UNITED STATES GOVERNMENT
FEDERAL COMMUNCIATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 4, 2013

TO: [redacted], [redacted]

CC: [redacted], [redacted]

FROM: [redacted]

SUBJECT: [redacted]

Overview

As a result of an [redacted] "sweep" of FCC computers, an FCC contract employee, [redacted] computer was noted as having inappropriate material, including pornography as well as unauthorized programs running on his machine. Subsequently the [redacted] team also conducted a remote imaging of [redacted] computer using [redacted]. The "sweep" results as well as a copy of the image results were turned over to the Office of Inspector General, Investigations Group. OIG conducted a computer forensic examination and an interview with [redacted].

Our investigation confirmed the existence of pornography on [redacted] computer. It also identified concerns with the lack of guidelines regarding the installation of software and the provision of administrative rights on Commission computers.

Case Number:	Case Title:
OIG-I-13-0009	[redacted]

Findings

[redacted] is employed as a contractor to the FCC through [redacted] and works as an [redacted] He has worked at the FCC for approximately [redacted] years.

[redacted] admitted to having unauthorized DVD converter software, Firefox and iTunes as well as some personal folders for some of his school material on his computer. [redacted] explained that a number of years ago he had been given administrative user rights to access a FCC financial system as part of his job. [redacted] admitted he used this administrative authorization to download the Firefox and iTunes program. [redacted] further stated the DVD converter software was added in early January 2013, but that, because he no longer had administrative rights and was thus unable to load the software, a friend of his, [redacted], a federal employee working in the IT office who has administrative rights, downloaded the converter software at his request. [redacted] intended to remove the converter software after he finished copying a music DVD, but could provide no specific date as to when he was going to remove the program. [redacted] said he had iTunes on his computer to listen to music. He said that "other people have iTunes" and that he "didn't think it was a problem (having iTunes) since it worked." In addition, [redacted] admitted to burning music CDs from his FCC computer, but he did not use Commission CDs in doing so.

[redacted] was then asked if he had any pornography on his computer and he responded "no, there definitely shouldn't be any of that." [redacted] admitted having "model shots" that would include pictures of women in bikinis or lingerie, but he ([redacted]) did not think those pictures constituted pornography. [redacted] received these "model shots" from buddies that were on an email chain and such pictures were sent around on a periodic basis. When asked to explain how investigators found pornography on his computer, [redacted] admitted that there "might be" some pornography videos on his system. A "buddy" of his may have put some videos on his [redacted]'s) iPod and when [redacted] plugged his iPod into his computer it may have synced the videos. [redacted] indicated there may have been four such videos on his computer. [redacted] was told that the number four did not correspond to the number of videos found during the forensic analysis of his computer. [redacted] then said that the number may be closer to "10 or 15." When it was explained to [redacted] that a total of 89 pornographic videos were found on his computer, [redacted] responded that he had used 3 or 4 iPods over the last few years, so 89 videos may be an accurate number. [redacted] stated he does not view the videos while at work nor share them with anyone at work and thinks they may have been synced to his computer 2 or 3 years

ago. [redacted] stated he last accessed the videos and/or knew about the videos "when they were first synced up." When confronted with the fact that the computer forensic examination showed that the video files were moved to his iTunes library on August 23, 2011 and October 7, 2011. [redacted] admitted he realized they were on his system and he was trying to remove them in August and October, 2011. However the forensic examination also showed that [redacted] had NOT viewed the video's since he moved them in August and October 2011.

In an interview with [redacted] on February 13, 2013 he provided the following information.

The majority of [redacted] s job dutie [redacted] here is no formal protocol involved in having non-standard software or hardware installed. Individuals may contact the help desk or [redacted] directly and make a request to have something installed. [redacted]

[redacted] had been through the cyber security training but has not received any additional guidance about which programs or hardware to install. The contractors had been through the same training but "they have been directed to not say no to any customer." If he said no to an installation, but a user then went to a contractor with the same request, the contractor shouldn't install the program. Contractors are "told not to say no, but they're not idiots." In addition, most of the requests he gets are from employees wanting to listen to music from their machine with which he does not have a problem, so he will help them out.

