

Dear JMD Staff:

I wanted to ask if I could amend this request? Leave for redirect?

The amendments would be as shown:

Pursuant to the Freedom of Information Act, I hereby request the following records:

I was seeking any and all records in JMD custody related to:

I was seeking copies of any investigation findings within the Insider Threat office(s) for any FBI or DEA employees worldwide for the period generated during this timeframe October 2019 - October 2018.

The DOJ insider threat directive was issued on Feb 12, 2014.

<https://www.justice.gov/jmd/file/865256/download>

I would like to receive the information in EFOIA style for electronic communication and production.

Please produce the documents in .pdf format via email.

Fee Categorization

For fee categorization purposes, I am a representative of the news media. Through this request, I am gathering information for my journalistic work with Muckrock.com, and DocumentCloud.com. I am an active participant in the dissemination of public records for public education purposes. Accordingly, I am 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); id. § 552(a)(4)(A)(iv)(II).

Request for Fee Waiver

Please waive any applicable fees. The release of the information is not primarily in my commercial interest and will contribute significantly to public understanding of government operations and activities.

Conclusion

If my request is denied in whole or part, please justify all withholdings by reference to specific exemptions and statutes, as applicable. For each withholding please also explain why your agency "reasonably foresees that disclosure would harm an interest protected by an exemption" or why "disclosure is prohibited by law. Duties in relation to this requested data require post-haste execution for support of national security interests. Please utilize the redaction feature ethically.

Vaughn Index Requested

I would appreciate your communicating with me by email.

I look forward to your determination regarding my request within 20 business days, as the statute requires.

Thank you in advance for your assistance.

*I've enclosed some supporting documentation to favor the amended request as the DOJ has adopted a policy in relation to the release of investigative findings and precedent reports.

Best,

/s/

William Fernandes



U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

April 17, 2018

MR. WILLIAM FERNANDES
MUCKROCK
DEPT MR 38820
411A HIGHLAND AVENUE
SOMERVILLE, MA 02144-2516

FOIPA Request No.: 1378216-000
Subject: OPR Abstract of Disciplinary Action Against
Massachusetts Employees
(2015-2016)

Dear Mr. Fernandes:

The enclosed documents were reviewed under the Freedom of Information Act (FOIA), Title 5, United States Code, Section 552. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemptions boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input type="checkbox"/> (j)(2)
<input type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)
_____	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)
_____	<input type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)

2 pages were reviewed and 2 pages are being released.

Below you will also find additional informational paragraphs about your request. Where applicable, check boxes are used to provide you with more information about the processing of your request. Please read each item carefully.

- ☐ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].
- ☐ This information has been referred to the OGA(s) for review and direct response to you.
- ☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

☐ In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

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

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

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

☐ The enclosed material is from the main investigative file(s), meaning the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown such additional references, if identified to the same subject of the main investigative file, usually contain information similar to the information processed in the main file(s). As such, we have given priority to processing only the main investigative file(s) given our significant backlog. If you would like to receive any references to the subject(s) of your request, please submit a separate request for the reference material in writing. The references will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely,



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

The enclosed documents represent the final release of information responsive to your Freedom of Information Act (FOIA) request. This material is being provided to you at no charge.

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

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

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

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

PRECEDENT REPORT

LIMITED TO:

To maintain the anonymity of the person(s) involved, the term "he" is being used to refer to both genders.

1 **OPR# 2014-0237, APU# 2015-0066** **Closed: 7/31/2015** **References: 2.6, 3.5, 3.6, 5.20, 5.22**

[REDACTED] b6
[REDACTED] (5.22) [REDACTED] b7C
(5.20); [REDACTED] (3.6);
[REDACTED] (3.5); [REDACTED]
[REDACTED] (2.6)

[REDACTED] 5.22, b6
[REDACTED] 5.20, [REDACTED] 3.5, [REDACTED] 3.6, [REDACTED] b7C
[REDACTED]
[REDACTED] 5.22 - [REDACTED] 5.20 [REDACTED] 3.5 - 5
[REDACTED] 3.6 - [REDACTED] 2.6 - [REDACTED]

MITIGATION:

AGGRAVATION:

FINAL ACTION(S): OPR PROPOSED DECISION Proposed DISMISSAL
OPR FINAL DECISION: DISMISSAL
DRB: AFFIRMED

2 **OPR# 2015-0016** **Closed: 3/6/2015** **References: 3.10, 3.9, 5.7**

[REDACTED] (3.10) [REDACTED] b6
[REDACTED] (3.9) [REDACTED] b7C
[REDACTED] (5.7).

