



governmentattic.org

"Rummaging in the government's attic"

Description of document: Selected Federal Election Commission (FEC) Inspector General (OIG) Investigation Reports 2022-2023

Requested date: 21-February-2025

Release date: 24-March-2025

Posted date: 19-May-2025

Source of document: Federal Election Commission
Attn: FOIA Requester Service Center
1050 First Street, NE
Washington, DC 20463
Fax: 202-219-3923
Email: FOIA@fec.gov
FOIA.gov

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: Katrina Sutphin <ksutphin@fec.gov>
Sent: Monday, March 24, 2025 at 03:07:48 PM EDT
Subject: Re: Your Freedom of Information Act Request to the Federal Election Commission FOIA [2025-211]

VIA ELECTRONIC MAIL

Re: Your Freedom of Information Act Request to the Federal Election Commission FOIA [2025-211]

This email is in response to the request you filed for information under the Freedom of Information Act (FOIA) dated and received by the Federal Election Commission's (FEC) FOIA Requester Service Center on February 21, 2025. Specifically, you requested:

"A copy of the final report and report of investigation and closing report and closing memo and referral for each of these closed investigations: I22INV00002, I22INV00033, I22INV00004 and I22INV00035."

We have searched our records and have located responsive documents, which we are releasing in part. Attached to this letter are 23 pages of responsive records the Agency located that are not exempt from disclosure. We have applied B(6) redactions to these records. We have withheld INV00004 under FOIA Exemption B(6) and INV00033 under B(5) and B(6). We have withheld 1 page of records under B(5). Please note that our response to your request does not include documents or publications publicly available on our website or compilations of publicly available news articles.

Exemption 5 protects from disclosure inter- or intra-agency memoranda or letters that would not be available by law to a party other than an agency in litigation with the agency, including documents covered by the attorney work-product, deliberative process, and attorney-client privileges. See 5 U.S.C. § 552(b)(5).

Exemption 6 protects personal information, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. See 5 U.S.C. § 552(b)(6).

Accordingly, your FOIA request has been granted in part.

You may contact our FOIA Public Liaison, Amber Smith at (202) 694-1437, for any 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.

You may appeal any adverse FOIA determination. Any such appeal must be filed in writing and should follow the guidelines set forth in 11 C.F.R. § 4.8. If you have any questions, please contact the FOIA Requester Service Center at FOIA@fec.gov, or (202) 694-1650.

Sincerely,

FOIA Requester Service Center

Case Number	I22INV00002	Case Title	Investigation of Alleged Misuse of Government Resources to Access Inappropriate Material		
Lead Agent	b6	Region / Office	OIG Office of Investigations	Case Status	Closed

Note: All fields marked with * are mandatory

Referral to Others

Referral Entry

Add Attachments

Date Referred	02/28/2022
Referred To	Other
Date Response Due	mm/dd/yyyy
Date Response Received	mm/dd/yyyy
Date Referral Closed	mm/dd/yyyy
Status of Referral	CLOSED
Name	
Email	
Phone	



Comments b6 b6 and b6 b6 contacted the Arlington Police Internet Crimes unit b6 b6 and the FBI WFO to inform them we found some images of potential child pornography and see if they want us to refer the case to them.




Insert Case Referral



Federal Election Commission
Office of the Inspector General

MEMORANDUM

TO: The Commission

FROM: Christopher Skinner 
Inspector General

SUBJECT: OIG Report of Investigation I22INV00002 - *Investigation of Alleged Misuse of Government Resources to Access Inappropriate Material*

ENCL: OIG Report of Investigation I22INV00002

DATE: December 14, 2023

This memorandum transmits the Office of Inspector General's (OIG) final Report of Investigation I22INV00002 - *Investigation of Alleged Misuse of Government Resources to Access Inappropriate Material*.

We initiated this investigation on January 26, 2022, based on a report that files on an FEC OGC shared drive contained sexually explicit videos. After an extensive investigation that involved review of multiple FEC drives and devices, the OIG concluded that **b6**, a then-FEC **b6**, violated federal regulation and agency policy concerning the use of government-issued information technology resources by downloading, copying, and/or viewing inappropriate material on **b6** FEC-issued laptops and an FEC shared drive between 2018 and 2022.

The OIG withheld case closure and summary publication at the request of external law enforcement personnel pending further investigation. As of December 11, 2023, the Arlington County Police Department reported that the case has been closed due to insufficient evidence.

Accordingly, detailed findings can be found in the enclosed report, a summary of which will be posted on the FEC OIG webpage in accordance with *OIG Policy 500.1, Issuance and Publication of OIG Investigative Reports*. Should you have any questions regarding this report and its conclusions, please contact **b6** at **b6**. Thank you.

cc: **b6**

b6

FEDERAL ELECTION COMMISSION

Office *of the* Inspector General



Report of Investigation

Investigation of Alleged Misuse of Government Resources to Access Inappropriate Material

Case Number: I22INV00002

August 10, 2022

RESTRICTED INFORMATION: This report is the property of the Office of Inspector General and is for **OFFICIAL USE ONLY**. This report is confidential and may contain information that is prohibited from disclosure by the Privacy Act, 5 U.S.C. §552a. Therefore, this report is furnished solely on an official need-to-know basis and must not be reproduced, disseminated or disclosed without prior written consent of the Inspector General of the Federal Election Commission or designee. All copies of the report have been uniquely numbered and should be appropriately controlled and maintained. Unauthorized release may result in civil liability and/or compromise ongoing federal investigations.