Without being asked, [redacted] volunteered that he recently installed the DVD converter program on [redacted] computer. He installed the DVD converter program on [redacted] computer to allow [redacted] to copy a music CD/DVD that was not playing properly. [redacted] claims he has not installed DVD converter software on any other FCC computer.

Case Number: OIG-I-13-0009	Case Title: [redacted]

[redacted] did not know why some people would say that iTunes wasn't allowed on some computer while others said it was. "I think iTunes is part of the standard FCC computer image so it should be there." He was asked if he's getting requests for tax or legal software and he responded "we don't have a need for that so we don't install it." [redacted] did not indicate there was a log to record what software was requested.

Conclusion

Based on the computer forensic examination findings and the admissions by [redacted] that he does have unauthorized programs on his FCC network computer as well as pornographic videos it is clear that [redacted] has violated the FCC Cyber Security Policy[1].

Recommendations

Based on our findings, we would recommend referring the case back to the [redacted] for disciplinary action as deemed appropriate and to the [redacted] to address the [redacted] issues as well as the OIG audit team for evaluation for a possible future audit. When addressing the cyber security issues [redacted] should consider determining what programs are acceptable and developing an approved list of software and hardware allowable on FCC network computers. Further the [redacted] should consider specific training for all [redacted] employees who have decisional authority regarding the downloading of programs or addition of hardware.

[1] FCC Cyber Security Program, Cyber Security Policy July 11, 2011

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: October 17, 2013

TO: [redacted]

CC: [redacted]

FROM: [redacted]

SUBJECT: FCC Employee [redacted], Prohibited Use of Government Equipment and Time and Attendance Issues

---

Background of Investigation

On March 21, 2013, FCC OIG initiated a proactive investigation of child pornography on the FCC Network (FCC OIG Case # [redacted]. To conduct the investigation, FCC Investigators provided a comprehensive listing of child pornography keywords to contractors from the [redacted] The contractors used the child pornography keywords to search for contraband on the network. On April 11, 2013, FCC Investigators were advised by contractor personnel assigned to the project that the keyword search had identified Internet Browser Favorites believed to be associated with child pornography on a computer workstation ([redacted]) assigned to [redacted] in the [redacted] The browser favorites included "youngamateurs", "Young Porn", and "Topless 16." On April 12, 2013, during an examination of access control badge data, FCC Investigator [redacted] identified a pattern of access that appears to indicate

indicate that [redacted] may be committing time and attendance fraud. As a result of this information an investigation was opened covering the computer misuse/potential child pornography issue as well as time and attendance fraud.

Scope of Investigation

FCC OIG staff conducted interviews and reviewed and analyzed relevant materials as detailed below.

Interviews

- [redacted] (Attachment #5)
- [redacted] (Attachment #6)
- [redacted] (Attachment #7)

Reports/Equipment Reviewed

- Forensic examination of [redacted]'s FCC-issued computer (Attachment #1 Media Analysis Report)

Findings: Prohibited Use of Government Equipment (Desktop Computer)

FCC Directive FCCINST 1479.4, FCC Cyber Security Program, effective May 1, 2011

Subparagraph 7.12 of FCCINST 1479.4 provides that users must:

- Read, sign indicating acceptance of, and comply with the FCC Computer System User Rules of Behavior;
- Use FCC information system resources only for authorized FCC business purposes, except as provided by the FCC's limited personal use policy;

FCC Cybersecurity Policy v3.1
Office of the Managing Director (OMD)
Effective Date: July 31, 2012

Paragraph 2.0.2 Broad Organizational Policies of FCC Cybersecurity Policy provides: Staff using FCC information systems or accounts must not participate in unethical, illegal or inappropriate activities such as: for-profit commercial activities, pirating software, stealing passwords, stealing credit card numbers, and

viewing/exchanging inappropriate written or graphic material (e.g., pornography).