MITIGATION:

AGGRAVATION:

FINAL ACTION(S): OPR PROPOSED DECISION Proposed 50 CALENDAR DAYS SUSPENSION WITHOUT PAY
OPR FINAL DECISION: 50 CALENDAR DAYS SUSPENSION WITHOUT PAY

PRECEDENT REPORT

LIMITED TO:

To maintain the anonymity of the person(s) involved, the term "he" is being used to refer to both genders.

3 **OPR# 2015-0185** **Closed: 8/28/2015** **References: 3.3**

(3.3).

b6
b7C

MITIGATION:

AGGRAVATION:

FINAL ACTION(S): OPR FINAL DECISION: 1 CALENDAR DAYS SUSPENSION WITHOUT PAY

4 **OPR# 2016-0124** **Closed: 9/7/2016** **References: 5.21**

in violation of (5.21 - Unprofessional Conduct - Off Duty).

AGGRAVATION:

FINAL ACTION(S): OPR FINAL DECISION: 7 CALENDAR DAYS SUSPENSION WITHOUT PAY

b6
b7C

Investigative Summary: Findings Concerning Allegations of Misconduct by an FBI Assistant Special Agent in Charge Involving Sexual Harassment

The Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the Federal Bureau of Investigation (FBI) that an FBI Assistant Special Agent in Charge (ASAC) had engaged in multiple instances of inappropriate touching and inappropriate comments of a sexual nature with several female FBI employees.

The OIG investigation substantiated the allegations that the FBI ASAC made inappropriate comments of a sexual nature towards employees and made inappropriate physical contact with employees. The OIG interviewed several witnesses who told the OIG that they were either inappropriately touched or that they had inappropriate comments made to them by the FBI ASAC. Other witnesses said they observed the FBI ASAC engage in such conduct with the employees. Although the FBI ASAC generally denied the allegations, stated that he did not recall if specific incidents occurred, or made partial, non-inculpatory admissions, the OIG found the witnesses' accounts to be consistent, credible, and corroborative of each other. Accordingly, the OIG concluded that the FBI ASAC lacked candor in his interview the OIG. Prosecution was declined. Lastly, the OIG found that the FBI ASAC improperly discussed the fact the he was the subject of an OIG investigation with several subordinate employees in violation of FBI directives designed to prevent obstruction of administrative investigations.

The FBI ASAC was voluntarily demoted during the course of the OIG's investigation and was transferred to a different division. The OIG has provided its report to the FBI for appropriate action.

Posted to oig.justice.gov on August 6, 2015



DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

INVESTIGATIVE SUMMARY | 21-090

Findings of Misconduct by a then FBI Special Agent in Charge and two then FBI Assistant Special Agents in Charge for Their Roles in an Unauthorized \$2 Million Purchase of Intellectual Property Related to a Classified Undercover Operation and Related Misconduct

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated an investigation upon the receipt of information from the Federal Bureau of Investigation (FBI) alleging that in 2014 senior FBI officials from a field division spent \$2 million in government funds without authorization and engaged in other acts of misconduct related to that expenditure.

The OIG investigation substantiated the allegation that the then Special Agent in Charge (SAC) and two then Assistant Special Agents in Charge (ASACs) of the field division participated in the \$2 million purchase of intellectual property related to a classified undercover operation without the authority to do so. The OIG found that these actions were a violation of FBI policy.

The OIG concluded that the ASACs failed to disclose accurate cash on hand figures related to the undercover operation in order to secure funding for the unauthorized intellectual property purchase, in violation of FBI policy. Additionally, the OIG determined that the SAC deliberately falsified a funding request for the classified undercover operation, in violation of FBI policy.