Table of Contents

Page

I. EXECUTIVE SUMMARY	3
II. STANDARDS	6
III. FINDINGS	7
IV. RECOMMENDATIONS	13

I. EXECUTIVE SUMMARY

The Federal Election Commission (FEC) Office of the Inspector General (OIG) initiated an investigation on January 26, 2022, based on a referral from the agency's Staff Director and the Office of General Counsel (OGC). The referral alleged that a file folder in a FEC shared drive contained videos depicting a nude woman.

After an extensive investigation that involved review of multiple FEC drives and devices, the OIG concluded that [REDACTED], an FEC [REDACTED], violated federal regulation and agency policy concerning the use of government-issued information technology resources by downloading, copying, and/or viewing inappropriate material¹ on [REDACTED] FEC-issued laptops and an FEC shared drive, between 2018 and 2022.

1. OGC File Folder (FEC Shared Drive)

OIG investigators obtained access to the files contained on the relevant FEC file folder with the assistance of the Office of the Chief Information Officer (IT). That file folder contained five sexually explicit or suggestive videos of a female. The folder and individual file properties indicated the creator was [REDACTED].

2. Subject's 2021-Issued Laptop Computer

The OIG sought assistance from IT to remotely scan [REDACTED] current FEC laptop that was issued to [REDACTED] in April 2021 to identify any additional inappropriate material. IT conducted a remote scan of [REDACTED] laptop and provided files to the OIG for review. OIG investigators identified 22 files that contained inappropriate material, including images of partially clothed or nude women and videos of women engaged in various acts, such as posing nude and engaging in actual or simulated masturbation.

3. Subject's 2017-Issued Laptop Computer

On February 10, 2022, the OIG requested [REDACTED] return [REDACTED] prior FEC laptop that was issued to [REDACTED] in July 2017 and was still in [REDACTED] possession. Upon obtaining and reviewing [REDACTED] prior FEC laptop, an IT scan identified approximately 125 gigabytes (GB) of data that appeared inappropriate and warranted OIG review. OIG investigators reviewed those files and identified:

- 8,166 images containing inappropriate material
- 687 videos containing sexually explicit or suggestive content
- 25 PDF files concerning sexual topics
- Numerous adult tourism guides and maps to find prostitutes, strip clubs, and erotic

¹ As used in this report, "inappropriate material" refers to images, videos, or text-based files that display or describe fully or partially nude persons and/or persons engaged in pornographic, sexually explicit, or sexually suggestive acts.

- massage parlors in various countries around the world including Costa Rica, Italy, Mexico, Myanmar, Cambodia, Thailand, and Vietnam
- Multiple files concerning serial killers, depression, mental health, and depression articles from various sources
- Several notable web searches were recovered from FEC equipment, but additional explanation is needed from b6 to corroborate the details

4. False or Misleading Statements

b6 testified over the course of two interviews that the files on the FEC shared drive and b6 current FEC laptop belonged to b6 and that b6 downloaded them to b6 government laptop from b6 personal cell phone.² b6 further testified that b6 took responsibility for b6 actions. However, b6 made numerous misleading and inconsistent statements during b6 interviews. Specifically:

- During b6 first interview, b6 testified that b6 began downloading inappropriate material in approximately 2021. However, data on b6 prior FEC-issued laptop established that b6 did so at least as early as 2018. b6 subsequently admitted b6 had copied inappropriate material to b6 FEC laptop from 2018-2021.
- When asked if b6 prior, 2017-issued FEC laptop contained inappropriate material, b6 testified that b6 had removed anything personal with a flash drive and did not disclose the existence of inappropriate material on that laptop. However, subsequent review identified thousands of files that contained inappropriate material organized into hundreds of folders on that laptop.
- b6 testified that b6 ceased using the 2017-issued laptop after b6 received a new laptop in April 2021, except that b6 attempted to log on to the 2017-laptop on one occasion after b6 received a new Personal Identity Verification (PIV) card in July 2021. However, review of b6 2017-issued laptop identified inappropriate files created in May, June, and July 2021, including 72 pornographic videos, pictures of nude women, and inappropriate animated drawings.

It appears that b6 subverted agency controls that prevent employees from using agency IT resources to access inappropriate material by downloading the material from USB devices rather than via internet connection. Indeed, metadata on b6 devices indicates at least 42 unique USB devices have been connected to b6 prior and current FEC laptops while in b6 possession.

The OIG withheld issuance of this report at the request of external law enforcement personnel. In addition, during the pendency of this investigation, the agency took action to

² As further detailed herein, the OIG did not obtain testimony regarding b6 prior FEC laptop because b6 interviews took place prior to review of that laptop.

remove b6 [REDACTED] access to FEC information systems and b6 [REDACTED] resigned on or about June 30, 2022.

The foregoing findings are provided for such action as may be appropriate. Additionally, the OIG recommends the following actions for the Commission to consider in efforts to reduce the potential for employees to misuse government-issued resources:

1. The Commission should review policies and practices concerning FEC employee use of external USB devices and the agency-established VPN to access agency systems in conducting business.
2. FEC IT should conduct a cost-benefit analysis of the feasibility of conducting routine scans of FEC equipment to detect inappropriate material on government-issued devices.

