI may take considerable time, members of the Department are encouraged to initiate the process at least 30 days in advance of seeking the Attorney General's authorization, and must coordinate with the National Security Division in seeking the DNI certification.**

- 4. Members of the Department may be authorized to apply for a warrant to obtain work product or other documentary materials of a member of the news media pursuant to the "suspect exception" of the Privacy Protection Act (PPA), 42 U.S.C. 2000aa(a)(1), (b)(1), when the member of the news media is a subject or target of a criminal investigation for conduct not based on, or within the scope of, newsgathering activities. In such instances, members of the Department must secure authorization from a Deputy Assistant Attorney General for the Criminal Division to apply for the warrant. 28 C.F.R. 50.10(d)(4). For example, if a member of the news media is the subject or target of a criminal investigation concerning the production or distribution of child pornography or an investigation concerning extortion, and the conduct is not based on, or within the scope of, such individual's newsgathering activities, an application for a warrant to search the individual's premises, property, communications records, or business records must be approved by a Deputy Assistant Attorney General for the Criminal Division.

Members of the Department must consult with the PSEU regarding whether the conduct at issue is based on, or within the scope of, newsgathering activities.

- 5. Members of the Department should not be authorized to apply for a warrant to obtain work product materials or other documentary materials of a member of the news media under the PPA suspect exception, *see* 42 U.S.C. 2000aa(a)(1) and (b)(1), if the sole purpose is to further the investigation of a person other than the member of the news media. 28 C.F.R. 50.10(d)(5).
- 6. **Searches of Non-Media Premises, Property, Communications Records, or Business Records.**
 - 2 A Deputy Assistant Attorney General (DAAG) for the Criminal Division may authorize an application

for a warrant to search the premises, property, or communications records of an individual ***other than a member of the news media***, e.g., an academic, but who is reasonably believed to have "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. 2000aa(a), (b). *See* 28 C.F.R. 50.10(d)(6).

- i. If the request involves the contemplated search of electronic or digital records, members of the Department shall submit a request to the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS).
 - ii. If the request involves only the contemplated search of physical premises, property, or records, members of the Department shall submit a request to the PSEU.
 - iii. The Criminal Division DAAG will determine (1) whether the individual or entity whose premises, property, or records may be searched is protected by the PPA; and, if so, (2) whether the information sought constitutes "work product materials" or "other documents" as defined by the PPA; and, if so, (3) whether the PPA's suspect exception or another exception to the general prohibition on the search and seizure of such materials is applicable.
7. In executing a warrant authorized by the Attorney General or by a Deputy Assistant Attorney General for the Criminal Division, investigators should use protocols designed to minimize intrusion into potentially protected materials or newsgathering activities unrelated to the investigation, including but not limited to keyword searches (for electronic searches) and filter teams. 28 C.F.R. 50.10(d)(7). Members of the Department should include proposed search and review protocols in their requests for authorization.

E. Notice to Affected Member of the News Media.

1. In matters in which the Attorney General has both determined that a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities, and authorized the use of a subpoena, court order, or warrant to obtain from a third party the communications records or business records of a members of the news media pursuant to 28 C.F.R. 50.10(c)(4)(i), (c)(5)(i), or (d)(1), members of the Department are not required to provide notice of the Attorney General's authorization to the member of the news media. *See* 28 C.F.R. 50.10(e)(1)(i). The Attorney General may, nevertheless, direct that notice be provided. If the Attorney General does not direct that notice be provided, the United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Attorney General within 90 days of the authorization (and every 90 days thereafter) an update regarding the status of the investigation, which update shall include an assessment of any harm that would be caused to the investigation if notice were provided to the affected member of the news media. The Attorney General shall consider such updates in determining whether to direct that notice provided.
2. Except as provided in 28 C.F.R. 50.10(e)(1), when the Attorney General has authorized the use of a subpoena, court order, or warrant to obtain from a third party communications records or business records of a member of the news media, the affected member of the news media shall be given reasonable and timely notice of the Attorney General's determination before the use of the subpoena, court order, or warrant, unless the Attorney General determines that, for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to

national security, or present an imminent risk of death or serious bodily harm. 28 C.F.R. 50.10(e)(2). The mere possibility that notice to the affected member of the news media, and potential judicial review, might delay the investigation is not, on its own, a compelling reason to delay notice. *Id.*

3. When the Attorney General has authorized the use of a subpoena, court order, or warrant to obtain communications records or business records of a member of the news media, and the affected member of the news media has not been given notice, pursuant to 28 C.F.R. 50.10(e)(2), of the Attorney General's determination before the use of the subpoena, court order, or warrant, the United States Attorney or Assistant Attorney General responsible for the matter **shall** provide to the affected member of the news media notice of the subpoena, court order, or warrant as soon as it is determined that such notice will no longer pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm. 28 C.F.R. 50.10(e)(3). In any event, such notice shall occur within 45 days of the government's receipt of any return made pursuant to the subpoena, court order, or warrant, *except that* the Attorney General may authorize delay of notice for an additional 45 days if he or she determines that for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm. *Id.* No further delays may be sought beyond the 90-day period. *Id.*
4. The United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Director of the Office of Public Affairs and to the Director of the Criminal Division's Office of Enforcement Operations a copy of any notice to be provided to the affected member of the news media at least 10 business days before such notice is provided, *and* immediately after such notice is, in fact, provided to the affected member of the news media. 28 C.F.R. 50.10(e)(4).

F. Questioning, Arresting, or Charging Members of the News Media.

1. No member of the Department shall subject a member of the news media to questioning as to any offense which he or she is suspected of having committed in the course of, or arising out of, newsgathering activities without first providing notice to the Director of the Office of Public Affairs and obtaining the express authorization of the Attorney General. 28 C.F.R. 50.10(f)(1).
 - i. The government need not view the member of the news media as a subject or target of an investigation, or have the intent to prosecute the member of the news media, to trigger the requirement that the Attorney General must authorize such questioning. *Id.* **Before questioning a member of the news media, members of the Department must consult with the PSEU whenever the proposed questioning may relate to an offense the member of the news media "is suspected of having committed in the course of, or arising out of, newsgathering activities" even if the government does not view the member of the news media as a subject or target of an investigation, or have the intent to prosecute the member of the news media.**
 - ii. If law enforcement authorities intend to question the member of the news media about criminal conduct he or she is suspected of having committed in the course of, or arising out of, newsgathering activities, the Attorney General must authorize any such questioning.

Conversely, if, at the time the request is made, law enforcement authorities do not intend to question the member of the news media about criminal conduct he or she is suspected of having committed in the course of, or arising out of, newsgathering activities, the Attorney General need not authorize such questioning. **Before questioning a member of the news media, members of the Department must consult with the PSEU whenever the proposed questioning may relate to an offense the member of the news media "is suspected of having committed in the course of, or arising out of, newsgathering activities."**

- iii. This requirement is not intended to inhibit the ability of law enforcement authorities to question or interview members of the news media on a voluntary basis when such questioning does *not* concern criminal conduct the member of the news media is suspected of having committed in the course of, or arising out of, newsgathering activities. For example, members of the Department do not need authorization, pursuant to 28 C.F.R. 50.10, to contact a member of the news media for the purpose of alerting such person to their status as a victim of or witness to a crime, or to question on a voluntary basis such person about their status as a victim of or witness to a crime – even if such status as a victim or witness is related to newsgathering activities. **Before questioning or interviewing a member of the news media in connection with their status as a victim of or witness to a crime, members of the Department must consult with the PSEU to confirm such status.**
2. No member of the Department shall seek a warrant for an arrest, or conduct an arrest, of a member of the news media for any offense which he or she is suspected of having committed in the course of, or arising out of, newsgathering activities without first providing notice to the Director of the Office of Public Affairs and obtaining the express authorization of the Attorney General. 28 C.F.R. 50.10(f)(2). **Before seeking an arrest warrant for, or arresting, a member of the news media, members of the Department must consult with the PSEU regarding whether the member of the news media engaged in the conduct at issue "in the course of, or arising out of, newsgathering activities."**
3. No member of the Department shall present information to a grand jury seeking a bill of indictment, or file an information, against a member of the news media for any offense which he or she is suspected of having committed in the course of, or arising out of, newsgathering activities without first providing notice to the Director of the Office of Public Affairs and obtaining the express authorization of the Attorney General. 28 C.F.R. 50.10(f)(3). **Before charging a member of the news media, members of the Department must consult with the PSEU regarding whether the member of the news media engaged in the conduct at issue "in the course of, or arising out of, newsgathering activities."**
4. In requesting the Attorney General's authorization to question, to seek an arrest warrant for, or to arrest, or to present information to a grand jury seeking an indictment or to file an information against, a member of the news media as provided in 28 C.F.R. 50.10(f)(1) – (f)(3), a member of the Department shall provide all facts necessary for a determination by the Attorney General. 28 C.F.R. 50.10(f)(4). To do so, the member of the Department should submit to the PSEU a memorandum describing the offense under investigation, the status of the investigation, and the role of the member of the news media in the conduct at issue and the relationship to such person's newsgathering activities; and a discussion of the rationale for the proposed questioning, arrest, or charging of the member of the news media in light of the purposes of the policy as set forth in 28 C.F.R. 50.10(a).

G. Exigent Circumstances.

1. A Deputy Assistant Attorney General for the Criminal Division may authorize the use of a subpoena or court order, as described in 28 C.F.R. 50.10(c), or the questioning, arrest, or charging of a member of the news media, as described in 28 C.F.R. 50.10(f), if he or she determines that the exigent use of such law enforcement tool is necessary to prevent or mitigate an act of terrorism; other acts that are reasonably likely to cause significant and articulable harm to national security; death; kidnapping; substantial bodily harm; conduct that constitutes a specified offense against a minor (for example, as those terms are defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006, 42 U.S.C. 16911), or an attempt or conspiracy to commit such a criminal offense; or incapacitation or destruction of critical infrastructure (for example, as defined in section 1016(e) of the USA PATRIOT Act, 42 U.S.C. 5195c(e)). 28 C.F.R. 50.10(g)(1)(i). A Deputy Assistant Attorney General for the Criminal Division may authorize an application for a warrant, as described in 28 C.F.R. 50.10(d), if there is reason to believe that the immediate seizure of the materials at issue is necessary to prevent the death of, or serious bodily injury to, a human being, as provided in 42 U.S.C. 2000aa(a)(2) and (b)(2). 28 C.F.R. 50.10(g)(1)(ii).
2. Within 10 business days of the approval by a Deputy Assistant Attorney General for the Criminal Division of a request for the exigent use of a particular law enforcement tool pursuant to 28 C.F.R. 50.10(g)(1), the United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Attorney General, to the Director of the Office of Public Affairs, and to the Director of the Criminal Division's Office of Enforcement Operations a statement containing the information that would have been provided in a request for prior authorization. 28 C.F.R. 50.10(g)(2).

H. Safeguarding

1. Any information obtained pursuant to a subpoena, court order, or warrant pursuant to 28 C.F.R. 50.10 shall be closely held so as to prevent disclosure of the information to unauthorized persons or for improper purposes. 28 C.F.R. 50.10(h). Specifically,
 - i. Access to information or records obtained from members of the news media or from third parties pursuant to 28 C.F.R. 50.10 shall be limited to personnel who are working on the investigation or related judicial or administrative proceedings and who have a direct need to know.
 - ii. Information or records obtained from members of the news media or from third parties pursuant to 28 C.F.R. 50.10 shall be used solely in connection with the investigation in which it was obtained, or related judicial or administrative proceedings; or for other purposes with the written consent of the affected member of the news media.
 - iii. Information or records obtained from members of the news media or from third parties pursuant to 28 C.F.R. 50.10 may not be shared with any other organization or individual inside or outside of the federal government, except as part of the investigation or as required in the course of judicial proceedings.
 - iv. At the conclusion of all proceedings related to or arising from the investigation, other than information or records disclosed in the course of judicial proceedings, or as required by law, the

Department shall retain only one copy of any records obtained from members of the news media or from third parties pursuant to 28 C.F.R. 50.10, which copy shall be maintained in a secure and segregated repository.

2. If the Attorney General or Deputy Attorney General finds that specific, identifiable records or information constitute evidence of a separate past or imminent crime involving (i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor, as defined by 42 U.S.C. § 16911(7); or (v) incapacitation or destruction of critical infrastructure, as defined by 42 U.S.C. § 5195c(e), the Attorney General or Deputy Attorney General may authorize broader use of the information.

I. **Failure to Comply with Policy.** Failure to obtain the prior approval of the Attorney General, as required by 28 C.F.R. 50.10, may constitute grounds for an administrative reprimand or other appropriate disciplinary action. 28 C.F.R. 50.10(i).