The OIG investigation also substantiated that one of the ASACs showed a lack of candor related to the purchase, in violation of FBI policy.

The SAC and one of the ASACs retired and one of the ASAC's resigned before the OIG's investigation was completed. Prosecution was declined.

The OIG has completed its investigation and has provided a classified report to the FBI for appropriate action.



Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether DOJ personnel have committed misconduct.



DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

INVESTIGATIVE SUMMARY | 21-096

Findings of Misconduct by a Then- Senior FBI Official for Having Numerous Unauthorized Contacts with the Media, and for Accepting Unauthorized Gifts from Members of the Media

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of records from the Federal Bureau of Investigation (FBI) Insider Threat Unit, alleging that a then-Senior FBI Official had numerous contacts with members of the media between January and November 2016 in violation of FBI policy. This matter is among the OIG investigations referenced on page 430 of the OIG's Review of Allegations Regarding Various Actions by the Department and the Federal Bureau of Investigation (FBI) in Advance of the 2016 Election (June 2018; <https://oig.justice.gov/reports/review-various-actions-federal-bureau-investigation-and-department-justice-advance-2016>).

Subsequent to the onset of the investigation, the OIG found indications that the Senior FBI Official received items of value from members of the media.

The OIG investigation substantiated the allegation that the Senior FBI Official had numerous unauthorized contacts with the media from 2014 through 2016, in violation of FBI policy. In addition to substantive communications with reporters, this media contact included unauthorized social engagements outside of FBI Headquarters involving drinks, lunches, and dinners.

The OIG also found that the Senior FBI Official violated federal regulations and FBI policy when the Senior FBI Official accepted tickets from members of the media to two black tie dinner events, one valued at \$225 and the other valued at \$300, and received transportation to one event from a reporter, all without prior authorization.

The Senior FBI Official retired from the FBI prior to being contacted by the OIG for an interview. When later contacted by the OIG for a voluntary interview, the Senior FBI Official declined to be interviewed. The OIG has the authority to compel testimony from current Department employees upon informing them that their statements will not be used to incriminate them in a criminal proceeding. The OIG does not have the authority to compel or subpoena testimony from former Department employees, including those who retire or resign during the course of an OIG investigation.



DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

INVESTIGATIVE SUMMARY | 21-096

The OIG has completed its investigation and is providing this report to the FBI for its information.



Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether Department of Justice personnel have committed misconduct.



DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

INVESTIGATIVE SUMMARY | 21-098

Findings of Misconduct by an FBI Assistant Director for Failure to Timely Report a Romantic Relationship with a Subordinate and Related Misconduct

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated an investigation after receiving information from the Federal Bureau of Investigation (FBI) Inspection Division, alleging that an Assistant Director was engaged in an inappropriate relationship with a subordinate.

The OIG investigation substantiated the allegation that the Assistant Director was engaged in a romantic relationship with a subordinate and failed to timely report the relationship, in violation of FBI policy. The OIG investigation also found that the Assistant Director allowed the relationship to negatively affect an appropriate and professional superior-subordinate relationship and to disrupt the workplace by interfering with the ability of other FBI employees to complete their work, and that the Assistant Director participated in a hiring or organizational decision involving the subordinate, all in violation of FBI policy.

The OIG has completed its investigation and provided its report to the FBI and DOJ's Office of Professional Responsibility for appropriate action.



Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether Department of Justice personnel have committed misconduct.



FOR IMMEDIATE RELEASE

July 14, 2021

**DOJ OIG Releases Report of Investigation and Review of the FBI's Handling of Allegations of Sexual Abuse
by Former USA Gymnastics Physician Lawrence Gerard Nassar**

Department of Justice (DOJ) Inspector General Michael E. Horowitz announced today the release of an Investigation and Review of the Federal Bureau of Investigation's (FBI) Handling of Allegations of Sexual Abuse by Former USA Gymnastics Physician Lawrence Gerard Nassar.

The DOJ Office of the Inspector General (OIG) found that senior officials in the FBI Indianapolis Field Office failed to respond to allegations of sexual abuse of athletes by former USA Gymnastics physician Lawrence Gerard Nassar with the urgency that the allegations required. We also found that the FBI Indianapolis Field Office made fundamental errors when it did respond to the allegations, failed to notify the appropriate FBI field office (the Lansing Resident Agency) or state or local authorities of the allegations, and failed to take other steps to mitigate the ongoing threat posed by Nassar.