II. STANDARDS

5 CFR § 2635.101(9) provides, “Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.” 5 CFR § 2635.102 defines employees to include any officer or employee of an agency with exceptions not relevant here.

In addition, the OIG identified two agency policies, *Commission Directive 58: Electronic Records, Software and Computer Usage* (Directive 58) and *Rules of Behavior and Acceptable Use Standard for Federal Election Commission Information and Systems Resources* (Rules of Behavior), that govern the use of government-furnished equipment, such as computers.

Directive 58 outlines the responsibilities of agency employees to ensure that FEC's information systems are used appropriately and protected from loss, misuse, or unauthorized access. To that end, the directive offers guidelines on the use of the agency's computer systems. One of the guidelines applies to sexually explicit materials found on the internet:

- E. The Internet contains material, such as sexually explicit material, that is not appropriate for the workplace. The FEC expects employees to conduct themselves professionally in the workplace and to refrain from using government resources for activities that are offensive to co-workers or the public.

The FEC provides employees with the Rules of Behavior during the completion of mandatory security awareness training.³ Rule 20(b) governs inappropriate material:

- 20. Use of government e-mail and Internet accounts is a privilege, not a right. Specifically:
 - a. There is no expectation of privacy in FEC electronic mail communications.
 - b. Do not send or store inappropriate material using your FEC e-mail or Internet accounts. Do not originate or forward chain letters or hoaxes. Pornography, inappropriate language, gender, racial and religious bias, and anything that may be viewed as sexual harassment will not be tolerated.
 - c. Do not auto-forward e-mail from your FEC account to a personal e-mail account.

³ As detailed in this report, ██████ received agency security awareness training in August 2017 and September 2021.

III. FINDINGS

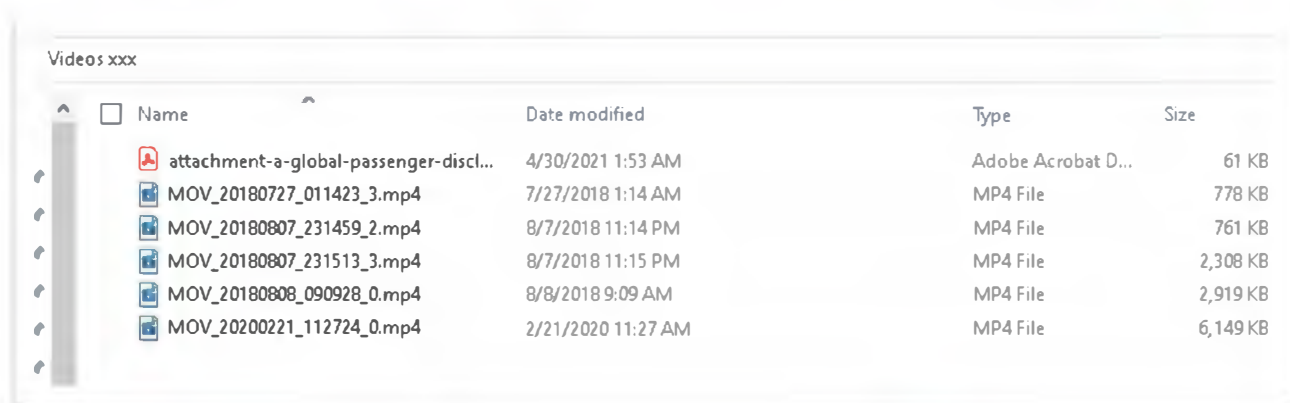
The Federal Election Commission (FEC) Office of the Inspector General (OIG) initiated this investigation on January 26, 2022, based on a referral from the agency's [REDACTED] and OGC that alleged a file folder in the FEC shared drive contained a folder labeled "videos XXX" with inappropriate material. The IG and Deputy IG conferred with the [REDACTED] b6 and Office of General Counsel (OGC) and concurred that the matter warranted investigation.

1. Files contained on the FEC OGC shared drive contained inappropriate material uploaded by FEC employee, [REDACTED] b6

The OIG sought assistance from the Office of the Chief Information Officer (IT) to confirm the sub-folder owner and preserve a copy for investigation. IT reviewed the properties in the folder and confirmed that the owner was [REDACTED] b6 an FEC [REDACTED] b6.

The OIG obtained a copy of the "videos XXX" sub-folder. The sub-folder contained six items: one PDF document and five video clips. The PDF document did not contain anything inappropriate. However, the five video clips featured a nude female performing various sexually suggestive acts.

According to the details retrieved from the Windows operating system, the inappropriate files appeared on the FEC servers in late July and early August 2018. The last video to appear in the "videos XXX" sub-folder appeared on the FEC servers in February 2020. As depicted below, the file named "MOV_20180808_090928_0.mp4" was modified on August 8, 2018, at 9:09 AM.⁴ The OIG obtained [REDACTED] timesheet for that pay period and verified [REDACTED] b6 workday included August 8, 2018, from 9:00 AM to 6:30 PM.