J. **General Provision.** The policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. 28 C.F.R. 50.10(j).

K. Review and Approval Process

1. **Issuing Subpoenas to Members of the News Media, or Using Subpoenas or Court Orders Issued Pursuant to 18 U.S.C. 2703 or 3123 to Obtain From Third Parties Communications Records or Business Records of Members of the News Media.** The Criminal Division shall review and evaluate all requests for the authorization of the Attorney General to issue subpoenas to members of the news media, or to use subpoenas or court orders issued pursuant to 18 U.S.C. 2703 or 3123 to obtain from third parties communications records or business records of a member of the news media, pursuant to 28 C.F.R. 50.10(c). Such requests should be submitted to the PSEU at least 30 business days before the anticipated use of the law enforcement tool, and shall address all applicable considerations identified in 28 C.F.R. 50.10(c)(4) and (c)(5).
2. **Applying for Warrants to Search the Premises, Property, Communications Records, or Business Records of Members of the News Media.** The Criminal Division shall review and evaluate all requests for authorization to apply for warrants to search the premises, property, communications records, or business records of members of the news media (or a person or entity that has "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication."). See 42 U.S.C. § 2000aa(a) and (b); 28 C.F.R. 50.10(d); and JM 9-19.240. Such requests shall be submitted to the PSEU at least 30 business days before the anticipated application for a warrant, and shall address all applicable considerations identified in 28 C.F.R. 50.10(d) and JM 9-19.240.
3. **Questioning, Charging, or arresting Members of the News Media.** The Criminal Division shall review and evaluate all requests for the authorization of the Attorney General to question, arrest, or charge a member of the news media. Such requests should be submitted to the PSEU at least 30 business days before the anticipated questioning, charging, or arrest, and shall address all applicable considerations identified in 28 C.F.R. 50.10(f).

4. **Review by the Director of the Office of Public Affairs.** Unless a Deputy Assistant Attorney General for the Criminal Division has authorized the exigent use of a covered law enforcement tool pursuant to 28 C.F.R. 50.10(g), or unless directed otherwise by the Attorney General, the Assistant Attorney General for the Criminal Division shall forward to the Director of the Office of Public Affairs for review and comment the Criminal Division's recommendation regarding any requests requiring a decision by the Attorney General.
5. **News Media Review Committee.** In February 2014, the Department created the News Media Review Committee to assist in balancing the investigative imperatives with the protection of the public's interest in the freedom of the press. See Memorandum from Attorney General to All Department Employees (Feb. 21, 2014); Memorandum from Deputy Attorney General James M. Cole to Heads of Department Components (Feb. 28, 2014). The News Media Review Committee is comprised of the Department's Chief Privacy and Civil Liberties Officer, the Director of the Office of Public Affairs, and Associate Deputy Attorney General, and two senior career Assistant United States Attorneys with relevant expertise and experience but no involvement (supervisory or otherwise) in the matter under consideration.
 - i. Unless a Deputy Assistant Attorney General for the Criminal Division has authorized the exigent use of a covered law enforcement tool pursuant to 28 C.F.R. 50.10(g), or unless directed otherwise by the Attorney General or the Deputy Attorney General, the Assistant Attorney General for the Criminal Division shall, in the following circumstances, forward to the News Media Review Committee for its review and comment the Criminal Division's recommendation:
 - a. If the request relates to the investigation of unauthorized disclosure of sensitive law enforcement or national defense information;
 - b. If Department attorneys request authorization to seek communications records or business records of a member of the news media without first negotiating with, or providing notice to, the affected member of the news media;
 - c. If Department attorneys request authorization to seek information from, or records of, a member of the news media that would reveal the identity of a confidential source; or
 - d. At the request of the Attorney General or Deputy Attorney General.
 - ii. After reviewing the relevant materials, and consulting with Department personnel, as necessary, the News Media Review Committee will communicate its recommendation in writing to the Attorney General and Deputy Attorney General.
6. **Notice to Criminal Division of Factual or Legal Developments.** When the Attorney General, an Assistant Attorney General, or a United States Attorney has authorized the use of a covered law enforcement tool to obtain information from, or records of, a member of the news media, members of the Department who requested and obtained such authorization shall immediately apprise the Criminal Division of any subsequent changes to or developments in the facts or circumstances relevant to the decision making process (e.g., considerations identified in 28 C.F.R. 50.10(c)(4), (c)(5), (d)(3), or (f)). When such disclosure of changed facts or circumstances is made, the member of the

Department may not issue the subpoena or move to compel compliance with the same unless expressly authorized to do so in writing by the Attorney General, the Deputy Attorney General, the Assistant Attorney General for the Criminal Division, or a Deputy Assistant Attorney General for the Criminal Division.

L. Reporting Requirements

1. When a United States Attorney or Assistant Attorney General has authorized the issuance of a subpoena to a member of the news media when the member of the news media expressly agrees to provide the requested information in response to a subpoena, pursuant to 28 C.F.R. 50.10(c)(3)(i); or has authorized the issuance of a subpoena to a member of the news media, or the use of a subpoena or court order to obtain from a third party the communications records or business records of a member of the news media, pursuant to 28 C.F.R. 50.10(c)(3)(ii), the United States Attorney or Assistant Attorney General shall provide written notice to the Director of Office of Public Affairs and the Director of the Criminal Division's Office of Enforcement Operations within 10 business days of the authorization of the issuance of the subpoena.
2. When the Attorney General has authorized the use of a subpoena, court order, or warrant to obtain from a third party the communications records or business records of a member of the news media, the United States Attorney or Assistant Attorney General responsible for the matter shall provide to the Director of the Office of Public Affairs and to the Director of the Criminal Division's Office of Enforcement Operations a copy of any notice to be provided to the affected member of the news media at least 10 business days before such notice is provided, *and* immediately after such notice is, in fact, provided to the affected member of the news media.
3. Within 10 business days of a Deputy Assistant Attorney General for the Criminal Division authorizing the exigent use of a particular law enforcement tool, pursuant to 28 C.F.R. 50.10(g), the United States Attorney or Assistant Attorney General responsible for the matter shall submit to the Attorney General, to the Director of the Office of Public Affairs, and to the Director of the Criminal Division's Office of Enforcement Operations a statement containing the information that would have been provided in requesting prior authorization.
4. All Department Divisions and United States Attorneys' Offices shall report to the Director of the Office of Public Affairs and to the Director of the Criminal Division's Office of Enforcement Operations by January 31 of each year whether a subpoena, § 2703(d) order, § 3123 order, or warrant, authorized by the Attorney General, or by a Deputy Assistant Attorney General for the Criminal Division, during the preceding calendar year was issued, served, or executed, and whether the affected member of the news media or third-party recipient of the subpoena, court order, or warrant complied with or challenged the same, and the outcome of any such challenge. This information will be used to prepare a public annual report regarding the Department's use of these law enforcement tools.

M. Mandatory Consultations.

1. To ensure the consistent interpretation and application of the policy, members of the Department must consult with the Criminal Division in the following circumstances, or regarding the following determinations:

- i. When there is a question regarding whether an individual or entity is a member of the news media.
 - ii. Whether an individual or entity is not covered by, and therefore not entitled to the protections of, the policy, pursuant to 28 C.F.R. 50.10(b)(1)(ii), which expressly provides that the protections of the policy do not extend to any individual or entity in certain circumstances (e.g., where there are reasonable grounds to believe that the individual or entity is a foreign power or agent of a foreign power).
 - iii. Whether the conduct at issue of the affected member of the news media constitutes or relates to "newsgathering activities."
 - iv. Whether the records sought constitute "communications records" or "business records." See 28 C.F.R. 50.10(b)(3).
 - v. Whether a proposed subpoena or court order falls within one of the exceptions to the Attorney General authorization requirement and, therefore, may be authorized by the United States Attorney or Assistant Attorney General responsible for the matter. See 28 C.F.R. 50.10(c)(3)(ii).
 - vi. Whether a member of the news media is a subject or target of an investigation relating to an offense committed in the course of, or arising out of, newsgathering activities. See 28 C.F.R. 50.10(c)(4)(i), (c)(5)(i), (d)(3), and (e).
 - vii. Whether proposed questioning of a member of the news media may relate to criminal conduct the member of the news media is suspected of having committed an offense in the course of, or arising out of, newsgathering activities. See 28 C.F.R. 50.101(f).
 - viii. Before moving to compel compliance with a subpoena, 2703(d) order, or 3123 order authorized by the Attorney General. 28 C.F.R. 50.10(c)(6).
 - ix. Although not expressly addressed in 28 C.F.R. 50.10, members of the Department must consult with the Criminal Division before taking steps to enforce subpoenas issued to member of the news media, or to compel compliance with subpoenas or court orders issued to third parties for communications records or business records of member of the news media, which subpoenas were issued or court orders obtained in the first instance by other Executive Branch departments or agencies.
 - x. Before seeking an order directing a news media entity-recipient of a subpoena authorized by an Assistant Attorney General or a United States Attorney pursuant to 28 C.F.R. 50.10(c)(3) not to disclose the existence of the subpoena to any other person or entity.
2. To satisfy the consultation requirement, members of the Department must submit to the PSEU a memorandum describing the relevant facts and addressing the relevant considerations. **Members of the Department may not employ the use of the law enforcement tool at issue until the Criminal Division has responded in writing.**

N. **Questions.** Any questions regarding the use of subpoenas, court orders issued pursuant to 18 U.S.C.

2703(d) or 3123, or search warrants to obtain information from, or records of, members of the news media; or regarding questioning, arresting, or charging members of the news media should be directed to the PSEU at pseu@usdoj.gov (link sends e-mail) or (202) 305-4023.

Footnotes

1. In *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), the Supreme Court held that a search of the offices of the Stanford newspaper for photographs that might help a police investigation of violent protests, which the paper had covered, did not violate either the Fourth or the First Amendments. In response, in 1980, Congress enacted the Privacy Protection Act (PPA), 42 U.S.C. 2000aa – 2000aa-7, to provide "the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment." S. Rep. No. 96-874, at 4 (1980), *reprinted in* 1980 U.S.C.C.A.N. 3950. The statute was intended "to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation." *Id.* at 11. The protections of the PPA apply not only to members of the news media, but also to a broader class of persons reasonably believed to have a purpose to disseminate information to the public. For additional guidance, see Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, pp. 101-109.

2. The PPA generally prohibits the search or seizure of "work product materials" or "other documents" possessed by a person, or entity in connection with, "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." Because such materials or documents may be found in the premises, property, communications records, or business records of an individual or entity protected by the PPA, any search of those places may implicate the PPA. Therefore, members of the Department must obtain authorization from a Deputy Assistant Attorney General for the Criminal Division to apply for a warrant to search the premises, property, or communications records of an individual *other than a member of the news media and who is reasonably believed to have a purpose to disseminate to the public a form of public communication*. See 28 C.F.R. 50.10(d)(6).

[updated January 2020] [cited in JM 9-11.140; JM 9-11.255]

9-13.410 - Guidelines for Issuing Subpoenas to Attorneys for Information Relating to the Representation of Clients

- A. **Authorization of the Criminal Division.** Because of the potential effects upon an attorney-client relationship that may result from the issuance of a subpoena to an attorney for information relating to the attorney's representation of a client, the Department exercises close control over such subpoenas. Such subpoenas (for both criminal and civil matters) must first be authorized by the Assistant Attorney General or a Deputy Assistant Attorney General for the Criminal Division before they may issue, *unless* the circumstances warrant application of one of the exceptions set forth in subsection D below. **However, any subpoena to be issued to an attorney in a civil or criminal matter arising principally under the internal revenue laws must be submitted to the Tax Division for authorization pursuant to Tax Division policies and procedures.** In instances requiring Department approval in which the matter arises under both the internal revenue and non-tax laws, the submission must be made to the Criminal Division for authorization, which will consult with the

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THE REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS,

and

THE ASSOCIATED PRESS,

Plaintiffs,

v.

FEDERAL BUREAU OF
INVESTIGATION,

and

UNITED STATES DEPARTMENT
OF JUSTICE,

Defendants.

Civil Action No. 1:15-cv-01392 (RJL)

THE REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS,

Plaintiff,

v.

FEDERAL BUREAU OF
INVESTIGATION,

and

UNITED STATES DEPARTMENT
OF JUSTICE,

Defendants.

Civil Action No. 1:18-cv-00345 (RJL)

THIRD DECLARATION OF DAVID M. HARDY

I, David M. Hardy, declare as follows:

(1) I am the Section Chief of the Record/Information Dissemination Section (“RIDS”), Information Management Division (“IMD”),¹ in Winchester, Virginia. I have held this position since August 1, 2002. Prior to joining the Federal Bureau of Investigation (“FBI”), from May 1, 2001 to July 31, 2002, I was the Assistant Judge Advocate General of the Navy for Civil Law. In that capacity, I had direct oversight of Freedom of Information Act (“FOIA”) policy, procedures, appeals, and litigation for the Navy. From October 1, 1980 to April 30, 2001, I served as a Navy Judge Advocate at various commands and routinely worked with FOIA matters. I am also an attorney who has been licensed to practice law in the State of Texas since 1980.