Paragraph 2.11 Internet Usage of FCC Cybersecurity Policy provides that unacceptable uses of the Internet when using an FCC internet connection or account include:
• You must not use the Internet to view or download pornography.

FCC Computer System User Rules of Behavior
Form A-201
Revised January 2006
(See Attachment #2 Rules of Behavior (ROB) signed by [redacted] 2/5/07)

FCC Computer System User Rules of Behavior provides:

POLICY FOR USE OF COMPUTER RESOURCES.
As an employee or contractor of the Federal Communications Commission (FCC), you are required to be aware of, and comply with the FCC's policy on usage and security of computer resources, per OMB Circular A-130, Appendix III. Use of this system is for FCC authorized purposes only. Any other use may be misuse of Government property in violation of Federal regulations. All information in this system is subject to access by authorized FCC personnel at any time. Individual users have no privacy interest in such information.

[redacted], identified eleven (11) image files depicting pornographic material on [redacted]s FCC-issued computer. Nine (9) of the eleven (11) images were of a young woman undressing another young woman. Because of the young age of the young women appearing in this series of images, [redacted]

[redacted] also identified a series of Microsoft Office documents that appear to be Craigslist posts including posts that describe sexual activity in graphic terms and other documents that appear to be fantasy stories involving an individual named "[redacted]" and describing sexual activity in graphic terms. Further, [redacted]

[1] [redacted]

investigator found documents that contain email exchanges between a person named "[redacted]" and women with whom "[redacted]" appears to be discussing sex for money. Lastly, the [redacted] discovered a large number of Internet "bookmarks" for websites that appear to contain pornography including several websites that may contain child pornography. The [redacted] did not find any evidence that [redacted] used the FCC network to access/obtain the pornographic material or to access Craigslist. Neither did the [redacted] find evidence that [redacted] was using the FCC network to distribute pornographic material. However, given the age of the material that was identified and given that the operating system on [redacted]s FCC issued computer has been upgraded since the material was obtained, it is possible that the FCC network was used to obtain the material and that the artifacts identifying that activity are no longer in the computer.

In an interview, [redacted] admitted using his FCC issued desktop for "other than official government work," including accessing personal email, searching "music stuff," and visiting adult sites. With regards to "adult sites," [redacted] admitted to visiting the sites frequently "depending on what's going on" and "how busy I am." In the last 2-3 months, he does not think he has visited any adult sites "because I've been busy." Prior to this time, "when things were slow" [redacted] would visit adult sites "about 8 hours or more a week." [redacted] offered that "people would say 'have you seen this site'" and send him an email with a link to the site. "If it's (the site) is blocked I would not go any further." He said he does not attempt to circumvent FCC internet safeguards. [redacted] explained that there are about [redacted] in [redacted] who are exchanging such links, but he would not provide their names. He is sent links about once a week. [redacted] also goes to sites that he researches or finds "interesting." Some of the prohibited sites he visits are from "non-prohibited" websites like "the DMV of Virginia."

About 10 years ago, when [redacted], he saw an employee with adult videos and movies and asked how he did that. The employee said he "had someone help him set something up to get access to sites." [redacted] did not ask how or who could help him because "I thought it was wrong that he shouldn't be doing it." Also, [redacted] thought that the implication was that an [redacted] helped the employee set it up. He thought the individual might have been an [redacted] at the time, but he knows it wasn't a [redacted] since [redacted] at that time. Again, [redacted] would not provide the name of this person and would not confirm if this person was still employed at the FCC. [redacted] admitted to using his home computer to access adult sites about "an hour or two (hours) a week." Because his wife and children also use the computer, he has set up his home computer to automatically delete cookies when he logs out.