Name	Date modified	Type	Size
attachment-a-global-passenger-discl...	4/30/2021 1:53 AM	Adobe Acrobat D...	61 KB
MOV_20180727_011423_3.mp4	7/27/2018 1:14 AM	MP4 File	778 KB
MOV_20180807_231459_2.mp4	8/7/2018 11:14 PM	MP4 File	761 KB
MOV_20180807_231513_3.mp4	8/7/2018 11:15 PM	MP4 File	2,308 KB
MOV_20180808_090928_0.mp4	8/8/2018 9:09 AM	MP4 File	2,919 KB
MOV_20200221_112724_0.mp4	2/21/2020 11:27 AM	MP4 File	6,149 KB

⁴ The OIG obtained [REDACTED] b6 timesheet for that pay period and verified [REDACTED] b6 workday included August 8, 2018, from 9:00 AM to 6:30 PM.

To obtain the circumstances surrounding the discovery of the sub-folder, the OIG interviewed the [b6] who reported the incident. According to the [b6] they were informed by a subordinate on January 6, 2022, that a staff attorney had found inappropriate material in the OGC folder while conducting research. Specifically, the staff attorney found a sub-folder labeled “videos XXX” while navigating through the OGC folders.

The [b6] further testified that approximately 20 minutes after learning of the folder, they notified the [b6]. The [b6] reviewed the content of one of the files, found that it contained sexually explicit material, and notified the OIG and [b6].

2. Review of [b6] current FEC-issued laptop identified additional inappropriate material.

The OIG requested that IT identify information resources assigned to [b6]. IT confirmed through agency records that the subject had been assigned two agency laptops, the first issued on July 19, 2017 (FEC asset tag 610344) and the second issued on April 20, 2021 (FEC asset tag 611916), as part of the agency-wide migration to Windows 10 systems.⁵ IT confirmed that both laptops were in [b6] possession and that the 2021-issued laptop was currently in use and could be remotely scanned.

OIG investigators requested that IT scan [b6] 2021-issued laptop to identify potential inappropriate material. On February 1, 2022, IT established a remote connection to [b6] 2021-issued laptop and discovered 45 files that warranted review. The OIG requested IT create an encrypted replica of all files and forward them to the OIG for further review. The OIG reviewed the 45 files and identified 22 files that contained inappropriate material, including files that were identical to the video files contained on the OGC shared drive.

OIG investigators identified 12 movie files, which contained nude women engaged in various sexual acts, three files containing images of nude women in various explicit poses, and an image of one woman clothed in lingerie kneeling on a bed. There were two image files: one of a woman with her middle finger extended in the air and a second image of the same woman with her finger in her mouth. The subject later identified this woman as [b6] interview; based on her appearance she appears to be the same woman in numerous other files, including the original videos discovered on the OGC shared drive.

OIG investigators also identified an image of a phallic device with a gift box and a Microsoft Word document containing a product review of the device. [b6] later confirmed during [b6] interview that [b6] was the author of the Word document. The 2021-issued laptop also contained material from the adult magazines *Bella Cariño* and *Chambeadoras*. Other

⁵ IT subsequently identified a third laptop that had been issued to [b6] years prior, but that laptop has since been decommissioned and was, thus, unavailable for review.

content included images of an advertisement for a life-size inflatable female sex doll and a woman holding a spandex buttock shaper.

3. b6 testified that the inappropriate material on the FEC drive and 2021-issued laptop were b6 but denied there was inappropriate material on b6 2017-issued FEC laptop.

On February 7, 2022, and February 11, 2022, OIG investigators interviewed b6 to obtain b6 sworn testimony. In summary, b6 admitted that the files on the shared drive and 2021-issued laptop belonged to b6 and were downloaded to b6 government laptop from b6 personal cell phone b6. b6 further stated that b6 took responsibility for b6 actions. However, when asked if b6 prior FEC laptop contained inappropriate material, b6 b6 stated that b6 had removed all personal data from b6 2017-issued FEC laptop.

On February 7, 2022, the OIG interviewed b6 via Microsoft Teams with National Treasury Employees Union (NTEU) representation present. As seen in the figure below, and with the assistance of b6 the OIG confirmed that FEC laptop tag 611916 was in b6 possession (relevant section highlighted in yellow).



During the interview, OIG investigators used Microsoft Teams to share the image of the sex doll advertisement and a document containing a product review for a phallic device. b6

b6 explained that b6 downloaded the doll advertisement because b6 thought it was amusing. When confronted with the product review, b6 admitted b6 was the author.

Also, during the interview, while an OIG investigator was preparing to display images via Microsoft Teams, b6 noticed two enqueued photographs and spontaneously stated (i.e., without having been asked) that the female in the two photographs is b6

b6 testified that b6 used b6 personal cell phone (Samsung Galaxy X5) to transfer personal files from the phone to a flash drive to free up memory. b6 stated b6 accomplished this by plugging b6 cell phone with a USB cable into b6 government laptop to transfer the files to b6 FEC computer's desktop. Then b6 would upload the files from the laptop to a personal flash drive. Review of the Windows 10 registry concluded that a Memorex USB flash drive was used to read and write the files onto the computer.

b6 requested a brief pause of the interview to confer with b6 NTEU representative. Upon resuming the interview, b6 declared b6 responsibility for the images. b6 stated that b6 was embarrassed by b6 behavior. b6 agreed to provide a voluntary written statement to the OIG explaining the details of b6 inappropriate use of agency equipment. b6 indicated b6 did not share the images with any agency employees. b6 stated b6 takes this "very, very seriously." b6 then stated b6 had nothing else to add because b6 was overwhelmed by the situation at the moment.