(2) In my official capacity as Section Chief of RIDS, I supervise approximately 244 employees who staff a total of twelve (12) Federal Bureau of Investigation Headquarters (“FBIHQ”) units and two (2) field operational service center units whose collective mission is to effectively plan, develop, direct, and manage responses to requests for access to FBI records and information pursuant to the FOIA as amended by the OPEN Government Act of 2007, the OPEN FOIA Act of 2009, and the FOIA Improvement Act of 2016; the Privacy Act of 1974; Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and Presidential and Congressional directives. My responsibilities also include the review of FBI information for classification purposes as mandated by Executive Order 13,526, 75 Fed. Reg. 707 (2010), and the preparation of declarations in support of claims asserted under Exemption 1 of the FOIA, 5 U.S.C. § 552(b)(1). I have been designated by the Attorney General of the United States as an original classification authority and a declassification authority

¹ In May 2018, the name of IMD was changed from the Records Management Division (“RMD”).

pursuant to E.O. 13526, §§ 1.3 and 3.1. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) Due to the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to Plaintiffs' requests for information from its files pursuant to the provisions of the FOIA, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. Specifically, I am familiar with the FBI's handling of the FOIA requests submitted by Plaintiffs requesting specific records relating to the Timberline High School Case, specific FBI guidelines and policies concerning undercover operations or activities in which a person may act as a member of the news media and more.

(4) This declaration is my third overall declaration in 1:15-cv-01392 and incorporates my previous declarations dated March 28, 2016, ECF No. 18-1 (hereinafter "First Hardy Declaration"), and my second declaration dated May 20, 2016, ECF No. 22-2 (hereinafter "Second Hardy Declaration"). This Declaration is in response to Plaintiffs' requests being litigated in both 1:15-cv-01392 (Remand) and 1:18-cv-00345 which civil actions were consolidated on February 11, 2019.

(5) The FBI processed a total of 611 responsive pages in response to Plaintiffs' combined FOIA requests in accordance with the court's remand decision in 1:15-cv-1392 and in response to the request being litigated in 1:18-cv-00345. Of the processed pages, 84 pages were released in full, 244 pages were released in part and 283 pages were withheld in their entirety. In accordance with *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), this declaration and accompanying *Vaughn Index* are being submitted in support of Defendants' Motion for Summary Judgment. This declaration provides the Court and Plaintiffs with the FBI's

justifications for withholding information in full or part pursuant to FOIA Exemptions 1, 3, 5, 6, 7(C), and 7(E), 5 U.S.C. §§ 552 (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E).

HISTORY OF PLAINTIFFS' FOIA REQUESTS

FOIPA Request Numbers 1313500-000, 1313504-000 1319113-000 and 1319138-000

(6) The history of Plaintiffs' FOIA requests specifically related to FOIPA Request Numbers 1313500-000, 1313504-000, 1319113-000 and 1319138-000 is set forth in my First Hardy Declaration in 1:15-cv-01392 (REMAND) and will not be recounted herein. *See* ECF No. 18-1, ¶¶ 5-33.

(7) On February 23, 2017, the District Court issued a Memorandum Opinion and entered an Order granting Defendant's Motion for Summary Judgment and Denying the Plaintiffs' Motion for Summary Judgment and/or Partial Summary Judgment and Motion for *In Camera* Review. *See* ECF Nos. 27 and 28.

(8) Plaintiffs' appealed the District Court's decision on the adequacy of Defendants' search to the United States Court of Appeals for the District of Columbia Circuit on or about March 14, 2017 and assigned Court of Appeals Docket No. 17-5042.

(9) On December 15, 2018, the United States Court of Appeals for the District of Columbia Circuit entered its opinion in re: Reporters Committee for Freedom of the Press and Associated Press v. Federal Bureau of Investigation and United States Department of Justice, No. 17-5042, concerning the FBI's searches for records responsive to Plaintiffs' requests. The court determined the FBI should 1) "set[] forth the search terms and the type of search performed" with specificity for the targeted searches it conducted; 2) search the same divisions for records for both Group I and Group II requests in a manner "reasonably expected to produce the information requested;" and 3) follow a clear and apparent lead indicating the Director's Office would likely maintain records responsive to Plaintiffs' requests.

(10) On February 8, 2018, the court entered a mandate, remanding Civil Action 1:15-cv-01392 to the United States District Court for the District of Columbia for further proceedings.

(11) Prior to the US Court of Appeal's opinion and mandate, Plaintiff Reporters Committee for Freedom of the Press ("RCFP"), submitted a new FOIA request to the FBI dated December 5, 2017. The new request sought later-in-time records were substantively similar to those requested by RCFP in its original request dated October 31, 2014, being litigated in 1:15-cv-01392. The new request also sought (1) information concerning comments provided by the FBI to the Department of Justice Office of the Inspector General in response to a draft OIG report, and (2) information concerning the FBI's Interim Policy Notice 0907N, including revisions, modifications and updates to the policy and records discussing the FBI's efforts to inform its employees of this interim policy. More specific details concerning this new FOIA request are discussed below.

FOIPA Request Numbers 1391028-000, 13935000, 1393558-000 and 1393559-000

(12) By letter dated December 5, 2017, Adam A. Marshall, on behalf of Plaintiff, Reporters Committee for Freedom of the Press, submitted a FOIA request, requesting the following:

1. All records consisting of, reflecting, referencing, or discussing the FBI's utilization of links to what are or appear to be news media articles or news media websites to install data extraction software, remote access search and surveillance tools, or the "Computer and Internet Protocol Address Verifier" ("CIPAV"), since November 1, 2014.
2. All records consisting of or reflecting the FBI's guidelines and policies concerning undercover operations or activities in which a person may act as a member of the news media, since November 1, 2014.
3. The FBI's Interim Policy Notice (PN) 0907N, adopted on or about June 7, 2016, and titled "Undercover Activities and Operations – Posing as a Member of the News Media or Documentary Film Crew" (the "Interim Policy Notice"). The Interim Policy Notice is referenced on pages ii, 2, 7-8, and 22 of a report titled "A Review of the FBI's Impersonation of a Journalist in a

Criminal Investigation” published by the Department of Justice’s Office of the Inspector General in September 2016 (the “IG Report”). A true and correct copy of the IG Report is attached hereto as Exhibit A.

4. The “comments” provided by the FBI to the Department of Justice Office of the Inspector General in response to a draft of the IG Report, and referenced in footnote 30 of the IG Report. *See* Ex. A.
5. Any and all records consisting of, referencing, or discussing FBI efforts to inform its employees about the Interim Policy Notice.
6. Any and all revisions, updates, or modifications to the Interim Policy Notice since June 8, 2016.

(*See* **Exhibit A.**)

(13) By letter dated December 11, 2017, the FBI acknowledged receipt of Plaintiff’s FOIA request and assigned it FOIPA Request Number 1391028-000. The FBI advised for the purposes of assessing fees it determined Plaintiff was either an educational institution, noncommercial scientific institution or a representative of the news media, and would be charged for only applicable duplication fees in accordance with 5 U.S.C. § 552(a)(4)(A)(ii)(II). The FBI further advised Plaintiff it could check the status of its request, or provide questions as to any FBI determinations, at www.fbi.gov/foia. Finally, the FBI advised Plaintiff of its right to appeal the FBI’s response determination by writing to the U.S. Department of Justice (“DOJ”), Office of Information Policy (“OIP”), within ninety (90) days from the date of this letter, or seek dispute resolution services by contacting the Office of Government Information Services (“OGIS”). (*See* **Exhibit B.**)

(14) By a second letter dated December 11, 2017, the FBI advised Plaintiff that “unusual circumstances” applied to the processing of the request, pursuant to 5 U.S.C. § 552(a)(6)(B)(iii), because there was: 1) a need to search for and collect records from field offices and/or other offices separate from RIDS; 2) a need to search for, collect, and examine a

voluminous amount of separate and distinct records; or 3) a need for consultation with another agency or two or more DOJ components. The FBI also advised Plaintiff that the payment of pertinent fees may apply to the request under 5 U.S.C. § 552(a)(4)(A)(viii). Finally, the FBI advised Plaintiff of its right to appeal the FBI's response determination by writing OIP, within ninety (90) days from the date of this letter, or seek dispute resolution services by contacting OGIS. (See **Exhibit C.**)

(15) By letter dated January 23, 2018, the FBI advised Plaintiff that because its request previously assigned FOIPA Request No. 1391028-000 requested records about multiple subjects and for administrative tracking purposes, additional FOIA numbers were assigned to the request as follows:

FOIPA Request No. 1393556-000

Subject: All records related to the FBI's utilization of links to news media articles or websites to install data extraction software, remote access search and surveillance tools, or the "Computer and Internet Protocol Address Verifier" (CIPAV) (November 1, 204 – Present)

FOIPA Request No. 1393558-000

Subject: Records related to the FBI's Interim Policy Notice (PN) 0907N (including: FBI efforts to inform its employees about the PN, and any/all revisions, updates, or modification to the PN)

FOIPA Request No. 1393559-000

Subject: "Comments" provided by the FBI to DOJ/OIG in response to a draft of IG Report (Footnote 30 of the IG Report "A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation")

The FBI further advised Plaintiff that it could check the status of its request, or provide questions as to any FBI determinations, at www.fbi.gov/foia. Finally, Plaintiff was advised of its right to appeal the FBI's response determination by writing to the OIP, within ninety (90) days from the date of this letter, or seek dispute resolution services by contacting the OGIS, by telephone or by email at ogis@nara.gov. (See **Exhibit D.**)

(16) On February 14, 2018, RCFP filed a complaint in the United States District Court for the District of Columbia, styled *Reporters Committee for Freedom of the Press v. Federal Bureau of Investigation, et al.* and assigned Civil Action No. 1:18-cv-00345. The complaint requested that the Court order Defendants to conduct a search reasonably calculated to identify all records responsive to their December 5, 2017 request; enjoin Defendants from withholding all records or portions thereof responsive to their request that are not specifically exempt from disclosure under FOIA; issue a declaration that Plaintiff is entitled to disclosure of the requested records; award Plaintiff reasonable attorney fees and costs reasonably incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E); and grant such other relief as this Court may deem just and proper. *See ECF No. 1.*

(17) On March 9, 2018, RCFP also filed a Motion to Consolidate Civil Action 1:15-cv-01392 and 1:18-cv-00345. *See ECF No. 33.*

(18) By letter dated July 13, 2018, the FBI made a combined interim release of records to Plaintiffs in response to its litigated requests in Civil Actions 1:15-cv-01392 and 1:18-cv-00345. The FBI advised Plaintiffs it reviewed 106 pages and 32 pages were being released in full or in part, with certain information withheld pursuant to FOIA Exemptions (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E). The FBI further advised Plaintiffs they could appeal the FBI's decision by submitting an appeal, by mail or online with OIP, within ninety days from the date of the letter; or seek dispute resolution services by contacting OGIS by telephone or by emailing ogis@nara.gov. Finally, the FBI advised Plaintiffs that records Bates-numbered RCFP-270 thru RCFP-283, RCFP-287 thru RCFP-302 and RCFP-319 thru RCFP-375 are responsive to requests being litigated in 1:18-cv-00345 and that RCFP-284 thru RCFP-286 and RCFP-303 thru RCFP-

318 are responsive to requests being litigated in both 1:15-cv-01392 and 1:18-cv-00345. (See **Exhibit E.**)

(19) By letter dated August 15, 2018, the FBI made an additional combined interim release of records to Plaintiffs in response to its litigated requests in Civil Actions 1:15-cv-01392 and 1:18-cv-00345. The FBI advised Plaintiffs it reviewed 414 pages and 243 pages were being released in full or in part, with certain information withheld pursuant to FOIA Exemptions (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E). The FBI further advised Plaintiffs they could appeal the FBI's decision by submitting an appeal, by mail or online with OIP, within ninety days from the date of the letter; or seek dispute resolution services by contacting OGIS by telephone or by emailing ogis@nara.gov. In addition, the FBI advised Plaintiffs that records Bates-numbered RCFP-378 thru RCFP-666, RCFP-683 thru RCFP-736, RCFP-754 thru RCFP-763 and RCFP-770 thru RCFP-789 are responsive to requests being litigated in 1:18-cv-00345; RCFP-667 thru RCFP-682 and RCFP-737 thru RCFP-753 are responsive to requests being litigated in both 1:15-cv-01392 and 1:18-cv-00345; and RCFP-376 thru RCFP-377 and RCFP-764 thru RCFP-769 are responsive to requests being litigated in 1:15-cv-01392. Finally, the FBI advised Plaintiffs additional material responsive to their request was previously processed and to avoid charging duplication fees unnecessarily, the FBI made these releases available on The Vault.² (See **Exhibit F.**)

(20) By letter dated September 14, 2018, the FBI made an additional combined interim release of records to Plaintiffs in response to its litigated requests in Civil Actions 1:15-cv-01392 and 1:18-cv-00345. The FBI advised Plaintiffs its consultations with other government agencies

² The responsive records are located on the Vault under two subject headings: (1) FBI Domestic Investigations and Operations Guide (DIOG) 2016 Version Part 01 and 02; and (2) FBI Domestic Investigations and Operations Guide (DIOG) 2016 Version Part 02 of 02.

were completed and information was withheld pursuant to FOIA Exemptions (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E).³ Deletions were made by the Federal Bureau of Investigation, the Department of Justice, Office of Inspector General and/or the Central Intelligence Agency. The FBI further advised Plaintiffs they could appeal the FBI's decision by submitting an appeal, by mail or online with OIP, within ninety days from the date of the letter; or seek dispute resolution services by contacting OGIS by telephone or by emailing ogis@nara.gov. In addition, the FBI advised Plaintiffs that records Bates-numbered RCFP-319 thru RCFP-375, RCFP-788 thru RCFP-789 are responsive to requests being litigated in 1:18-cv-00345. Finally, the FBI advised Plaintiffs that upon further review of the processed records, it was determined on Bates-numbered page RCFP-291 in the 5th redaction box, there was no coding notated for the FBI's assertion of (b)(6) and (b)(7)(C) to withhold the information. They were advised that the redaction box should identify (b)(6)-1 and (b)(7)(C)-1. (See **Exhibit G.**)

(21) By letter dated January 10, 2019, the FBI made an additional combined interim release of records to Plaintiffs in response to its litigated requests in Civil Actions 1:15-cv-01392 and 1:18-cv-00345. The FBI advised Plaintiffs it reviewed 1 page and 1 page was being released in full or in part, with certain information withheld pursuant to FOIA Exemption (b)(7)(E). The FBI further advised Plaintiffs to direct any further inquiries to the attorney representing the Government in this matter. Finally, the FBI advised Plaintiffs record Bates-numbered RCFP-790 is responsive to requests being litigated in 1:15-cv-01392. (See **Exhibit H.**)

³This release addressed 59 pages of records previously reviewed by the FBI and withheld as Referral/Consult in its' July 13, 2018 and August 15, 2018 releases. Of the 59 pages sent to other government agencies for consultation, 5 pages were released in full or in part to Plaintiffs and 54 pages were withheld in full as either duplicate or pursuant to applicable FOIA Exemptions.