After eight months of inaction by the FBI Indianapolis Field Office, the FBI Los Angeles Field Office received the same allegations. The OIG found that while the Los Angeles Field Office took numerous investigative steps, it too failed to notify the FBI Lansing Resident Agency or state or local authorities of the allegations, and failed to take other steps to mitigate the ongoing threat posed by Nassar. The FBI Lansing Resident Agency did not become aware of the Nassar allegations until after the Michigan State University Police Department (MSUPD) executed a search warrant on Nassar's residence in September 2016, following the MSUPD's receipt of separate complaints of sexual abuse by Nassar, and discovered child pornography at Nassar's residence. During this period from July 2015, when the allegations were first reported to the FBI, to September 2016, Nassar continued to treat gymnasts at Michigan State University, a high school in Michigan, and a gymnastics club in Michigan. Ultimately the investigations determined that Nassar had engaged in sexual assaults of over 100 victims and possessed thousands of images of child pornography, led to his convictions in federal and state court, and resulted in Nassar being sentenced to incarceration for over 100 years.

The OIG further found that, when the FBI's handling of the Nassar matter came under scrutiny from the public, Congress, the media, and FBI headquarters in 2017 and 2018, Indianapolis Field Office officials did not take responsibility for their failures. Instead, they provided incomplete and inaccurate information to make it appear that they had been diligent in responding to the sexual abuse allegations.

The specific findings of the report include:

- Officials in the Indianapolis Field Office violated numerous FBI policies in handling the Nassar allegations. Specifically, officials in the Indianapolis Field Office:

- failed to formally document a July 28, 2015 meeting with USA Gymnastics during which the FBI first received the allegations against Nassar;
 - failed to properly handle and document receipt and review of relevant evidence, i.e., a thumb drive provided by USA Gymnastics President Stephen D. Penny, Jr.;
 - failed to document until February 2017 an interview of a gymnast that was conducted on September 2, 2015, during which the gymnast alleged sexual assault by Nassar; and
 - failed to transfer the Nassar allegations to the FBI Lansing Resident Agency, where venue most likely would have existed for potential federal crimes.
- Indianapolis Field Office Special Agent in Charge (SAC) W. Jay Abbott and an Indianapolis Field Office Supervisory Special Agent (Indianapolis SSA) made false statements. Specifically, we concluded that the gymnast interview summary that the Indianapolis SSA drafted in February 2017, 17 months after the interview took place, contained materially false statements and omitted material information. We further concluded that the Indianapolis SSA made materially false statements when twice questioned by the OIG about the victim interview. In addition, we concluded that Abbott made materially false statements during his OIG interviews to minimize errors made by the Indianapolis Field Office in connection with the handling of the Nassar allegations.
 - Abbott violated FBI policy and exercised extremely poor judgment under federal ethics rules when he, without prior authorization, communicated with Penny about a potential job opportunity with the U.S. Olympic Committee, an entity with which Penny had professional connections. Abbott communicated with Penny about the potential job opportunity while the two continued to discuss the allegations against Nassar and while Abbott took an active role in conversations about the FBI's public statements regarding USA Gymnastics' handling of those allegations. Abbott should have known—and we found that he in fact did know—that this conduct would raise questions regarding his impartiality. Further, Abbott applied for the position with the U.S. Olympic Committee, and then falsely denied that he had done so when questioned by the OIG on two separate occasions.

In addition, the OIG identified shortcomings in the FBI's policies, including its policy regarding notification of local law enforcement agencies in child exploitation cases, that should be further assessed to ensure that the FBI can more effectively handle these types of matters. The DOJ OIG made four recommendations to the FBI to address the concerns we identified. The FBI agreed with the recommendations.