On February 8, 2022, after consulting with NTEU counsel, b6 emailed OIG investigators and declined to provide a written statement attesting to b6 actions.

OIG investigators conducted a second interview with b6 on February 11, 2022. b6 was again represented by the NTEU. During the interview, b6 stated b6 was aware that it was improper to store images of nude women or women engaged in sexual acts on b6 FEC laptop. When asked if b6 prior FEC laptop contained inappropriate material, b6 b6 stated that b6 had removed all personal data from b6 prior FEC laptop.

4. Review of b6 prior FEC-issued laptop identified additional inappropriate material.

Concurrent with the foregoing interviews, the OIG requested b6 return b6 prior FEC laptop that was issued to b6 in July 2017 and was still in b6 possession. On February 11, 2022, IT received b6 laptop and established chain of custody documentation. IT reported damage to the front left and side of the laptop. The OIG requested that IT scan the laptop for any potential inappropriate material. The scan identified approximately 125 gigabytes (GB) of data that warranted OIG review. OIG investigators reviewed the data and identified the following:

- 687 videos that contained inappropriate material (e.g., fully or partially nude persons and/or persons engaged in pornographic, sexually explicit, or sexually suggestive acts)⁶
- 8,166 sexually explicit or suggestive images
- Adult tourism guides and maps to find prostitutes in Costa Rica, Italy, Mexico, Myanmar, Thailand, and Vietnam that were copied from multiple websites
- Metadata that indicated at least 42 cameras, USB flash drives, or similar devices had been connected to b6 laptop
- Several notable web searches were recovered from FEC equipment, but additional explanation is needed from b6 to corroborate the details

5. b6 made misleading and inconsistent statements during b6 interviews.

b6 made numerous misleading and inconsistent statements based on contradictions among the testimony from b6 first interview, b6 follow-up interview and evidence obtained from b6 government laptops. Specifically:

- In b6 first interview, b6 testified b6 began downloading the inappropriate material from b6 cell phone to b6 government laptop approximately one year prior (i.e., 2021). During the follow-up interview, after confronted with evidence that contradicted b6 prior statement, b6 admitted that b6 copied the inappropriate files from b6 cellular phone to b6 FEC laptop from 2018 to 2022. Additionally, review of the laptop issued to b6 in 2017 identified inappropriate files uploaded by b6 as early as Wednesday, November 21, 2018, at 11:51:01 AM, EST, during b6 scheduled work hours.
- In b6 first interview, OIG investigators asked b6 if there were any inappropriate materials on the 2017-issued laptop. b6 responded that b6 had removed anything personal with a flash drive and did not disclose the existence of inappropriate material on that laptop. However, review of the computer recovered thousands of files that contained inappropriate material organized in hundreds of folders on the laptop.
- During a follow-up interview, b6 testified b6 never used the 2017-issued laptop after b6 received a new laptop in April 2021. b6 also stated that the last time b6 logged into the 2017-issued laptop was when b6 received b6 current laptop, except that b6 attempted to log into the 2017-issued laptop to verify that it worked when b6 had b6 Personal Identity Verification (PIV) card renewed in July 2021. However, review of b6 2017-issued laptop identified inappropriate files created in May, June, and July 2021. Specifically, 72 pornographic videos, pictures of nude women, and inappropriate animated drawings were created after April 2021. The OIG and IT

⁶ A "Videos XXX" folder was discovered on the subject's 2017-issued laptop. The original five videos discovered on the FEC servers on January 6, 2022 were in this folder.

review identified no additional files that were created on the 2017-issued laptop after July 7, 2021, implying that b6 used b6 2017-issued laptop exclusively for inappropriate and unofficial purposes after b6 received b6 new laptop in April 2021.

6. b6 conduct violated federal regulation and agency policy concerning use of IT resources.

b6 violated the provision of 5 CFR § 2635.101(9) that provides, “Employees shall protect and conserve Federal property and shall not use it for other than authorized activities” by using b6 government laptop to view and/or transfer inappropriate material from b6 personal cell phone (or other device) to a flash drive (or other device). It is clear that doing so is unauthorized in light of relevant agency policies (Directive 58 and the FEC Rules of Behavior), both of which prohibit the use of agency information resources to access sexually explicit material.

The OIG confirmed with OCIO that b6 had received training on computer security awareness. b6 training certificate showed that b6 completed “FEC Security Awareness Policies, Regulations, and Best Practices” on August 8, 2017. The course content included a copy of the Rules of Behavior, which contained information on the proper usage of agency equipment. Additionally, OCIO confirmed that b6 last completed security awareness training in September 2021.

b6 conduct created significant risks to agency information technology resources by exposing agency systems (including a shared drive on the agency server) to potentially harmful files that may include viruses and malware. Moreover, b6 actions to subvert agency controls by copying files from a personal device potentially exacerbated those risks. A review of b6 2017-issued laptop indicated b6 had connected at least 42 cameras, USB flash drives, or similar devices to the laptop without approval from IT. Connecting a personal device that is not approved by IT to the agency’s resources increases the potential to introduce viruses and malware to the agency’s systems.