(22) On February 11, 2019, the Court granted the Plaintiffs' Motion to Consolidate Civil Action 1:15-cv-01392 and 1:18-cv-00345 and directed the parties to make all future filings in Civil Action 1:15-cv-01392.

(23) By letter dated May 10, 2019, the FBI made an additional combined interim release of records to Plaintiffs in response to its litigated requests in Civil Actions 1:15-cv-01392 and 1:18-cv-00345. The FBI advised Plaintiffs it reviewed 27 pages and 13 pages were being released in full or in part, with certain information withheld pursuant to FOIA Exemptions (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E). The FBI further advised Plaintiffs to direct any further inquiries to the attorney representing the Government in this matter. In addition, the FBI advised Plaintiffs records Bates-numbered RCFP-791 thru RCFP-812 are responsive to requests being litigated in 1:15-cv-01392 and records Bates-numbered RCFP-813 thru RCFP-817 are responsive to 1:18-cv-00345. Finally, the FBI advised Plaintiffs that the Central Intelligence Agency determined that information it previously withheld on RCFP-789 may be released and therefore, the FBI reprocessed this page and included it as part of this release. (See **Exhibit I**.)

(24) By letter dated May 31, 2019, the FBI made its final release of records to Plaintiffs in response to its litigated requests in Civil Actions 1:15-cv-01392 and 1:18-cv-00345. The FBI advised Plaintiffs it reviewed 63 pages and 34 pages were being released in full or in part, with certain information withheld pursuant to FOIA Exemptions (b)(5), (b)(6), and (b)(7)(C). Deletions were made by the Federal Bureau of Investigation and the Department of Justice, Office of Inspector General. The FBI further advised Plaintiffs to direct any further inquiries to the attorney representing the Government in this matter. Finally, the FBI advised Plaintiffs records Bates-numbered RCFP-818 thru RCFP-880 are responsive to requests being litigated in 1:18-cv-00345. (See **Exhibit J**.)

FBI'S SEARCH FOR RESPONSIVE RECORDS

(25) FBI/RIDS conducted searches reasonably calculated to locate responsive records subject to the FOIA. Specifically, FBI conducted searches within its Seattle Field Office, where the Timberline High School case originated; Discovery Processing Units and National Security and Cyber Law Branch within its Office of General Counsel; Operational Technology Division; Criminal Cyber Response and Services Branch; the Behavioral Analysis Unit within the Critical Incident Response Group; Cyber Division; Criminal Investigative Division; Training Division; Office of Public Affairs; Office of Congressional Affairs; Inspection Division; National Security Branch; and Internal Policy Office. The FBI also conducted limited email searches of its unclassified and classified email systems sent to or received by former FBI Director James Comey and former Section Chief Michael T. Gavin. In addition, the FBI conducted a search of archived records associated with the Director's Office that fell within the date range of Plaintiff's initial FOIA request.

(26) Thus, the FBI conducted adequate searches reasonably calculated to locate records responsive to Plaintiffs' requests and subject to the FOIA; located responsive records; and identified no leads to additional responsive records within the scope of Plaintiffs' requests.

JUSTIFICATION FOR NONDISCLOSURE UNDER THE FOIA

Explanation of the Coded Format Used to Describe and Justify Withholdings

(27) All documents responsive to Plaintiffs' requests and subject to the FOIA were processed to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide Plaintiffs with all material in the public domain and with all reasonably segregable non-exempt information in the responsive records. No reasonably segregable, non-exempt portions have been withheld from Plaintiffs. Further description of the information withheld, beyond what is provided in this declaration, could identify the actual

exempt information that the FBI has protected. Copies of the pages released in part and in full have been consecutively numbered “RCFP - 270 through RCFP - 880” at the bottom of each page. Pages withheld in their entirety (*e.g.*, removed per exemption or duplicates) were replaced by a “Deleted Page Information Sheet” (“DPIS”), identifying the reason and/or the applicable FOIA exemptions relied upon to withhold the pages in full, as well as Bates numbers for the withheld material. The DPISs and Bates-numbered pages that were withheld in part were provided to Plaintiffs and will be made available to the Court upon request. The exemptions asserted by the FBI as grounds for non-disclosure of portions of documents are FOIA Exemptions 1, 3, 5, 6, 7(C) and 7(E), 5 U.S.C. § 552 (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E).

(28) The Bates-numbered documents contain, on their face, coded categories of exemptions that detail the nature of the information withheld pursuant to the provisions of the FOIA. The coded categories are provided to aid the Court’s and Plaintiffs’ review of the FBI’s explanation of the FOIA exemptions it asserted to withhold material. The coded, Bates-numbered pages together with this declaration and *Vaughn* Index attached hereto as **Exhibit K** demonstrate that all material withheld by the FBI is exempt from disclosure pursuant to the cited FOIA exemptions, or is so intertwined with protected material that segregation is not possible without revealing the underlying protected material.

(29) Each instance of information withheld on the Bates-numbered documents is accompanied by a coded designation that corresponds to the categories listed below. For example, if (b)(7)(C)-1 appears on a document, the “(b)(7)(C)” designation refers to FOIA Exemption (7)(C) protecting against unwarranted invasions of personal privacy. The numerical designation of “1” following the “(b)(7)(C)” narrows the main category into a more specific

subcategory, such as “Names and/or Identifying Information of FBI Special Agents/Professional Staff.”

(30) Listed below are the categories used to explain the FOIA exemptions asserted to withhold the protected material:

SUMMARY OF JUSTIFICATION CATEGORIES	
CODED CATEGORIES	INFORMATION WITHHELD
Exemption (b)(1)	INFORMATION CLASSIFIED PER EXECUTIVE ORDER 13,526
(b)(1)-1	Intelligence Activities, Sources and Methods (E.O. 13526 §1.4(c) <i>[cited at times in conjunction with (b)(3)-1]</i>
Exemption (b)(3)	INFORMATION PROTECTED BY STATUTE
(b)(3)-1	National Security Act of 1947 [50 U.S.C. Section 3024(i)(1)] <i>[cited at times in conjunction with (b)(1)-1]</i>
(b)(3)-2	This Coded Category is no longer being applied to Bates-numbered pages RCFP-609.
Exemption (b)(5)	PRIVILEGED INFORMATION
(b)(5)-1	Deliberative Process Privilege
Exemption (b)(6) and Exemption (b)(7)(C)	CLEARLY UNWARRANTED INVASION OF PERSONAL PRIVACY AND UNWARRANTED INVASION OF PERSONAL PRIVACY
(b)(6)-1 and (b)(7)(C)-1	Names and/or Identifying Information of FBI Special Agents and Professional Staff
(b)(6)-2 and (b)(7)(C)-2	Name and/or Identifying Information of Non-FBI Federal Government Personnel
(b)(6)-3 and (b)(7)(C)-3	Names and/or Identifying Information of Third Parties Investigative Interest
(b)(6)-4 and (b)(7)(C)-4	Names and/or Identifying Information of Third Parties Merely Mentioned
(b)(6)-5 and (b)(7)(C)-5	Names and/or Identifying Information of Local Law Enforcement Personnel

Exemption (b)(7)(E)	LAW ENFORCEMENT INVESTIGATIVE TECHNIQUES AND PROCEDURES
(b)(7)(E)-1	Operational Directives
(b)(7)(E)-2	Undercover Operation
(b)(7)(E)-3	Identity and/or Location of FBI or Joint Units, Squads, Divisions
(b)(7)(E)-4	Internal FBI Secure Fax Number, Email or IP Address, Intranet/Web Address
(b)(7)(E)-5	Sensitive Investigative Techniques and Procedures, Including the Deployment of Computer and Internet Protocol Address Verifier ("CIPAV")
(b)(7)(E)-6	This Coded Category is not applicable to Bates-numbered pages RCFP-270 through RCFP-880.
(b)(7)(E)-7	Collection and Analysis of Information
(b)(7)(E)-8	This Coded Category is no longer being applied to Bates-numbered pages RCFP-279 thru RCFP-282 and RCFP-799. Instead, the FBI upon further review of the records has determined all assertions of (b)(7)(E)-8 on these Bates-numbered pages is changed to (b)(7)(E)-1. <i>See ¶ 73, infra.</i>
(b)(7)(E)-9	This Coded Category is no longer being applied to Bates-numbered pages RCFP-279 thru RCFP-282.
(b)(7)(E)-10	Sensitive File Numbers or Subfile Names

(31) The large majority of the withholdings made pursuant to FOIA Exemption Coded Categories (b)(1)-1, (b)(3)-1, (b)(5)-1, (b)(6)/(b)(7)(C)-1 thru -5, and (b)(7)(E)-1 thru -5, and -7, in the records Bates-numbered RCFP-270 through RCFP-880 are either similar to, or identical to the withholdings made in the prior productions previously briefed in 1:15-cv-01392; wherein this Honorable Court entered its February 23, 2017 Memorandum Opinion and Order granting the Defendants' Motion for Summary Judgment and denying Plaintiffs' Motion for Summary Judgment and/or Partial Summary Judgment and Plaintiffs' Motion for In Camera Review and/or Other Appropriate Relief. *See ECF Nos. 27 and 28.* The withholdings that were not previously addressed in the prior briefing relate to information withheld pursuant to FOIA Exemption Coded Categories (b)(7)(E)-3 and (b)(7)(E)-10.

EXEMPTION (b)(1)
CLASSIFIED INFORMATION

(32) The FBI's analysis for the withholding of classified information contained in these documents is based on the standards articulated in the FOIA statute, 5 U.S.C. § 552(b)(1). Exemption (b)(1) protects from disclosure those records that are:

- (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 pursuant to such Executive Order.

(33) Before I consider an Exemption (b)(1) claim for withholding agency records, I determine whether the information in those records satisfies the requirements of Executive Order ("E.O. ")13526, the E.O. governing the classification and protection of information that affects the national security,⁴ and whether the information complies with the various substantive and procedural criteria of the E.O. E.O. 13526, signed by President Barack Obama on December 29, 2009, is the E.O. that currently applies to the protection of national security information. I am bound by the requirements of E.O. 13526, when making classification determinations.

(34) In order for information to be properly classified, and thus properly withheld from disclosure pursuant to Exemption (b)(1), the information must meet the requirements set forth in E.O. 13526 § 1.1 (a):

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in § 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in

⁴ Section 6.1 (cc) of E.O. 13526, defines "National Security" as "the national defense or foreign relations of the United States."

damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(35) As I will explain in further detail below, in my role as an original classification authority, I have determined that the information withheld pursuant to Exemption (b)(1) is under the control of the United States Government, is classified and requires a classification marking at the "Secret" level since the unauthorized disclosure of this information reasonably could be expected to cause serious damage to national security. *See* E.O. 13526 § 1.2(a)(2). In addition to these substantive requirements, certain procedural and administrative requirements of E.O. 13526 must be followed before information can be considered properly classified, such as, proper identification and marking of documents. In particular, I made certain that all procedural requirements of E.O. 13526 were followed:

- (1) each document was marked as required and stamped with the proper classification designation;
- (2) each document was marked to indicate clearly which portions are classified, which portions are exempt from declassification as set forth in E.O. 13526 § 1.5(b);
- (3) the prohibitions and limitations on classification specified in E.O. 13526 § 1.7 were adhered to;
- (4) the declassification policies set forth in E.O. 13526 §§ 3.1 and 3.3 were followed; and
- (5) any reasonably segregable portions of these classified documents that did not meet the standards for classification under E.O. 13526 were declassified and marked for release, unless withholding was otherwise warranted under applicable law.