Report: Today's report and an interactive timeline of key events is available on our website at the following link: <https://oig.justice.gov/reports/investigation-and-review-federal-bureau-investigations-handling-allegations-sexual-abuse>

###



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

April 6, 2021

FOIPA Request No.: 1493405-000
Subject: Employee Misconduct Complaints
to Insider Threat Office resulting in OPR
Investigations
(October 2018 – October 2019)

Dear Mr. Fernandes:

This letter is in response to your Freedom of Information/Privacy Acts (FOIPA) request. Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

Material responsive to your request is being withheld in its entirety by the FBI pursuant to subsections (b)(6) and (b)(7)(C). See attached Explanations of Exemptions.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. **"Part 1"** of the Addendum includes standard responses that apply to all requests. **"Part 2"** includes additional standard responses that apply to all requests for records about yourself or any third party individuals. **"Part 3"** includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

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

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Sincerely,

A handwritten signature in black ink, appearing to read "M. G. Seidel", with a stylized flourish at the end.

Michael G. Seidel
Section Chief,
Record/Information
Dissemination Section
Information Management Division

Enclosure

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E), (b)(7)(F), and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

- (i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems or locations where responsive records would reasonably be found. A standard search normally consists of a search for main files in the Central Records System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. Unless specifically requested, a standard search does not include references, administrative records of previous FOIPA requests, or civil litigation files. For additional information about our record searches, visit www.fbi.gov/services/information-management/foipa/requesting-fbi-records.
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.
- (iv) **National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private Citizens cannot request a name check.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

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

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

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

EFOIA Request

Fee waiver requested

Dear Information Officer:

Records sought:

For the FBI Insider Threat Office, I was seeking any records of employee misconduct complaints generated to the Insider Threat office for any employees worldwide for the period

October 2019 - October 2018.

I was seeking any investigations completed during this timeframe which resulted in FBI OPR action for employee misconduct.

The DOJ insider threat directive was issued on Feb 12, 2014.

<https://www.justice.gov/jmd/file/865256/download>

I would like to receive the information in EFOIA style for electronic communication and production. Please produce the documents in .pdf format via email.

Fee Categorization

For fee categorization purposes, I am a representative of the news media. Through this request, I am gathering information for my journalistic work with Muckrock.com, and DocumentCloud.com. I am an active participant in the dissemination of public records for public education purposes. Accordingly, I am 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); id. § 552(a)(4)(A)(iv)(II).

Request for Fee Waiver

Please waive any applicable fees. The release of the information is not primarily in my commercial interest and will contribute significantly to public understanding of government operations and activities.

Conclusion

If my request is denied in whole or part, please justify all withholdings by reference to specific exemptions and statutes, as applicable. For each withholding please also explain why your agency

"reasonably foresees that disclosure would harm an interest protected by an exemption" or why
"disclosure is prohibited by law. Duties in relation to this requested data require post-haste execution for support of national security interests. Please utilize the redaction feature ethically.

Vaughn Index Requested

I would appreciate your communicating with me by email:

I look forward to your determination regarding my request within 20 business days, as the statute requires.

Thank you in advance for your assistance.

Sincerely,

William Fernandes

Intelligence

Public Affairs



Approved On: 12 FEB 2014

DOJ ORDER

INSIDER THREAT

PURPOSE: This Order establishes policy and assigns responsibilities for a Department of Justice (DOJ) Insider Threat Prevention and Detection Program (ITPDP).

SCOPE: This Order is applicable to all DOJ Components with access to classified information, including classified computer networks controlled by DOJ; all classified information on those networks; and DOJ employees, contractors, and others who access classified information or classified computer networks controlled by DOJ ("cleared employee").

ORIGINATOR: Justice Management Division, Information Technology Security Staff

CATEGORY: (I) Administrative, (II) Information Technology

AUTHORITY: Executive Order (EO) 13587 of October 7, 2011, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; EO 12968 of August 2, 1995 (as amended), Access to Classified Information; EO 13526 of December 29, 2009, Classified National Security Information; Presidential Memorandum of November 21, 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

CANCELLATION: None

DISTRIBUTION: This Order is distributed electronically to those components referenced in the "SCOPE" section as well as posted to the DOJ Directives electronic repository ([SharePoint](#)).