IV. RECOMMENDATIONS

The foregoing findings are provided for such action as may be appropriate. Additionally, the OIG recommends the following actions for the Commission to consider in efforts to reduce the potential for employees to misuse government-issued resources. The OIG will report and track the status of these recommendations, similar to any audit or special review.

1. The Commission should review policies and practices concerning FEC employee use of external USB devices and the agency-established VPN to access agency systems in conducting business.
2. FEC IT should conduct a cost-benefit analysis of the feasibility of conducting routine scans of FEC equipment to detect inappropriate material on government-issued devices.



Federal Election Commission
Office of the Inspector General

MEMORANDUM

TO: The Commission

FROM: [REDACTED] b6

SUBJECT: Report of Investigation I22INV00035: Allegation of Improper Hiring Practices

DATE: December 12, 2022

1. Background and Summary

The Federal Election Commission (FEC) Office of the Inspector General (OIG) received an anonymous hotline complaint on July 29, 2022 that alleged improprieties concerning a recent hiring action for an Assistant General Counsel (Team Lead) for Enforcement Team 5. Specifically, the complaint alleged the Enforcement Division of the Office of General Counsel (OGC) failed to follow proper procedures in recruiting a new Team Lead for Enforcement Team 5 by filling a vacancy that was not posted through USAJOBS and failing to compete the vacancy. Furthermore, the complaint alleged the [REDACTED] b6 [REDACTED] did not solicit interest in the position on an acting basis as has purportedly become the customary practice within OGC.

The OIG initiated a preliminary inquiry after receiving the hotline allegation. Since the complaint was anonymous, the OIG was unable to contact the complainant for additional details. As such, the OIG conducted the inquiry with the limited information provided in the complaint form.

The OIG inquiry found the allegation was not substantiated because, contrary to the complaint, the selection for the vacancy generally followed applicable federal guidelines and internal policies for federal hiring. Specifically, the vacancy was announced on USAJOBS (as part of an announcement to fill multiple Team Lead positions for Enforcement) four months prior to the selection of the Team 5 position. Moreover, contrary to the allegation that OGC did not solicit interest on an acting basis, the OIG found that OGC made two internal announcements in the latter part of 2021 for detail opportunities in the Team 5 position. Finally, the selection for Enforcement Team 5 was competed using a hiring panel comprised of three FEC managers. Accordingly, the OIG found no evidence to support the complaint and closed this matter with no recommendations for FEC management.

2. Relevant Standards

The Merit System Principles codified at 5 U.S.C. § 2301 guide agencies when recruiting and selecting applicants for federal positions. In particular, 5 U.S.C. § 2301(b)(1) provides:

(b) Federal personnel management should be implemented consistent with the following merit system principles:

(1) Recruitment should be from qualified individuals from appropriate sources in an endeavor to achieve a work force from all segments of society, and selection and advancement should be determined solely on the basis of relative ability, knowledge, and skills, after fair and open competition which assures that all receive equal opportunity.

The FEC Office of Human Resources (HR) provided the OIG with an additional internal policy, Personnel Instruction 300.1. It sets forth the policies and procedures adopted by the Commission to carry out the Merit System Principles. It provides, in relevant part:

III. POLICY: It is the policy of the Commission to ensure that all qualified applicants are provided an equitable and systematic means of consideration for advertised vacancies based on merit. Further, it is the Commission's policy that internal selections and promotions be based on merit. No individual will be discriminated against or extended special consideration based on any of the following: race, color, religion, national origin, sex, age, political affiliation, handicapping condition, nepotism, personal favoritism or other non-merit factors.

Additionally, Personnel Instruction 300.1 sets forth the procedure for announcing vacancies, such as publishing announcements on USAJOBS. The relevant part states:

B). Posting Vacancy Announcements:--In consultation with the Originating Office, the Office of Human Resources will prepare a vacancy announcement to be published on the Agency Jobs Web Site, Agency Bulletin Boards, and OPM USA Jobs when filled outside the agency as required by Title 5 CFR Section 330.706, and other locations as listed below and the listing will include the following information.

3. Facts

In the course of reviewing the facts and circumstances surrounding the recruitment action in question, the OIG obtained and reviewed relevant records. The OIG also interviewed the [REDACTED] as a subject matter expert and fact witness related to the selection process. Those records and the [REDACTED] testimony established the following.

By way of background, in the latter part of 2021, OGC made two internal announcements for temporary detail opportunities within the office. On August 10, 2021, the [REDACTED] sent an email announcement to FEC staff soliciting interest for three temporary detail positions in Enforcement because of recent staff departures. One of the three positions was for the Enforcement Team 5 Lead. OGC re-advertised the Team 5 position via email on October 5, 2021, along with other team lead acting opportunities.

The [REDACTED] announced the selections for the temporary details to agency staff via email on November 2, 2021. Among the four selectees were three individuals who were eventually appointed to permanent positions as Team Leads.

The recruitment for the permanent Team Lead positions occurred on March 15, 2022, when the Office of the Staff Director sent an internal email to FEC staff informing them that, “the Federal Election Commission is recruiting for the position of Assistant General Counsel for Enforcement, GS-905-15.” The email featured a link to the posting on USAJOBS. The vacancy announcement, FEC-11396461-OPM, opened on March 15, 2022, and closed on March 28, 2022. The announcement stated there were few (i.e., multiple) vacancies in Washington, D.C., and that additional selections may be made from the announcement.