FINDINGS OF DECLARANT REGARDING
EXEMPTION (b)(1)

(36) With the above requirements in mind, I personally and independently examined the FBI information withheld pursuant to Exemption (b)(1) in two documents. The first

document, Bates-numbered RCFP 376 is an email dated October 31, 2014 forwarded to Ronald J. Yearwood on April 24, 2018 providing him responses to the Deputy Assistant Director's (DAD's) detailed questions about the mechanics of the Seattle Timberline investigation. The second document, Bates-numbered RCFP 721 and 722, is an attachment to an email and contains references from the National Security Undercover Operations Policy Implementation Guide ("NSUOPG") provided by Chief Michael T. Gavin to specific FBI personnel and counsel thought to be of assistance to them as they reviewed issues to be covered at an upcoming briefing. As a result of this examination, I determined the classified information continues to warrant classification at the "Secret" level pursuant to E.O. 13526 § 1.4 category (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology as the unauthorized disclosure of information that could reasonably be expected to cause serious damage to the national security. Therefore; the FBI is asserting FOIA Exemption (b)(1) to withhold this information.

INTELLIGENCE ACTIVITIES, SOURCES AND METHODS

(37) E.O. 13526 § 1.4 (c) exempts intelligence activities (including covert action), intelligence sources or methods, or cryptology. An intelligence activity or method includes any intelligence action or technique utilized by the FBI against a targeted individual or organization that has been determined to be of a national security interest. An intelligence method is used to indicate any procedure (human or non-human) utilized to obtain information concerning such individual or organization. An intelligence activity or method has two characteristics. First, the intelligence activity or method – and information generated by it – is needed by U.S. intelligence/counterintelligence agencies to carry out their missions. Second, confidentiality

must be maintained with respect to the activity or method if the viability, productivity and usefulness of its information is to be preserved.

(38) Classification redactions may be made to protect from disclosure information that would reveal the actual intelligence activities and methods used by the FBI against specific targets of foreign counterintelligence investigations or operations; identify a target of a foreign counterintelligence investigation; or disclose the intelligence gathering capabilities of the activities or methods directed at specific targets. The criteria utilized in determining what actions by an individual or organization warrant the commencement of an investigation, or cause a certain activity to be given investigative attention over others, could be revealed through disclosure of these intelligence methods or activities. In the records at issue, the FBI protected information pertaining to specific FBI's intelligence sources and methods, including its intelligence gathering capabilities. Specifically, the sources and methods described in these records are used by the FBI in current national security investigations (i.e. intelligence or counterintelligence investigations). Disclosure could reasonably be expected to cause serious damage to the national security. As a result, I have determined this information is properly classified at the "Secret" level, properly classified pursuant to E.O. 13526 § 1.4(c) and is exempt from disclosure pursuant to FOIA Exemption (b)(1). This harm justification applies to all (b)(1) material withheld under E.O. 13526 § 1.4(c).

**DEFENDANT'S BURDEN OF ESTABLISHING
EXEMPTION (b)(1) CLAIMS**

(39) The information withheld in this case pursuant to Exemption 1 was examined in light of the body of information available to me concerning the national defense and foreign relations of the United States. This information was not examined in isolation. Instead, the information was evaluated with careful consideration given to the impact that disclosure of this

information will have on other sensitive information contained elsewhere in the United States' intelligence files, including the secrecy of that other information. Equal consideration was given to the impact that other information, either in the public domain or likely known or suspected by present or potential adversaries of the United States, would have upon the information I examined, and upon attempts by a hostile entity to analyze such information.

(40) In those instances where, in my judgment, the disclosure of this information could reasonably be expected to cause a serious damage to the national security, and its withholding outweighed the benefit of disclosure, I exercised my prerogative as an original classification authority and designated that information as classified in the interest of national security at the "Secret" level, and invoked FOIA Exemption (b)(1) to prevent disclosure. Likewise, the justifications for the withheld classified information have been prepared with the intent that they be read with consideration given to the context in which the classified information is found, but also other information already in the public domain, as well as information likely known or suspected by hostile intelligence entities. It is my judgment that any greater specificity in the description and justification set forth with respect to the intelligence activities (including special activities) or intelligence sources or methods could reasonably be expected to jeopardize the national security of the United States. As a result, the classified information appearing in these documents has been appropriately classified pursuant to E.O. 13526 and withheld pursuant to FOIA Exemption (b)(1). A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(1)-1 is set forth in the attached *Vaughn* Index, **Exhibit K**.

EXEMPTION (b)(3)
INFORMATION PROTECTED BY STATUTE⁵

(41) 5 U.S.C. § 552(b)(3) exempts from disclosure information which is:

specifically exempted from disclosure by statute... provided that such statute (A) (i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.

(b)(3)-1 National Security Act of 1947 [50 U.S.C. § 3024(i)(1)]

(42) Exemption (b)(3)-1 was asserted in conjunction with Exemption 1, in references from the National Security Undercover Operations Policy Implementation Guide (NSUOPG) provided by Chief Michael T. Gavin to specific FBI personnel and counsel thought to be of assistance to them as they reviewed issues to be covered at an upcoming briefing, to withhold information pursuant to Section 102A(i)(1) of the National Security Act of 1947 (“NSA”), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (“IRTPA”), 50 U.S.C. §3024(i)(1), which provides that the Director of National Intelligence (“DNI”) “shall protect from unauthorized disclosure intelligence sources and methods.”⁶ As relevant to U.S.C. § 552(b)(3)(B), the National Security Act of 1947 was enacted before the date of enactment of

⁵ Upon further review of the records, the FBI is no longer asserting underlying Exemption (b)(3)-2, pursuant to 18 U.S.C. § 3123 to withhold Bates-numbered page RCFP-609. It was earlier determined and set forth in 15-cv-01392 (Remand), in the Second Declaration of David M. Hardy (ECF No. 22-2) that Exemption 3 pursuant to 18 U.S.C. § 3123 was no longer sustainable, since a relevant court order was unsealed in the FBI’s investigation demonstrating the FBI’s request for a pen register. Notwithstanding the same, the FBI continues to assert Exemptions (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E) to withhold RCFP-609 in its entirety.

⁶ Section 1024(i)(1) of the National Security Act was previously codified at 50 U.S.C. § 403(i)(1). As a result of the reorganization of Title 50 of the U.S. Code, Section 102A(i)(1) is now codified at 50 U.S.C. § 3024(i)(1).

the OPEN FOIA Act of 2009.⁷ On its face, this federal statute leaves no discretion to agencies about withholding from the public information about intelligence sources and methods. Thus, the protection afforded to intelligence sources and methods by 50 U.S.C. § 3024(i)(1) is absolute. *See CIA v. Sims*, 471 U.S. 159 (1985).

(43) In order to fulfill its obligation of protecting intelligence sources and methods, the DNI is authorized to establish and implement guidelines for the Intelligence Community (“IC”) for the classification of information under applicable laws, Executive Orders, or other Presidential Directives, and for access to and dissemination of intelligence. 50 U.S.C. § 3024(i)(1)(i)(1). The FBI is one of 17 member agencies comprising the IC, and as such must protect intelligence sources and methods.

(44) As described above, Congress enacted the NSA, as amended by the IRTPA, to protect the IC’s sources and methods of gathering intelligence. Disclosure of such information presents the potential for individuals to develop and implement countermeasures, which would result in the loss of significant intelligence information, relied upon by national policymakers and the IC. Given that Congress specifically prohibited the disclosure of information pertaining to intelligence sources and methods used by the IC as a whole, I have determined the FBI’s intelligence sources and methods would be revealed if any of the withheld information is disclosed to Plaintiffs, and thus, the FBI is prohibited from disclosing the information under 50 U.S.C. § 3024(i)(1). Thus, this information was properly withheld pursuant to Exemption 3, at times in conjunction with Exemption 1. A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(3)-1 is set forth in the attached *Vaughn* Index, **Exhibit K**.

⁷ The OPEN FOIA Act of 2009 was enacted October 28, 2009, Pub.L. 111-83, 123 Stat. 2142, 2184; 5 U.S.C. §552(b)(3)(B).

EXEMPTION (b)(5) - PRIVILEGED INFORMATION

(45) FOIA Exemption 5 protects “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.” 5 U.S.C. § 552(b)(5).

(46) Exemption 5 has been construed to exempt documents or information normally privileged in the civil discovery context and incorporates, *inter alia*, the attorney work product, attorney-client and deliberative process privileges. Generally, the attorney work product privilege protects documents and other memoranda prepared by an attorney or under the direction of an attorney as part of, or in reasonable anticipation of litigation. The attorney-client privilege protects confidential communications from a client to an attorney and from an attorney to a client for the purpose of seeking and providing legal advice. The deliberative process privilege protects predecisional, deliberative communications that are part of a process by which agency decisions are made. It protects materials prepared as part of an agency decisionmaker’s formulation of opinions, advice, evaluations, deliberations, policies, proposals, conclusions, or recommendations.

(47) In order to apply Exemption 5, agencies must first satisfy the threshold requirement – *i.e.*, show that the information protected was “inter-agency or intra-agency.” Once the threshold is satisfied, agencies must satisfy the element of the pertinent privilege. With respect to the attorney work product privilege, agencies must show that the withheld information was created by, or for, an attorney in reasonable anticipation of litigation. With respect to attorney-client privilege, agencies must show that the withheld information concerns confidential information shared by a client with an attorney for the purpose of obtaining legal advice or assistance, or legal advice or assistance provided by an attorney to a client reflecting confidential

information. With respect to the deliberative process privilege, agencies must show that the withheld information was both pre-decisional – *i.e.*, antecedent to a final agency decision – and deliberative – *i.e.*, part of the process in which the agency engaged in an effort to reach a final decision (whether or not any final decision was ever reached).

(b)(5)-1 Deliberative Process Privilege

(48) In Coded Category (b)(5)-1 the FBI protected privileged deliberative materials within the responsive records. The general purpose of the deliberative process privilege is to prevent injury to the quality of agency decisions. Thus, material containing or prepared in connection with the formulation of opinions, advice, evaluations, deliberations, policies, proposals, conclusions, or recommendations may properly be withheld. The privilege also protects records and information that if disclosed, would reveal the agency's collection of multitudinous facts, and the sorting, evaluation, and analysis of those facts in order to make recommendations or reach a final agency decision. The agency's treatment of such information is itself, a deliberation and is a deliberative process properly protected by the privilege. Disclosure of this type of information would have an inhibiting effect upon agency decision-making and the development of policy because it would chill full and frank discussions between agency personnel and decision makers regarding a decision. If agency personnel know that their preliminary impressions, opinions, evaluations, or comments would be released to the general public, they would be less candid and more circumspect in expressing their thoughts, which would impede the fulsome discussion of issues necessary to reach a well-reasoned decision.

(49) Exemption 5 is predicated on the recognition that release of this privileged information would inhibit the government's development of policy and stifle its decision-making process. Furthermore, exempting such documents from disclosure also protects against public

confusion that might result from preliminary disclosure of opinions and information that do not, in fact, reflect the final views or policies of the FBI. The FBI invokes Exemption 5 and the deliberative process privilege because FBI employees would hesitate to offer their candid and conscientious opinions to superiors or coworkers if they knew their opinions of the moment might be made a matter of public record at some future date, and because such self-censorship would, in turn, degrade the quality of agency decisions by depriving the decision-makers of fully-explored options developed from robust debate. The FBI also relies on Exemption 5 in conjunction with the deliberative process privilege to ensure that FBI employees are not forced to operate in a fishbowl when collecting and analyzing information leading to final agency decisions.

(50) The FBI relied on the deliberative process privilege, in conjunction with Exemption 5, to protect information in the responsive records reflecting the decision-making process of the FBI, alone or in conjunction with other DOJ components, regarding (1) the scope and focus of the FBI's investigation in the Timberline High School Case, and (2) the creation, modification and/or implementation of policy directives and guidelines regarding certain undercover investigations. Specifically, the FBI withheld information contained in (1) an Email chain providing recommended revisions to a draft letter to the Editor of the New York Times; (2) draft reports compiled by the United States Department of Justice, Office of Inspector General ("USDOJ, OIG") concerning the FBI's Seattle Timberline Investigation; (3) blank/fillable forms used by the FBI for providing comments and corrections to reports it reviewed and used here to submit comments on the OIG draft report; (4) draft PowerPoint Slides concerning undercover operations; (5) USDOJ, OIG Memorandums discussing OIG's preliminary conclusions and recommendations regarding the Timberline investigation; and (6) Emails between FBI's

attorneys and other FBI personnel discussing matters pertaining to the application of an investigative technique, implementation of Policy Notice 0907N pertaining to certain undercover investigations and a USDOJ, OIG report concerning information discussing the FBI's handling of the Timberline School Investigation. I discuss how each category of records are predecisional and deliberative below.