Case Number:	Case Title:
OIG-I-13-0024	[redacted]

[redacted] acknowledged that there is a banner when he logs onto his FCC issued computer that advised against "using the computer for personal stuff." In addition, he said that he "knew it was wrong" but continued to do it because "work was slow and I was interested in what other people and employees sent to me." He would also search for sites using Internet Explorer. He stated does not use Google Chrome or Mozilla/Firefox.[2] [redacted] was initially reluctant to acknowledge visiting the adult sites was wrong, but later in the interview agreed that it was against our (FCC) code of ethics and conduct, but that he was going to these sites out of boredom.

With regards to the bookmarks on his computer, [redacted] "did not think he bookmarked anything" or "only a small amount." He appeared shocked to learn of the number of sites that the forensic examine had uncovered. [redacted] thought he had "deleted everything." When asked why he found it necessary to delete cookies and browser items, [redacted] admitted he "knew it was wrong to go to these sites" and he was "concerned about things that were transmitted with these sites, like viruses." [redacted] reiterated "I do not bookmark anything at least not on purpose." When asked again, [redacted] said, "I might bookmark a couple things but I don't think so."

[redacted] stated that he "cannot think of any time" that he viewed pictures of children without clothes on, but has viewed pictures of children with clothes on. He asserted that the adult web sites he went to "had a waiver on the bottom, the one that says that the girls in the pictures are 18 and above."[3] [redacted] did affirm that the "girls were young looking." [redacted] reiterated he would click on links sent to him by other employees and said "I would guess there could be some under 18."

When first asked, [redacted] denied ever visiting Craigslist. When asked again, [redacted] admitted going to Craigslist to "buy stuff, like a crib." [redacted] specifically asked [redacted] if he had ever visited the adult section of Craigslist. Only at this time did [redacted] admit to "probably" going to the adult section "about 4 or 5 years ago." [redacted] continued "I may have gone to the site about a year ago just because it's there." He said he never chatted or emailed

---

[2] [redacted] We identified a significant amount of Mozilla Firefox activity during the period from 2/8/2013 and 4/19/2013 and a small amount of Google Chrome activity between the period from 2/1/2013 and 2/4/2013.

[3] 18 USC § 2257 - Record keeping requirements and 28 C.F.R. Part 75 CHILD PROTECTION RESTORATION AND PENALTIES ENHANCEMENT ACT OF 1990; PROTECT ACT; ADAM WALSH CHILD PROTECTION AND SAFETY ACT OF 2006; RECORDKEEPING AND RECORD-INSPECTION PROVISIONS

anyone. In addition, [redacted] claimed he never met up with anyone from the site. [redacted] specifically asked [redacted] "are you saying that you have never exchanged emails of a sexual nature with someone on Craigslist?" He responded, "it escapes my memory, but it sounds plausible." [redacted] asserted that "it was a funny gesture, an experiment, but I never chatted with anyone." He confirmed that he never used a chat program via Craigslist but "maybe I exchanged emails."

[redacted] does not use any external media (thumb drive, external hard drive) to transfer documents or spreadsheets between his work computer and his home computer. At first, he said that he only emailed documents to himself, but later admitted to burning spreadsheets to CDs and transporting those back and forth.

Findings: Time and Attendance Issues

5 USC § 6101 - Basic 40-hour workweek; work schedules; regulations

(a) (1) For the purpose of this subsection, "employee" includes an employee of the government of the District of Columbia and an employee whose pay is fixed and adjusted from time to time under section 5343 or 5349 of this title, or by a wage board or similar administrative authority serving the same purpose, but does not include an employee or individual excluded from the definition of employee in section 5541 (2) of this title, except as specifically provided under this paragraph.
(3) Except when the head of an Executive agency, a military department, or of the government of the District of Columbia determines that his organization would be seriously handicapped in carrying out its functions or that costs would be substantially increased, he shall provide, with respect to each employee in his organization, that—

(A) assignments to tours of duty are scheduled in advance over periods of not less than 1 week;
(B) the basic 40-hour workweek is scheduled on 5 days, Monday through Friday when possible, and the 2 days outside the basic workweek are consecutive;
(C) the working hours in each day in the basic workweek are the same;
(D) the basic nonovertime workday may not exceed 8 hours;
(E) the occurrence of holidays may not affect the designation of the basic workweek; and
(F) breaks in working hours of more than 1 hour may not be scheduled in a basic workday.