OGC made two selections from the recruitment, and on April 27, 2022, the [REDACTED] informed FEC staff that OGC had selected two individuals for Team Leads to fill vacancies in Team 1 and Team 5.

On July 29, 2022, one of the selectees sent an email to agency staff informing them he was departing the agency. On the same day, the [REDACTED] sent an email announcement to staff informing them that another employee had been selected as Team Lead for Team 5, effective July 31, 2022.

The [REDACTED] testified that the hiring manager used the certificate of qualified applicants from announcement FEC-11396461-OPM to make an additional selection to fill the Team Lead for Team 5, which was corroborated by the relevant records. OIG review of the selection certificate issued on April 7, 2022, confirmed that three internal applicants made the list as “best qualified” with scores above 90 percent. Two of the three applicants were selected for the announcement. A second selection was made on July 21, 2022, the documentation for which indicated the third applicant was selected under the same announcement number.

The [REDACTED] testified that this strategy was used routinely within the agency because it saves the Commission time and resources in the recruitment process (rather than initiating a new recruitment action). The [REDACTED] testimony is generally consistent with FEC Personnel Instruction 300.1, which authorizes hiring managers to make selections from a certificate for up to six months. It provides:

27. SELECTION CERTIFICATE. The official list of Best-Qualified candidates referred to the Selecting Official. The list is valid for up to six months from issue date.

The OIG also reviewed the interview notes recorded by the hiring panel who interviewed all three candidates. The three candidates had experience in OGC and received positive ratings from the hiring panel according to the panelists' notes and score sheets. Furthermore, the Commission ultimately approved the selection of the third selectee by a vote of 6-0.

Timeline of Events Related to Hiring Action for Assistant General Counsel Position



4. Conclusion

The OIG 's inquiry did not substantiate the allegations in the complaint. Contrary to the complaint, the vacancy was filled through a USAJOBS posting and the position was competitively filled using a hiring panel. In addition, the record established that OGC did in fact solicit interest in the position on an acting basis. The OIG was unable to seek additional information related to the allegations since it came from an anonymous complainant. As such, it is unclear why the complainant was misinformed or otherwise incorrect on those points.

We have no recommendations for the agency in this matter. However, because the OIG has received similar allegations in the past related to agency hiring practices, the OIG may conduct further review of agency hiring practices via audit or special review. The OIG will announce any such review upon initiation.

cc:


b6



Federal Election Commission
Office of the Inspector General

MEMORANDUM

TO: The Commission

FROM: Christopher Skinner
Inspector General 

SUBJECT: Preliminary Report of Investigation of Alleged Misuse of Government Resources to Access Inappropriate Material by [REDACTED] (I22INV00002)

DATE: March 9, 2022

1. Background and Summary

The Federal Election Commission (FEC) Office of the Inspector General (OIG) initiated an investigation on January 26, 2022, based on a report that files on an FEC Office of General Counsel (OGC) shared drive contained sexually explicit videos. As detailed further herein, as of the date of this memorandum, the OIG investigation has identified the following on FEC information resources maintained by b6 [REDACTED], an b6 [REDACTED]

- 191 sexually explicit or suggestive videos with a combined duration of over 473 minutes
- 375 images of partially clothed or totally nude individuals
- 23 images of three females whom investigators reasonably suspect are under the age of 18 based on their physical appearances and which are currently under review for potential criminal investigation/prosecution
- Numerous adult tourism guides and maps to find prostitutes, strip clubs, and erotic massage parlors in various countries around the world including Mexico, Costa Rica, and Thailand
- Multiple files concerning serial killers, depression and mental health, that include news articles and cartoons
- Metadata that indicates 42 unique USB devices have been connected to b6 [REDACTED] prior and current FEC laptops while in [REDACTED] possession

The preliminary findings provided in this memorandum are subject to change pending completion of the investigation. The following preliminary findings are provided for such action as may be necessary to, among other things, protect and secure FEC information technology resources and maintain a safe and healthy workforce and workplace.

2. Administrative Standards

The OIG identified 5 CFR § 2635.101 relating to the use of government properties as applicable in this investigation. 5 CFR § 2635.101(9) provides, “Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.”

In addition, the OIG identified two agency policies that govern the use of government furnished equipment, such as computers: *Commission Directive 58: Electronic Records, Software and Computer Usage* (Directive 58) and *Rules of Behavior and Acceptable Use Standard for Federal Election Commission Information and Systems Resources* (Rules of Behavior).

Directive 58 outlines the responsibilities of agency employees to ensure that FEC’s information systems are used appropriately and protected from loss, misuse, or unauthorized access. To that end, the directive offers guidelines on the use of the agency’s computer systems. One of the guidelines applies to sexually explicit materials found on the Internet. Guideline E advises employees that the internet contains material, such as sexually explicit material, that is not appropriate for the workplace, and the FEC expects its employees to refrain from using government resources for activities that are offensive to coworkers or the public.

The FEC document *Rules of Behavior and Acceptable Use Standards for Federal Election Commission Information and Systems Resources* sets forth additional rules concerning the use of FEC information resources. Rule 20(b) provides, in relevant part, “Do not send or store inappropriate material using your FEC e-mail or internet accounts.” The rule further provides, “Pornography, inappropriate language, gender, racial and religious bias, and anything that may be viewed as sexual harassment will not be tolerated.”