(51) The emails described in the first category are pre-decisional in that they precede former FBI Director Comey's letter to the Editor of the New York Times released at Bates-numbered pages RCFP-284 thru RCFP-286. The withheld materials are deliberative in that the emails contain detailed discussions and proposals leading to the decision about how the FBI would respond to the New York Times and others concerning the FBI's handling of the Seattle Timberline Investigation.

(52) The documents described in the second, third, and fifth categories are pre-decisional because they precede the final USDOJ, OIG report released at Bates-numbered pages RCFP-851 thru RCFP-880. The withheld materials are deliberative in that they reflect advice and information that FBI and OIG shared concerning the USDOJ, OIG report on the Seattle Timberline Case.

(53) The drafts described in the fourth category are pre-decisional because they precede a potential final PowerPoint presentation regarding FBI's policies and procedures for conducting undercover operations. The withheld information is deliberative because the drafts reflect preliminary proposals and recommendations about how to ultimately instruct FBI personnel about conducting undercover operations.

(54) The emails described in the sixth category are pre-decisional because they precede the FBI's Policy Notice 0907N released in part at Bates numbered pages RCFP-278 thru

RCFP-283 and the final USDOJ, OIG report released at Bates-numbered pages RCFP-851 thru RCFP-880. The withheld information is deliberative because it reflects internal advice and recommendations relied upon by the decision makers when deciding what policy changes would be made regarding how certain undercover investigations would be approved in which the FBI impersonated documentary film crews and/or member(s) of the news media and how FBI personnel would be notified of the policy change.

(55) The information withheld warrants protection because it is: a) contained within intra-agency documents; b) pre-decisional; and c) deliberative. Finally, although factual information is generally not privileged under the deliberative process privilege, it can be protected if it is inextricably intertwined with deliberative information. The FBI concluded that the factual information in the responsive records here was part of the deliberation itself and inextricably intertwined with deliberative information, and therefore, it cannot be extricated from deliberative material. Accordingly, the FBI has properly withheld this privileged information pursuant to FOIA Exemption (b)(5)-1. A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(5)-1 is set forth in the attached *Vaughn* Index, **Exhibit K**.

EXEMPTION (b)(7) THRESHOLD

(56) Before an agency can invoke any of the harms enumerated in Exemption (b)(7), it must first demonstrate that the records or information at issue were compiled for law enforcement purposes. Pursuant to 28 U.S.C. §§ 533, 534, and Executive Order 12333 as implemented by the Attorney General's Guidelines for Domestic FBI Operations ("AGG-DOM") and 28 C.F.R. § 0.85, the FBI is the primary investigative agency of the federal government with authority and responsibility to investigate all violations of federal law not exclusively assigned to another agency, to conduct investigations and activities to protect the

United States and its people from terrorism and threats to national security, and further the foreign intelligence objectives of the United States. Under this investigative authority, portions of the responsive records were compiled for purposes of investigating and gathering intelligence information, and apprehending and prosecuting subjects suspected of terrorism against the United States; these records relate to enforcement of pertinent federal laws and within the core law enforcement duty of the FBI. Other portions of the responsive records were compiled during the FBI's criminal investigation of a third-party subject for violations of 18 U.S.C. § 875(c), Interstate Transmission of Communication Containing Threat to Injure, and 1030(a)(5)(A)(i) and (B)(iv), Computer Intrusion Causing a Threat to Public Safety. This description applies to all of the records the FBI withheld pursuant to the various coded categories of FOIA exemptions (b)(7)(C) and (b)(7)(E). The FBI is responsible for detecting and investigating violations of Federal criminal laws, international terrorism, and threats to national security. Thus, these records were compiled for a law enforcement purpose; they fall within the law enforcement duties of the FBI. Therefore, the information meets the threshold requirement of Exemption (b)(7).⁸

EXEMPTIONS (b)(6) AND (b)(7)(C)
CLEARLY UNWARRANTED AND UNWARRANTED
INVASIONS OF PERSONAL PRIVACY

(57) Exemption 6 exempts from disclosure “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal

⁸ This threshold would also apply to the DOJ OIG reports which are comprised of FBI information concerning its handling of the Seattle Timberline investigation as well as information concerning several of its policies and procedures.

privacy.” 5 U.S.C. § 552(b)(6). All information that applies to a particular person falls within the scope of Exemption 6.

(58) Exemption 7(C) similarly exempts from disclosure “records or information compiled for law enforcement purposes [when disclosure] could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7)(C).⁹

(59) When withholding information pursuant to these two exemptions, the FBI is required to balance the privacy interests of the individuals mentioned in these records against any public interest in disclosure. In asserting these exemptions, each piece of information was scrutinized to determine the nature and strength of the privacy interest of every individual whose name and/or identifying information appears in the documents at issue. When withholding the information, the individual’s privacy interest was balanced against the public’s interest in disclosure. For purposes of these exemptions, a public interest exists only when information about an individual would shed light on the FBI’s performance of its mission to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. In each instance wherein information was withheld pursuant to Exemptions 6 and 7(C), the FBI determined that the individuals’ privacy interests clearly outweighed any public interest in disclosure. Every effort

⁹ The practice of the FBI is to assert Exemption 6 in conjunction with Exemption 7(C). Although the balancing test for Exemption 6 uses a “would constitute a clearly unwarranted invasion of personal privacy” standard and the test for Exemption 7(C) uses the lower standard of “could reasonably be expected to constitute an unwarranted invasion of personal privacy,” the analysis and balancing required by both exemptions is sufficiently similar to warrant a consolidated discussion. The privacy interests are balanced against the public’s interest in disclosure under both exemptions.

has been made to release all segregable information contained in these records without invading the privacy interests of these individuals.

(b)(6)-1 and (b)(7)(C)-1

**Names and/or Identifying Information of
FBI Special Agents and Professional Staff**

(60) In Coded Categories (b)(6)-1 and (b)(7)(C)-1, the FBI protected the names, identifying information, Unique Employee Identification Numbers (“UEIDs”),¹⁰ email addresses, telephone numbers and personnel cellular telephone numbers of FBI Special Agents (“SAs”) and professional staff who were responsible for receiving, reviewing, analyzing, supervising, conducting and/or maintaining the investigative activities and the day-to-day operations of the FBI reflected in the responsive documents. Additional responsibilities included, but were not limited to, compiling information, disseminating information to FBI personnel, as well as reporting on the status of the investigations. FBI SAs and professional staff, attorneys and paralegals have access to information regarding official law enforcement investigations, and therefore may become targets of harassing inquires for unauthorized access to information regarding such investigations if their identities were released. Assignments of SAs, professional staff, attorneys and paralegals to any particular matter or investigation are not by choice. Publicity (adverse or otherwise) regarding any particular investigation to which they have been assigned may seriously prejudice their effectiveness in conducting other investigations. The privacy consideration is also to protect FBI SAs, professional staff, attorneys and paralegals as individuals, from unnecessary, unofficial questioning as to their assistance rendered in matters such as described in the processed records, or their conduct in other investigations and/or legal matters, whether or not they are currently employed by the FBI. For example, an individual

¹⁰ UEIDs are singular numbers assigned to employees, and serve as a means of identification within the government.

targeted by such law enforcement actions may carry a grudge. Such individuals may seek revenge on the agents, professional staff, attorneys and/or paralegals involved in a particular investigation or legal matter. Thus, these FBI employees maintain substantial privacy interests in not having their identities, information, UEID, email addresses, telephone numbers and personnel cellular telephone numbers¹¹ disclosed. In contrast, there is no public interest to be served by disclosing the identities of the SAs, professional staff, attorneys and/or paralegals to the general public because their identities would not significantly increase the public's understanding of the FBI's operations and activities.

(61) Accordingly, the FBI protects the names and identifying information of all lower ranking personnel in all FBI records, including records compiled for reasons other than law enforcement, pursuant to FOIA Exemption 6.

(62) First, there is no public interest in the release of this specific information because release of the names and identifying information of lower ranking FBI personnel does not shed light on government operations. Second, there are cognizable privacy interests connected to the release of FBI employee names and identifying information regardless of the specific position held, *e.g.*, a Special Agent, Intelligence Analyst, or Professional Staff. As a law enforcement and intelligence agency with myriad missions including counterterrorism, counterintelligence, and cybercrime, mere employment with the FBI – and the access to classified information that it provides – puts all FBI employees at risk of clearly unwarranted invasions of privacy.

¹¹ Given the personal nature of an individual's mobile device, which by its very nature is routinely carried on one's person when he or she is physically out of the office, at home, and/or on personal time, there is a greater potential for invasion of privacy in the disclosure of such cellular telephone numbers than there is in an individual's office telephone number. The release of such information could subject those employees to unwarranted harassment in their personal time and personal lives, and as such the release of such information would "constitute a clearly unwarranted invasion of personal privacy."

(63) Additionally, all FBI employees possess Top Secret clearances allowing access to classified material and systems, including Sentinel, the FBI's electronic "next generation" case management system where sensitive criminal and national security investigative information is stored. Positive identification as an FBI employee is of genuine interest to criminal elements, terrorists, and foreign intelligence services. As a result, the FBI routinely protects the names and identifying information of all lower ranking employees as their status of an FBI employee, on its own, may subject them to harassment by criminals seeking access to FBI information or retribution, violent acts of terrorists who advocate bodily harm against U.S. law enforcement and military personnel in furtherance of ideology, or recruitment by foreign agents intent on espionage. As such, FBI professional staff have identifiable privacy interests in protection from the harms above as well as unnecessary, unofficial questioning as to the conduct of investigations or the law enforcement activities they support.

(64) Moreover, these identifiable harms are not confined to FBI occupation and do not turn on whether or not the FBI records disclosing the identifying employee information was compiled for a law enforcement purposes. Adversaries who pose harm to the FBI are not required to draw distinctions between FBI employees based on occupation or the reason an FBI record was compiled--the key piece of information is identifying the individual as a member of the FBI. For instance, a foreign intelligence agent seeking to recruit an FBI employee might pursue an opportunity to turn a professional staff employee to try to get access to classified information.

(65) Finally, applying the balance of interests, the identifiable FBI employee privacy interests articulated above outweigh the lack of any public interest in disclosure demonstrating how government works, thus triggering a clearly unwarranted invasion of privacy with

reasonably foreseeable harm to those privacy interests. Accordingly, the FBI properly withheld their names, identifying information, email addresses and personnel cellular telephone numbers pursuant to Exemptions 6 and 7(C). A complete list of the Bates-numbered pages containing Exemption Coded Categories (b)(6)-1 and (b)(7)(C)-1 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(6)-2 and (b)(7)(C)-2 **Name and Identifying Information of**
Non-FBI Federal Government Employee

(66) In Coded Categories (b)(6)-2 and (b)(7)(C)-2, the FBI protected the name of a non-FBI federal government employee identified in one document responsive to Plaintiff's requests. Disclosure of the identity and identifying information of a non-FBI federal government employee could subject this individual to unauthorized inquiry and harassment and would constitute a clearly unwarranted invasion of his/her personal privacy. The rationale for protecting a non-FBI federal government employee is the same as that for FBI employees discussed at ¶¶ 60-65, *supra*. In balancing the legitimate privacy interest of this individual against any public interest in disclosure, the FBI determined that there is no *bona fide* public interest in this information because its disclosure will not shed light on the operations and activities of the federal government. Accordingly, the FBI concluded that the disclosure of this information would "constitute a clearly unwarranted" and "unwarranted invasion of their personal privacy." The FBI properly protected the name and identifying information of a non-FBI federal government employee pursuant to FOIA Exemptions 6 and 7(C). A complete list of the Bates-numbered pages containing Exemption Coded Categories (b)(6)-2 and (b)(7)(C)-2 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(6)-3 and (b)(7)(C)-3**Names and/or Identifying Information of a
Third Parties of Investigative Interest**

(67) In Coded Categories (b)(6)-3 and (b)(7)(C)-3, the FBI protected the names and/or identifying information of third-parties who were of investigative interest to the FBI or other law enforcement agencies during the Timberline investigation. Identification as a subject of a criminal investigation such as the individuals identified in the responsive material pertaining to the investigation of the bomb threats and distributed denial of service (“DDOS”) attacks received at Timberline School District, carries a strong negative connotation and a stigma. Release of the identities of these individuals to the public could subject them to harassment or embarrassment, as well as undue public attention. Accordingly, the FBI has determined that these individual maintain a substantial privacy interest in not having their identity disclosed. In contrast, disclosing personal information about these individuals would not significantly increase the public’s understanding of the FBI’s or other law enforcement agencies’ performance of their mission and so the FBI concluded that there was no public interest here sufficient to override these individuals’ substantial privacy interests. For these reasons, the FBI properly withheld this information pursuant to FOIA Exemptions 6 and 7(C). A complete list of the Bates-numbered pages containing Exemption Coded Categories (b)(6)-3 and (b)(7)(C)-3 is set forth in the attached *Vaughn Index*, **Exhibit K**.

