

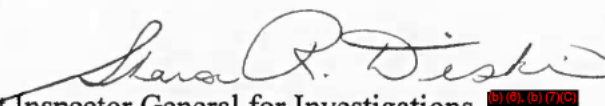


UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL



MEMORANDUM

DATE: January 29, 2020

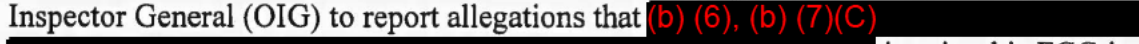
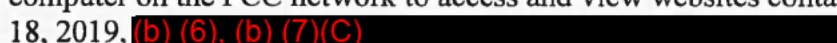
TO: David L. Hunt, Inspector General

THROUGH: Sharon R. Diskin, Assistant Inspector General for Investigations, 
, (b) (6), (b) (7)(C) 

FROM: (b) (6), (b) (7)(C), (b) (6), (b) (7)(C) Investigator

SUBJECT: (b) (6), (b) (7)(C)

Overview

On October 17, 2019, Tom GREEN, Chief Human Capital Officer within the Federal Communications Commission (FCC) Office of Managing Director, contacted the FCC Office of Inspector General (OIG) to report allegations that (b) (6), (b) (7)(C)  is using his FCC-issued computer on the FCC network to access and view websites containing pornography. On October 18, 2019, (b) (6), (b) (7)(C)  the Network Security Operations Team (NSOC), provided activity logs associated with (b) (6), (b) (7)(C)'s FCC-issued computer that appeared to show (b) (6), (b) (7)(C)'s FCC-issued computer accessing websites containing pornography. Based on the allegations, OIG initiated an investigation of (b) (6), (b) (7)(C). Specifically, OIG investigated allegations that (b) (6), (b) (7)(C) used an FCC-issued computer on the FCC network to access and view pornography.

Case Number:
OIG-I-20-0001

Case Title:
(b) (6), (b) (7)(C)

REPORT OF INVESTIGATION (continuation sheet)

Investigation

To investigate this matter, OIG performed the following steps:

1. Obtained and reviewed FCC Computer System User Rules of Behavior forms signed by (b) (6), (b) (7)(C) on (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C). Obtained and reviewed Cyber Security Awareness Training (CSAT) certificate awarded to (b) (6), (b) (7)(C) on (b) (6), (b) (7)(C). Users are required to acknowledge and agree to FCC Rules of Behavior to complete CSAT training and receive a certificate indicating the completion of training.
2. Obtained and reviewed FCC headquarters cardkey access records for (b) (6), (b) (7)(C).
3. Obtained and performed a forensic examination of (b) (6), (b) (7)(C)'s FCC-issued computer. (b) (6), (b) (7)(C) uses a Virtual Desktop Infrastructure (VDI) Virtual Machine (VM).
4. Obtained and performed a forensic examination of (b) (6), (b) (7)(C)'s Outlook mailbox ((b) (6), (b) (7)(C)@fcc.gov).
5. Obtained and performed a forensic examination of (b) (6), (b) (7)(C)'s Office 365 archived e-mail.
6. Obtained and performed a forensic examination of (b) (6), (b) (7)(C)'s network share (N:\ drive).
7. Obtained and performed forensic examinations of memory extracted by NSOC staff from (b) (6), (b) (7)(C)'s FCC-issued computer (VDI Virtual Machine) on November 5, 2019, November 7, 2019, November 15, 2019, November 18, 2019, and November 19, 2018.
8. Obtained and reviewed pagefile.sys files (virtual memory) extracted by NSOC staff from (b) (6), (b) (7)(C)'s FCC-issued computer (VDI Virtual Machine) on November 12, 2019, November 15, 2019, and November 18, 2019.

Conclusion

The forensic examination of digital evidence identified several artifacts indicating that (b) (6), (b) (7)(C) used his FCC-issued computer (VDI Virtual Machine) to access websites containing pornographic material. For example, the OIG (b) (6), (b) (7)(C) investigator identified two (2)

Case Number: OIG-I-20-0001	Case Title: (b) (6), (b) (7)(C)
-------------------------------	------------------------------------

REPORT OF INVESTIGATION (continuation sheet)

unique google searches that return pornographic images. The google search “teen footworship gifs” was identified six (6) times and the google search “(b) (6), (b) (7)(C)” was identified three (3) times. In addition, the OIG (b) (6), (b) (7)(C) investigator was able to identify numerous Uniform Resource Locators¹ (or “URLs”) for websites containing pornography from memory extracted from (b) (6), (b) (7)(C)’s FCC-issued computer (VDI Virtual Machine). Further, the OIG (b) (6), (b) (7)(C) investigator identified a single partial image that carved from memory that appears to be pornographic.

During the course of our investigation, NSOC management expressed concern that (b) (6), (b) (7)(C)’s activity was continuing and that the activity was compromising network security since websites containing pornography are often known to contain malicious code or “malware” (e.g., viruses, spyware, ransomware, etc.). As a result, (b) (6), (b) (7)(C) management met with (b) (6), (b) (7)(C) on December 11, 2019 and advised him of the on-going investigation. FCC OIG was subsequently advised by NSOC staff that there was no reported inappropriate activity after (b) (6), (b) (7)(C)’s meeting with (b) (6), (b) (7)(C) management.

On (b) (6), (b) (7)(C), we received an email message from the (b) (6), (b) (7)(C) announcing (b) (6), (b) (7)(C)’s retirement and farewell celebration scheduled for (b) (6), (b) (7)(C).

Recommendations

Based on the announcement of (b) (6), (b) (7)(C)’s retirement, we would recommend no further investigation into this issue at this time.

¹ A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

Case Number: OIG-I-20-0001	Case Title: (b) (6), (b) (7)(C)
-------------------------------	------------------------------------