3. Preliminary Findings

a. OGC File Folder

OIG investigators obtained access to files contained on the relevant FEC file folder with the assistance of the Office of IT Operations (IT). That file folder contained five sexually explicit or suggestive videos of a female. The folder and individual file properties indicated the creator was b6, which IT confirmed after review.

b. Subject Laptop Computer #1

The OIG further sought assistance from IT to remotely scan b6 current FEC laptop that was issued to b6 in April 2021 to identify any additional inappropriate material. IT conducted a remote scan of b6 laptop and provided files to the OIG for review. OIG investigators identified 22 files that contained inappropriate material, including images of partially clothed or nude women and videos of women engaged in various acts, such as posing nude and engaging in actual or simulated masturbation.

During interviews conducted on February 7, 2022, and February 10, 2022, [REDACTED] admitted to OIG investigators that [REDACTED] had downloaded the foregoing files to [REDACTED] current FEC laptop using a personal USB device. [REDACTED] further denied the existence of inappropriate material on [REDACTED] prior FEC laptop and stated [REDACTED] had deleted all personal files from [REDACTED] prior laptop.

c. Subject Laptop Computer #2

On February 10, 2022, the OIG requested [REDACTED] return [REDACTED] prior FEC laptop that was issued to [REDACTED] in July 2017 and was still in [REDACTED] possession. On February 11, 2022, IT received [REDACTED] laptop and established chain of custody documentation. The OIG requested IT scan the laptop for any potential inappropriate content. The scan identified approximately 127 gigabytes (GB) of data that appeared inappropriate and warranted OIG review. OIG investigators reviewed those files and identified (as of the date of this report):

- Hundreds of sexually explicit or suggestive videos and images, including 23 images of three females whom investigators reasonably suspect are under the age of 18 based on their physical appearances and which are currently under review for potential criminal investigation/prosecution
- Adult tourism guides and maps to find prostitutes, strip clubs, and erotic massage parlors in various countries around the world including Mexico, Costa Rica, and Thailand
- 16 anime (cartoon) files concerning depression
- 35 files referencing serial killers, such as news articles
- Multiple files referencing mental health

d. False or Misleading Statements

[REDACTED] made numerous false or misleading statements based on the testimony from [REDACTED] first interview and subsequent follow-up interview, along with forensic evidence performed on [REDACTED] government laptops. Specifically:

- In the February 7 interview, [REDACTED] testified [REDACTED] started downloading the inappropriate material from [REDACTED] personal cell phone to [REDACTED] government laptop approximately a year ago. It was only during the follow-up interview and after having been confronted by OIG investigators that [REDACTED] admitted [REDACTED] copied the inappropriate files from [REDACTED] cellular phone to [REDACTED] FEC laptop from 2018 to as recently as 2022. Additionally, forensic analysis of the prior laptop issued to [REDACTED] in 2017 determined that [REDACTED] uploaded inappropriate files dating back to 2018.
- During the February 7 interview, OIG investigators asked [REDACTED] if there was any inappropriate material on the 2017-issued laptop. [REDACTED] responded [REDACTED] had removed anything that was of a personal nature with a flash drive. However, a forensic analysis of the laptop identified over 127 GB of inappropriate material organized into multiple folders on the laptop.

- During the February 10 interview, OIG investigators asked b6 if any of the inappropriate activities took place during b6 work hours. b6 stated b6 did not engage in any of the inappropriate activities prior to 2020 because b6 did not bring b6 laptop home from the office, and that b6 “did not really do stuff like that as much at the agency.” However, a forensic analysis of the 2017-issued laptop showed b6 uploaded inappropriate files during the agency’s core work hours from 2018 to 2021, and while b6 was in duty status.
- In the same February 10 interview, b6 testified b6 never used the 2017-issued laptop once b6 had received a new laptop in April 2021. b6 also stated that the last time b6 logged into the 2017-issued laptop was when b6 got the new one, except that b6 attempted to log into the 2017-issued laptop to verify that it worked when b6 had b6 Personal Identity Verification (PIV) card renewed in July 2021. However, a forensic analysis identified inappropriate files dating to May 2021 and June 2021 were on b6 2017-issued laptop.

e. Timeframe

OIG review of metadata associated with the foregoing files determined that b6 transferred sexually explicit or otherwise inappropriate content to b6 FEC-issued laptops during 31 different pay periods beginning as early as November 21, 2018. The data indicate that b6 conduct continued to as recent as January 3, 2022. Based on b6 work schedule, OIG investigators have preliminarily determined that b6 created, accessed, or modified sexually explicit or otherwise inappropriate content on b6 laptop at least 45 different times during work hours and while in a duty status.

In total, as of the date of this report, the OIG has identified 352 sexually explicit or suggestive videos with a combined duration of over 8 hours. Additionally, the OIG identified approximately 896 images of partially clothed or totally nude individuals. In addition, the OIG identified 42 unique USB devices that have been connected to b6 prior and current FEC laptops while in b6 possession.

The investigation is ongoing due to the volume of remaining material that requires review. As of the date of this report, OIG investigators have identified an additional 1,219 image files that require review.

The foregoing is provided for such action as may be appropriate. The investigation is ongoing, and the preliminary findings provided in this memorandum are subject to change pending completion of the investigation.

cc:

b6