(b)(6)-4 and (b)(7)(C)-4**Names and/or Identifying Information of
Third Parties Merely Mentioned**

(68) In Coded Categories (b)(6)-4 and (b)(7)(C)-4, the FBI protected the names and identifying information of third parties merely mentioned in the records at issue. Identifying information may include, but is not limited to, names, telephone/facsimile numbers, mobile/cellular telephone numbers, Email addresses and other personal information. The FBI has information about these third parties in its files because these individuals either contacted the

FBI to obtain information concerning an FBI investigation, to include the FBI's handling of the same, or were merely mentioned in an FBI newsletter disseminated to FBI personnel, which newsletter documents the FBI's notice to its employees of certain new and/or revised policies, announcements and other information. These individuals were not of investigative interest to the FBI. These third parties maintain legitimate privacy interest in not having their identifying information disclosed. Disclosure of these third parties' names and identifying information could reasonably be expected to draw negative and unwanted attention to these individuals and could subject these individuals to possible harassment. Accordingly, the FBI determined that these third parties maintain a substantial privacy interest in not having information about them disclosed. After identifying the substantial privacy interests these individuals maintain, the FBI balanced their right to privacy against the public interest in the disclosure. The FBI has determined that the personal privacy interests in non-disclosure outweighed the public in disclosure, as disclosure would not shed any light on the operations and activities of the FBI. Thus, disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy. Accordingly, the FBI properly protected this information pursuant to FOIA Exemptions 6 and 7(C). A complete list of the Bates-numbered pages containing Exemption Coded Categories (b)(6)-4 and (b)(7)(C)-4 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(6)-5 and (b)(7)(C)-5

**Names and/or Identifying Information of
Local Law Enforcement Personnel**

(69) In Coded Categories (b)(6)-5 and (b)(7)(C)-5, the FBI withheld the names and identifying information of local law enforcement personnel from two pages of responsive records. These employees were acting in their official capacity and aided the FBI in the law enforcement investigative records responsive to Plaintiffs' requests. The rationale for protecting

the identities of FBI SAs and professional staff discussed at ¶¶ 60-65, *supra*, also supports withholding the names and identifying information of these local law enforcement personnel. To release the identities of these law enforcement personnel could subject them as individuals to unnecessary, unwarranted harassment which would constitute an unwarranted invasion of privacy. Furthermore, these individuals could become a prime target for compromise if their identities were known. There is no public interest to be served in releasing the identities of these individuals. The FBI concluded that the disclosure of this information would constitute a clearly unwarranted and an unwarranted invasion of their personal privacy. Accordingly, the FBI properly protected this information pursuant to FOIA Exemptions 6 and 7(C). A complete list of the Bates-numbered pages containing Exemption Coded Categories (b)(6)-5 and (b)(7)(C)-5 is set forth in the attached *Vaughn* Index, **Exhibit K**.

EXEMPTION (b)(7)(E)
INVESTIGATIVE TECHNIQUES AND PROCEDURES

(70) 5 U.S.C. § 552(b)(7)(E) provides protection for:

Law enforcement records which 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.

(71) Exemption (b)(7)(E) has been asserted to protect information containing sensitive investigatory techniques and procedures authorized for use by the FBI. This exemption affords categorical protection to techniques and procedures used in law enforcement investigations; it protects techniques and procedures not well-known to the public as well as non-public details about the use of well-known techniques and procedures. While several documents could easily be characterized as consisting fully of information that would disclose investigative techniques and procedures, and thus would be eligible for protection under (b)(7)(E) in their entirety, the

FBI endeavored to release as much segregable information as possible to Plaintiffs. The release of additional information would disclose techniques and/or procedures used in law enforcement, criminal and national security investigations or prosecutions, or would disclose guidelines for law enforcement, criminal and national security investigations or prosecutions that could reasonably be expected to risk circumvention of the law.

(72) The FBI's rationale for protecting this information cannot be examined in a vacuum; it must be analyzed within the larger context of our country's current national security climate. The FBI is charged with protecting the nation from security risks posed by U.S. and non-U.S. individuals, organizations (such as terrorist groups), and foreign nations that seek to harm the United States. Thus, if specific investigative techniques or procedures are made public, the very criminals and terrorist groups who seek harm to U.S. interests can use the information to their advantage, learn FBI tactics in gathering information, and develop countermeasures to avoid detection.

(b)(7)(E)-1 Operational Directives

(73) In Coded Category (b)(7)(E)-1, the FBI protected certain information contained in the FBI's Domestic Investigations and Operations Guide; Undercover Sensitive Operations Policy Guide; and Policy Notice 0907N (Undercover Activities and Operations - Posing as a Member of the News Media or a Documentary Film Crew)¹² responsive to Plaintiffs' requests. This law enforcement material comprises operational directives that provide information and instruct FBI employees on the proper use of certain sensitive non-public FBI procedures, techniques, and guidance for conducting investigations. In the course of providing these

¹² Upon further review, the FBI hereby asserts Exemption Coded Category (b)(7)(E)-1 to withheld information previously withheld citing Exemption Coded Category (b)(7)(E)-8 on Bates-numbered pages RCFP-278 thru RCFP-282.

instructions, these guides identify the procedures, techniques, and strategies at issue.

Specifically, the protected information falls within both subtypes of 7(E): law enforcement techniques and procedures and law enforcement guidelines. Releasing such information would not only provide sensitive, unknown investigative techniques, it would also reveal sensitive unknown uses of these specific techniques and procedures. If released, the information would provide individuals and entities with a unique look inside the FBI's law enforcement and national security "playbooks." Armed with such information, criminals could predict how and when the FBI will respond to certain suspicious/criminal activities, and the investigative techniques the FBI is most likely to employ in those situations. This would afford criminals the ability to preemptively modify their behavior in a manner that avoids detection and disrupt the very investigative procedures, techniques, and strategies that these FBI guides are intended to protect. Consequently, the release of this information would increase the risk that targets of both criminal and national security investigations could develop countermeasures and avoid detection by interfering with the FBI's ability to effectively use these important law enforcement techniques. Release of this information would allow individuals and entities seeking to commit crimes or threaten U.S. national security an opportunity to avoid detection and circumvent the law. Thus, the FBI properly withheld this information pursuant to FOIA Exemption 7(E). A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-1 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(7)(E)-2 Undercover Operation

(74) In Coded Category (b)(7)(E)-2, the FBI protected non-public details about undercover operations conducted by the FBI and described in the records responsive to Plaintiffs' requests. The non-public details relate specifically to the FBI's Seattle Timberline

investigation and FBI undercover operations in general.¹³ If the FBI were to disclose these non-public details about how it conducts undercover operations and releases details of the specific techniques used during this undercover operation, it could have devastating operational consequences and would jeopardize future use of undercover operations by the FBI in similar cases or under similar circumstances; thus, disclosure of these details would risk circumvention of the law. The FBI properly protected information about this undercover operation pursuant to Exemption 7(E). A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-2 is set forth in the attached *Vaughn* Index, **Exhibit K**.

**(b)(7)(E)-3 Identity and/or Location of FBI or
Joint Units, Squads, and/or Divisions**

(75) In Coded Category (b)(7)(E)-3, the FBI protected the location and/or identity of FBI units and joint units, squads, sections and divisions within the responsive records. The existence of these particular squads, units, sections and divisions is not known to the general public. The office location and units are usually found in the administrative headings of internal FBI documents and in the signature blocks of electronic mail correspondence. These headings identify the locations of the office and unit that originated or received the documents. Revealing their names, numbers, and alpha designators would reveal the level of focus the FBI has applied to certain areas within the assigned enforcement activity, and as relevant here, to the investigative realm of domestic terrorism. While the harm of releasing the identity of a particular FBI operational unit may not be self-evident from the face of these records, the release of these unit identities could reasonably be expected to risk circumvention as disclosure (i) would provide a kernel of information about the application and focus of FBI domestic

¹³ Upon further review, the FBI hereby asserts Exemption Coded Category (b)(7)(E)-2, along with (b)(7)(E)-1 to withhold information on Bates-numbered page 278.

terrorism investigative capability and presence in the associated geographical area(s); (ii) this piece of information alone identifies the particular unit(s) internal designation, its geographical disposition, and the unit's primary activity; (iii) and this piece of information alone and/or when combined with other information in mosaic fashion, provides key insight into limited FBI resources that are employed in this type of enforcement activity in a particular area. For example, the knowledge that the FBI has an internal unit designation of "Squad X" in a particular area for a particular type of investigative activity could reasonably be applied by criminal elements or terrorists to plan and structure their activities in a manner that avoids detection and disruption by the FBI, thus enhancing their ability to circumvent the law. In addition, the revelation of the involvement of one or more units of differing focus in an investigation is critical information that can allow for adjustments of behaviors and activities by criminals, to avoid detection and/or disruption by the FBI. Accordingly, the FBI properly asserted Exemption 7(E) to protect this information. A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-3 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(7)(E)-4 Internal FBI Secure Fax Numbers and/or Phone numbers, Email or IP Addresses, Intranet/Web Addresses

(76) In Coded Category (b)(7)(E)-4, the FBI protected internal secure fax numbers, telephone numbers and Email addresses. Release of this type of information could allow individuals under investigation to exploit the FBI's Information Technology system, by allowing the opportunity to misuse these venues. Criminals could interfere with the FBI's ability to timely and accurately conduct investigations, by exploiting this unclassified but non-public information, and by inundating these venues with faxes, phone calls or Emails providing inaccurate and misleading information. Such actions could arm them with the information or ability to

circumvent the law. Additionally, release of this information would allow individuals to disrupt official business and could subject FBI employees to harassing phone calls, facsimiles and Emails. Thus, the FBI properly protected this information from disclosure pursuant to FOIA Exemption 7(E). A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-4 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(7)(E)-5 Sensitive Investigative Techniques And Procedures, Including The Deployment Of Computer and Internet Protocol Address Verifier (“CIPAV”)

(77) In Coded Category (b)(7)(E)-5, the FBI protected the non-public details concerning the deployment of CIPAV, as well as other techniques and procedures utilized by the FBI in both criminal and national security investigations, including information revealing what types of techniques and procedures are routinely used in such investigations and are not publicly known, as well as non-public details about the use of well-known techniques and procedures. The government’s use of CIPAV in the Timberline High School investigation is a known public fact; however, the specific details concerning the deployment of CIPAV are not well-known. All documents at issue contain sensitive information about the deployment of CIPAV and other specific investigative methods and techniques used by the FBI in furtherance of both criminal and national security investigations.

(78) To describe the investigative methods and techniques in further detail would highlight the very information the FBI seeks to protect pursuant to this exemption. Revealing details about information-gathering methods and techniques commonly used in both criminal and national security investigations, and the circumstances under which they are used, would enable the targets of those methods and techniques to avoid detection of and develop countermeasures to circumvent the FBI’s ability to effectively use such critical law enforcement methods and

techniques in current and future criminal and national security investigations, thus risking the circumvention of the law. Accordingly, the FBI properly withheld this information pursuant to FOIA Exemption 7(E). A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-5 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(7)(E)-7 Collection and Analysis Of Information

(79) In Coded Category (b)(7)(E)-7 the FBI has protected the techniques and procedures it uses to collect and analyze information in connection with both criminal and national security investigations. Specifically, on Bates-numbered page RCFP-630, the FBI protected information concerning an FBI undercover operation that is unrelated to the Seattle Timberline investigation in a portion of an email chain dated February 8, 2016, wherein FBI personnel were trying to determine whether that undercover investigation would meet the requirements for Deputy-Director approval pursuant to the newly changed policy. The release of this information would disclose the identity of methods used in collecting and analyzing information, including how and from where the FBI collects information, and the methodologies employed to analyze it. Such disclosures would enable investigative subjects to circumvent similar and currently used techniques. The relative utility of these techniques could be diminished if the actual techniques were released. In turn, this would facilitate the accumulation of information by investigative subjects regarding the circumstances under which specific techniques were used or requested to collect certain information, how the information collected is analyzed, and the usefulness of the information obtained. Release of this information would enable criminals and terrorists to educate themselves on techniques employed by the FBI in collecting and analyzing information, thus allowing them to take countermeasures to circumvent the effectiveness of these techniques.

(80) Similar to the reasoning articulated above, the FBI's use of CIPAV during the FBI's investigation of the Timberline High School investigation is a known public fact; however, the specific details collected by this tool, as well as the other methods the FBI utilizes to collect, and analyze the information are not publically known. Several of these documents contain sensitive information about investigative methods used by the FBI in conducting both criminal and national security investigations. The methods are detailed within the documents in varying degrees of specificity. Releasing information on these methods and use would, in essence, highlight the types of activities, facts, or occurrences that are of particular interest to the FBI in both criminal and national security investigations. Publicly disclosing investigative methods, analysis of information gleaned from the methods, or any other sort of details regarding it, would inform individuals of the kinds of information the FBI is interested in capturing and would afford them the opportunity to employ countermeasures to circumvent detection or alter behavior to mislead investigators. Accordingly, the FBI properly withheld this information pursuant to FOIA Exemption 7(E). A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-7 is set forth in the attached *Vaughn* Index, **Exhibit K**.