APPROVED BY: Eric H. Holder, Jr.
Attorney General

ACTION LOG

All DOJ directives are reviewed, at minimum, every five years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled or superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Approval	Eric H. Holder, Jr.	Feb. 12, 2014	This Order establishes policy and assigns responsibilities for a Department of Justice (DOJ) Insider Threat Prevention and Detection Program (ITPDP).



TABLE OF CONTENTS

Glossary of Terms..... 4

I. Policy 5

 A. Insider Threat Prevention and Detection Program..... 5

 B. Insider Threat Working Group..... 5

II. Roles and Responsibilities 5

 A. Senior Department Official..... 5

 B. CI Executive Agents. 5

 C. The DOJ ITWG..... 5

 D. DOJ ITPDP 6

 E. Heads of Components 7

Appendix A: Authorities..... 8

GLOSSARY OF TERMS

DEFINITIONS

Term	Definition
Counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities (EO 12333, as amended).
Insider	Any person with authorized access to any U.S. Government resource including personnel, facilities, information, equipment, networks or systems.
Insider Threat	The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of Departmental resources or capabilities.

ACRONYMS

Acronym	Meaning
AAG/A	Assistant Attorney General for Administration
CI	Counterintelligence
CRM	Criminal Division
DOJ	Department of Justice
EO	Executive Order
FBI	Federal Bureau of Investigation
IA	Information Assurance
ITPDP	Insider Threat Prevention and Detection Program
ITWG	Insider Threat Working Group
JMD	Justice Management Division
NSD	National Security Division
OIG	Office of the Inspector General
SDO	Senior Department Official

I. Policy

- A. Insider Threat Prevention and Detection Program.** This Order establishes a DOJ ITPDP for deterring, detecting, and mitigating insider threats. It uses counterintelligence (CI), security, information assurance (IA), and other relevant functions and resources to identify and counter the insider threat. The ITPDP takes advantage of existing federal laws, statutes, authorities, policies, programs, systems, and architectures in order to counter the threat of those insiders who may use their authorized access to compromise classified information. The DOJ ITPDP shall employ risk management principles, tailored to meet the distinct needs, mission, and systems of individual Components, and shall include appropriate protections for legal, privacy, civil rights, and civil liberties requirements.
- B. Insider Threat Working Group.** The Insider Threat Working Group (ITWG) was established pursuant to Executive Order (EO) 13587 to develop policies, objectives, and priorities for integrating security, counterintelligence, user audits, monitoring, and other safeguarding capabilities within the DOJ, in accordance with its charter. The working group will also develop minimum standards and guidance for implementing the insider threat program initiatives throughout DOJ consistent with the U.S. Government insider threat program's national standards and guidance.

II. Roles and Responsibilities

- A. Senior Department Official.** The Assistant Attorney General for Administration (AAG/A) is designated as DOJ's Senior Department Official (SDO) with authority to provide and delegate management, accountability, and oversight of the DOJ ITPDP.
1. The SDO or his designee chairs the ITWG, which is composed of senior staff from Departmental Components with responsibilities for counterintelligence, security, information assurance, human resources, general counsel, and any other relevant responsibilities, functions, and/or resources the SDO deems should be associated with the DOJ ITWG, in accordance with its charter.
 2. The SDO shall issue standards, guidance, and policy developed by the ITWG.
- B. CI Executive Agents.** The Executive Agents for Departmental counterintelligence investigations are the Director of the FBI and the Assistant Attorney General for National Security or their designees. The CI Executive Agents will coordinate all counterintelligence operations, investigations, and prosecutions within DOJ.
- C. The DOJ ITWG.** The DOJ ITWG shall:

1. Develop Departmental minimum standards and guidance consistent with the Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.
2. Address development and implementation of insider threat detection and prevention capabilities and coordinate Departmental resources and procedures for program effectiveness.
3. Consult with records management, legal counsel, ethics officials, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, or civil liberties issues (including use of personally identifiable information) are appropriately addressed.
4. Consult with OIG regarding the establishment of a referral process for complaints and allegations.

