Federal Election Commission
Office *of the* Inspector General

INVESTIGATIVE SUMMARY I22INV00002 DATE: DECEMBER 21, 2023

Investigation of Alleged Misuse of Government Resources to Access Inappropriate Material

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 an FEC shared drive contained videos depicting a nude person.

After an extensive investigation that involved review of multiple FEC drives and devices, the OIG found that an FEC paralegal specialist violated federal regulation and agency policy concerning the use of government-issued information technology resources by downloading, copying, and/or viewing inappropriate material on his FEC-issued laptops and an FEC shared drive, between 2018 and 2022.[1] The OIG issued a Report of Investigation to the Commission on August 10, 2022, that detailed the following findings.[2]

First, files on the FEC shared drive contained inappropriate material uploaded by the subject. The files consisted of five video clips that featured a nude female performing various sexually suggestive acts.

Second, a review of the subject's FEC-issued laptops identified additional inappropriate material. At the OIG's request, the FEC Office of the Chief Information Officer (OCIO) identified through agency records that the subject had been issued two agency laptops, one in 2017 and the second in 2021 as part of an agency-wide migration effort.[3] A review of the 2021 laptop's contents identified 45 files that warranted 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 FEC shared drive.

Third, in the course of two interviews with OIG investigators, the subject testified that the inappropriate material on the shared drive and 2021 laptop were his, but denied there was inappropriate material on his 2017 laptop. The subject admitted that the files on the shared drive

[1] As used in this summary, "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.

[2] As further detailed herein, the OIG withheld publication of this summary pending criminal investigation. In addition, the agency promptly removed the subject's access to FEC information systems and the subject resigned on or about June 30, 2022.

[3] OCIO subsequently identified a third laptop that had been issued to the subject years prior, but that laptop had since been decommissioned and, thus, was unavailable for review.

and 2021 laptop belonged to him and were downloaded to his government laptop from his personal cell phone. The subject further testified that he took responsibility for his actions.

Fourth, despite the subject's denials concerning the 2017 laptop, OIG review of that laptop identified additional inappropriate material. A forensic analysis of the laptop identified approximately 125 gigabytes (GB) of data that contained potentially inappropriate material, including 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)
- 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 the laptop

Fifth, the subject made misleading and inconsistent statements during his interviews. Specifically:

- In the initial interview with OIG investigators, the subject testified he began downloading the inappropriate material from his cell phone to his government laptop approximately one year prior (i.e., 2021). During the follow-up interview, after having been presented with evidence that contradicted his prior statement, the subject admitted that he copied the inappropriate files from his cellular phone to his FEC laptops from 2018 to 2022. Additionally, review of the laptop issued to him in 2017 identified inappropriate files uploaded as early as November 21, 2018, during his scheduled work hours.
- In the initial interview, OIG investigators asked if there were any inappropriate materials on the 2017 laptop. He responded that he had removed anything personal with a flash drive and did not disclose the existence of inappropriate material on that laptop. However, as noted above, digital forensic review identified thousands of files that contained inappropriate material organized in hundreds of folders on the laptop.
- During the follow-up interview, the subject testified he never used the 2017 laptop after he received a new laptop in April 2021. He also stated that the last time he logged into the 2017 laptop was when he received the 2021 laptop, with one exception. However, review of his 2017 laptop identified inappropriate files created in May, June, and July 2021. Specifically, 72 pornographic videos, pictures of nude persons, and inappropriate animated drawings were created after April 2021. The review identified no additional files that were created on the 2017 laptop after July 7, 2021, implying that the subject used his 2017 laptop exclusively for inappropriate and unofficial purposes after he received his 2021 laptop.

The investigation found that the subject's conduct violated 5 CFR § 2635.101(9), which provides, "Employees shall protect and conserve Federal property and shall not use it for other than authorized activities," by using his government-issued laptops to view and/or transfer inappropriate material from his personal cell phone to a flash drive. The OIG found the subject

also violated agency polices that prohibit the use of agency information resources to access sexually explicit material.

In addition, OIG investigators identified evidence of sexually explicit images that were potentially unlawful. Accordingly, the OIG referred the matter to external law enforcement agencies for possible criminal charges. In addition, during the OIG investigation, the agency took prompt action to remove the subject's access to FEC information systems and the subject resigned on or about June 30, 2022.

The OIG withheld case closure and summary publication at the request of external law enforcement personnel pending criminal investigation. On December 11, 2023, external law enforcement reported to the OIG that the criminal case was closed due to insufficient evidence.

The results of the OIG investigation were provided to the agency for such action as may be appropriate. The OIG also made two recommendations 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 OCIO should conduct a cost-benefit analysis of the feasibility of conducting routine scans of FEC equipment to detect inappropriate material on government-issued devices.