(b)(7)(E)-10 Sensitive File Numbers or Subfile Names

(81) In Coded Category (b)(7)(E)-10 the FBI has protected sensitive case file numbers. The FBI has determined that this exemption is appropriate for protecting these file numbers as the release of file numbering convention identifies the investigative interest or priority given to such matters. Applying a mosaic analysis, suspects could use these numbers (indicative of investigative priority), in conjunction with other information known about other individuals and/or techniques, to change their pattern of activity to avoid detection, apprehension, or create alibis for suspected activities, etc. Exacerbating this harm, releasing these file numbers provides

criminals with a tracking mechanism by which they can place particular files/investigations within the context of larger FBI investigative efforts. Continued release of sensitive investigative file numbers would provide criminals with an idea of how FBI investigations may be interrelated and when, why, and how the FBI pursued different investigative strategies. This would provide criminals with a means of judging where the FBI allocates its limited investigative resources, how the FBI responds to different investigative circumstances, what the FBI knows and when/how they obtained that knowledge, and if there are knowledge-gaps in the FBI's gathered intelligence. Given this data, determined criminals could obtain an exceptional understanding as to how they might structure their behavior to avoid detection and disruption by FBI investigators, enabling them to circumvent the law. Accordingly, the FBI properly asserted Exemption 7(E) to protect this type of information. A complete list of the Bates-numbered pages containing Exemption Coded Category (b)(7)(E)-10 is set forth in the attached *Vaughn* Index, **Exhibit K**.

CONSULTATIONS AND/OR REFERRALS

(82) While processing records responsive to Plaintiffs' requests, the FBI identified information which either originated with or contained other government agencies' information and/or equities. Pursuant to established DOJ procedures, the FBI consulted with the U.S. Department of Justice, Office of Inspector General and the Central Intelligence Agency, and asked them to make disclosure determinations concerning their information.

U.S. DEPARTMENT OF JUSTICE, OFFICE OF INSPECTOR GENERAL ("DOJ OIG")

(83) The FBI identified 13 documents, consisting of 120 pages (Bates-numbered "RCFP-319 through RCFP-375," and "RCFP-818 through RCFP-880") which either originated with or contained DOJ OIG's information and/or equities. Following consultations between DOJ OIG and FBI, it was determined that certain information contained in these documents was

exempt from disclosure pursuant to Exemptions (b)(5), (b)(6) and (b)(7)(C). DOJ OIG provided a Declaration to support its withholdings in the records responsive to Plaintiffs' requests. *See Exhibit L.*

CENTRAL INTELLIGENCE AGENCY ("CIA")

(84) The FBI identified one document (Bates-numbered "RCFP-789," which contained CIA information and/or equities. Following consultations between CIA and FBI, it was originally determined that certain information contained in this document was exempt from disclosure pursuant to Exemptions 1 and 3. Following the FBI's protection of this information and release of this record to Plaintiff, the CIA re-evaluated its withholding and determined the information on RCFP-789 may be released. Accordingly, the FBI reprocessed Bates-numbered page, RCFP-789 and included it in a January 10, 2019 supplemental release to Plaintiff. *See Exhibit I.*

SEGREGABILITY

(85) During the processing of Plaintiffs' requests, each responsive page was individually examined to identify non-exempt information that could be reasonably segregated from exempt information for release. All segregable information has been released to Plaintiffs. As demonstrated herein, the only information withheld by the FBI consists of information that would trigger reasonably foreseeable harm to one or more interests protected by the cited FOIA exemptions.

(86) As discussed in paragraph 5 *supra*, there were 611 responsive pages identified and of those pages, 84 pages were Released in Full ("RIF"), 244 pages were Released in Part ("RIP"), and 283 pages were Withheld in Full ("WIF"). Each of these categories is discussed below to further address segregability.

(a) Pages RIF. Following the segregability review, RIDS determined that 84 pages could be released in full without redactions as there was no foreseeable harm to an interest protected by a FOIA exemption.

(b) Pages RIP. RIDS further determined that 244 pages could be released in part with redactions pursuant to the specific FOIA exemptions identified on these pages and described herein. These pages comprise a mixture of material that could be segregated for release and material that was withheld as release would trigger foreseeable harm to one or more interests protected by the cited FOIA exemptions on these pages.

(c) Pages WIF. Finally, RIDS determined that 284 pages were withheld in their entirety. Of these pages, RIDS determined 201 pages were duplicates of other records previously released to Plaintiffs in whole or in part. The remaining 83 pages were withheld in full as they are fully covered by one or more of the cited FOIA exemptions, therefore, there was no information that could be reasonably segregated for release without triggering foreseeable harm to one or more of the cited FOIA exemptions.

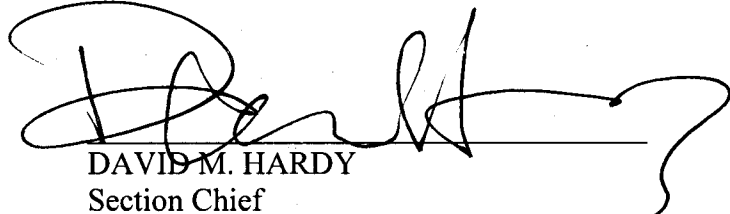
CONCLUSION

(87) The FBI conducted a reasonable search for records responsive to Plaintiffs' FOIA requests and subject to the FOIA. The FBI has processed and released all reasonably segregable information from the responsive records to Plaintiffs. Information was properly withheld pursuant to FOIA Exemptions 1, 3, 5, 6, 7(C), and 7(E), 5 U.S.C. §§ 552 (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E). The FBI has carefully examined the responsive records and has determined the information withheld from Plaintiffs, if disclosed, would reveal classified information, would violate federal statutes governing release of information on national security operations; would reveal privileged information, would cause a clearly unwarranted invasion of personal privacy; could reasonably be expected to constitute an unwarranted invasion of personal

privacy; or would disclose techniques and procedures for law enforcement investigations or prosecutions the disclosure of which, could reasonably be expected to risk circumvention of the law. Accordingly, the FBI has released all reasonably segregable, non-exempt information to Plaintiffs in response to their FOIA requests to the FBI.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibits A - L attached hereto are true and correct copies.

Executed this 20th day of June, 2019.



DAVID M. HARDY
Section Chief
Record/Information Dissemination Section
Information Management Division
Federal Bureau of Investigation
Winchester, Virginia

EXHIBIT 13

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, November 03, 2014 2:38 PM
To: KORTAN, MICHAEL P. (OPA) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Cc: GIULIANO, MARK F (DO) (FBI)
Subject: DRAFT letter to NY Times UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Editor:

[REDACTED]

b5 -1

[REDACTED]

b5 -1

[REDACTED]

b5 -1

[REDACTED]

b5 -1

[REDACTED]

b5 -1

RCFP-303



=====
Classification: UNCLASSIFIED

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, November 03, 2014 6:16 PM
To: COMEY, JAMES B. (DO) (FBI); KORTAN, MICHAEL P. (OPA) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Cc: GIULIANO, MARK F (DO) (FBI)
Subject: RE: DRAFT letter to NY Times UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

And after reading the Cyber write up I would add the language below in red.

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, November 03, 2014 2:38 PM
To: KORTAN, MICHAEL P. (OPA) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Cc: GIULIANO, MARK F (DO) (FBI)
Subject: DRAFT letter to NY Times --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Editor:

b5 -1

b5 -1

RCFP-305

[REDACTED]

b5 -1

[REDACTED]

b5 -1

[REDACTED]

b5 -1

[REDACTED]

b5 -1

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

EXHIBIT 14



LOCAL

WEATHER

INVESTIG

55°

LIVE TV

TRENDING

Live Blog: Coronavirus Updates

Race in America

Bay Area Reopening Plans

Remembering

4 WEATHER
ALERTS

FBI: San Francisco Bomb Suspect Sought Toxins

According to the affidavit, Chamberlain said he wanted to use the abrin to ease the suffering of cancer patients.

By Associated Press • Published June 6, 2014



• Updated on [June 7, 2014](#) at 4:50 am

A man charged with possessing explosive material at his San Francisco apartment also used an anonymous, Internet-based marketplace to try to buy biological agents and lethal toxins, the FBI said in documents unsealed Friday.

In the search warrant affidavit, FBI Special Agent Michael Eldridge said witnesses reported shipping the poison abrin to suspect Ryan Chamberlain.

It was unclear, however, if Chamberlain ever received the poison that is found in the seeds of a plant called the rosary pea.

Trending Stories



BELMONT

Woman Intentionally Coughs
on Bartender in Belmont Bar

Authorities have not said what, if anything, Chamberlain intended to do with the toxins or with the bomb-making materials found at his apartment.

- FBI Manhunt for "Armed and Dangerous" PR Consultant Expands**

Chamberlain said he wanted to use the abrin to ease the suffering of cancer patients, according to the affidavit.

3:22

RAW VIDEO: Attorney Confronts FBI on "Green Fuzz" in Ryan Chamberlain

The 42-year-old Chamberlain was arrested Monday after a three-day manhunt that authorities said was prompted by the discovery of bomb-making materials at his apartment.

Chamberlain apparently came to the attention of the FBI as it investigated and monitored the online marketplace where people allegedly bought and sold guns, bombs, drugs, chemicals and counterfeit goods.

- U.S. Magistrate Orders Full Psychiatric Exam For San Francisco Man Accused Of**



SAN FRANCISCO

Man Describes San Francisco Garage Confrontation After Video of Incident Goes Viral



CORONAVIRUS

List of Coronavirus Cases in the Bay Area



CORONAVIRUS

Governor Orders Bars in 7 California Counties to Close

SPONSORED

Marbella Villas Might Be Cheaper Than You Think in 2020

Villas Marbella | Search Ads

Weather Forecast

SAN JOSE, CA

55°

Clear
0% Precip

TONIGHT

57°

TOMORROW

87°

PRESENTED BY

Possessing Bomb Materials

Also on Friday, U.S. Magistrate Judge Nathanael Cousins refused to let Chamberlain post bail pending his trial, which has not yet been scheduled.

Local



GOLDEN STATE KILLER • 7 HOURS AGO

California's Alleged Golden State Killer Set to Plead Guilty



BELMONT • 11 HOURS AGO

Woman Intentionally Coughs on Bartender in Belmont Bar

Chamberlain has been charged with one count of possessing material that could be used to build an explosive device. He has not entered a plea. His public defender declined comment outside court.

The judge scheduled an afternoon hearing to determine whether to transfer Chamberlain to a secured psychiatric unit at a hospital, where he could undergo an exam.

- **Attorney Challenges FBI Over "Green Fuzz" in Ryan Chamberlain Case**

Copyright AP - Associated Press

WHAT DO YOU THINK?



The NFL fined the Patriots \$1.1M, banned their TV crew from shooting games this season and took away a third-round pick in 2021 as punishment for illegally filming a 2019 Bengals-Browns game. Do you feel this is a fair punishment?

- ☐ Not sure / I don't follow the NFL
- ☐ It is a fair punishment
- ☐ It is not enough of a punishment
- ☐ It is too much of a punishment

NEXT



The Best US Dating Sites for...

SPONSORED • TOP US DATING SITES

If You're A Frequent Driver,...

SPONSORED • REACT

Work From Home Jobs May Earn...

SPONSORED • WORK FRO...

Best Superfoods To Boost Up...

SPONSORED • SUPERFOODS IMPROVE YOUR IMM...

New Portable AC

SPONSORED • WEARABLEAC

Hand-Picked And Verified...

SPONSORED • SEEKNCHE...

Exclusive interview of...

SPONSORED • TENNIS MA...

Looking for funds? Consider a loan. Send a request, receive a...

SPONSORED • CREDITTRUST SHORT-TERM LOANS

Diets That Work for Women and Have Stood the Test of Time -...

SPONSORED • HEALTHUPON

These Cowboy Boots are Takin...

SPONSORED • TECOVAS

PRIDE

People Rally in San Francisco Streets for 50th Pride

People Rally in San Francisco Streets for Earthquake Weekend

FACE MASKS

What to Wear: Feds' Mixed Messages on Masks Sow Confusion

Celebrities You Probably Didn't...

SPONSORED • O THE OPRAH MAGAZINE

Early Warning Signs of...

SPONSORED • METASTATI...

Current Health Insurance Price...

SPONSORED • HEALTH IN...


Migraine Relief. Research Latest Treatment For Migraine...

SPONSORED • YAHOO SEARCH

CORONAVIRUS VACCINE




Summer May Decide Fate of Leading Shots in Vaccine Race

Virus Updates: China Cases Stabilize, Italy Sees Drop in Deaths as US Cases Soar

BAY AREA

SUBMIT TIPS FOR

INVESTIGATIONS



NEWSLETTERS

CONNECT WITH US

- [Send Feedback](#)[KNTV Employment Information](#)[Terms of Service](#)[Privacy Policy – New](#)[Do Not Sell My Personal Information](#)
- [Ad Choices](#)[Advertise With](#)[KNTV Public In](#)

Copyright © 2020 NBC Universal Inc. All rights reserved