D. DOJ ITPDP. The DOJ ITPDP operates under the joint authorities of the heads of the Justice Management Division (JMD), the National Security Division (NSD), and the Federal Bureau of Investigation (FBI). The DOJ ITPDP shall:

1. Operate jointly at a secure operations facility or facilities designated by the SDO.
2. Establish and operate a centralized organizational entity within the operation center(s) to monitor, collect, audit, and analyze data about employees and contractors for insider threat detection and mitigation. Relevant information defined in Departmental insider threat standards and guidance and stored within Components will be made available to the operation center(s).
3. Monitor user activity on DOJ classified computer networks.
4. Evaluate, on an ongoing basis, personnel security records and reporting information.
5. Develop and promulgate Departmental insider threat education, training and awareness, to include employee insider threat reporting responsibilities.
6. Develop an integrated system for the timely reporting of all insider threat incidents and concerns to the DOJ ITPDP for appropriate action and referral to appropriate Departmental investigative organizations.
7. Identify and recommend to the DOJ ITWG standards for any current or future federal and/or public data sources that should be considered for collection and analysis.
8. Develop and implement insider threat information analysis, reporting, and response capabilities.

9. Refer all counterintelligence inquiries that indicate classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power to the DOJ CI Executive Agents.
10. Assist Departmental Components as necessary to implement and improve insider threat detection and prevention capabilities.
11. Conduct assessments of Departmental Components, as directed by the SDO, to determine the level of organizational compliance with this policy and minimum insider threat standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee in accordance with 2.1(c) of EO 13587.

E. Heads of Components. The head of each Departmental Component with employees who have access to classified information, or that operate or access classified computer networks, or the Component head's designee, shall:

1. In coordination with the DOJ ITPDP, implement DOJ policy and minimum standards issued pursuant to this policy.
2. Ensure that insider threat concerns are reported to the DOJ ITPDP as defined in Departmental insider threat standards and guidance issued pursuant to this policy.
3. Promulgate additional Component guidance, if needed, to reflect unique mission requirements consistent with meeting the minimum standards and guidance issued pursuant to this policy.
4. Under the guidance of the DOJ ITPDP, perform self-assessments at least annually of compliance with insider threat policies and standards and report the results to the DOJ ITPDP.
5. Enable independent assessments, in accordance with Section 2.1(d) of EO 13587, of compliance with established insider threat policy and standards by providing information and access to personnel of the ITPDP.
6. Implement insider threat education, training, awareness, and reporting responsibilities issued pursuant to this policy.
7. The Departmental Components with elements that are members of the Intelligence Community (IC) shall establish an Insider Threat Detection and Prevention capability that meets mission and IC requirements and that integrates with the DOJ ITPDP.

APPENDIX A: AUTHORITIES

Nothing in this policy shall be construed to supersede or change the requirements of the National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order 12333, as amended (2008); Executive Order 13467, (2008); Executive Order 13526, (2009); Executive Order 12829, as amended, (1993); Executive Order 13549 (2010); Executive Order 13587 (2011), and Executive Order 12968, (1995) and their successor orders or directive.



U.S. Department of Justice

Justice Management Division

Office of General Counsel

Washington, D.C. 20530

MuckRock.com
110778-52139965@requests.muckrock.com

RE: JMD FOIA # 125643

Dear Mr. Fernandes,

I am responding on behalf of the Justice Management Division (JMD) to your Freedom of Information Act (FOIA) request dated April 7, 2021, for “records in JMD custody related to: Any records of employee misconduct complaints generated to the Insider Threats office(s) for any FBI or DEA employees worldwide for the period October 2019 – October 2018” and “copies of any investigations completed during the same timeframe which resulted in FBI OPR or DEA OPR action for employee misconduct.”

We have conducted a search within JMD, but any records relating to misconduct incidents reported to the Justice Insider Threat Center are withheld in full under FOIA Exemptions 6 and 7(C), which relate to information the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy, and Exemption 7(E), which concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. Investigation records resulting in FBI or DEA OPR action, if any, would be maintained by the FBI or DEA, not JMD.

You may contact our FOIA Public Liaison, Karen McFadden at (202) 514-3101 or JMDFOIA@usdoj.gov for further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with JMD’s determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the

instructions on OIP's website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

Morton J. Posner
Deputy General Counsel