5 USC Chapter 63, Subchapter I – Annual and Sick Leave

5 USC § 6302 - General provisions

(a) The days of leave provided by this subchapter are days on which an employee would otherwise work and receive pay and are exclusive of holidays and nonworkdays established by Federal statute, Executive order, or administrative order.

According to the Federal Communications Commission's Employee Handbook, page 16, "Tours of duty will be established by the supervisor to cover an eight and one-half hour period, including lunch, and will begin between 7:00 a.m. and 10:00 a.m. and end between 3:30 p.m. and 6:30 p.m."

[redacted] admitted to teleworking but does not recall signing anything to formalize his telework arrangement. (Attachment #4 Telework Agreement for [redacted]) He teleworks approximately one day a week and usually works on spreadsheets.

[redacted]'s tour of duty is from 8am until 4:30pm. However, he often shows up at 8:30 or 9:00am and "works through lunch" to make up the hours. [redacted] said, "[redacted] "rarely gets in at 8:00" and arrives "more likely at 10:00 or 10:30." Access Badge Data shows that [redacted] typically arrives between 9:30 and 11am (usually around 10/10:30 am). [redacted] said he will ask before taking leave or leaving early and then follow-up with putting the leave requests in WebTA. [redacted] said, [redacted] and [redacted] have allowed him to leave early, work times other than his tour of duty, or do work after hours at home." Additionally, [redacted] states that he only leaves early about 2 times or less a week.

When interviewed [redacted] said he expects employees to work their full tour of duty (8 hours) each day. [redacted] stated he would "absolutely not" let an employee cut corners and never authorized [redacted] to leave early, work times other than his tour of duty or do work after hours at home. [redacted] would "never ever do that."

According to [redacted], [redacted] have an "informal arrangement" that allows him to come in late and put in leave slips and/or work later to make up any time owed to the government. When interviewed, [redacted] admitted to not knowing when [redacted] actually arrives or departs but has a "gut feeling" and "suspects" that [redacted] may not be taking the full amount of leave he should be taking for the time he is not actually at work. [redacted] commented "I've thought to myself, he's putting in leave slips but is he putting in enough?" (Attachment

#3 Access control badge data analysis Spreadsheet) [redacted] approves [redacted]'s leave in WebTA, but does not verify that [redacted] is in the office during the hours he should be.

[redacted] was specifically asked why our review of his badge data versus his leave data would show 189 hour shortfall, (that he was out of the office for 189 hours for which leave was not approved) from February 4, 2013 through August 12, 2013. He appeared shocked and did not think that was possible. [redacted] stated that "I oftentimes work at home after hours and keep a mental report of the hours I work at home." In addition, he said "if I'm working at home, I don't charge it." [redacted] could not explain what "I don't charge it" means. He admitted that he may have some "delayed reporting," but he usually catches up with leave requests the next day or by the end of the time period. When he works at home "in my mind I'm off-setting my leave." He explained that, if he does work for a couple hours in the morning and then goes to the doctor, if he's worked the hours, he won't take leave. However, he keeps "a mind total" and "internal notes" of the extra hours he worked. He suggested that his calendar would have the notes about his hours but also offered "my calendar might not even be correct." [redacted] insisted that he works at home to cover any hours that he hasn't worked in the building and keeps it all "mentally."

Conclusions: Prohibited Use of FCC Owned Computer

Our investigation has established that [redacted] engaged in personal, extensive non-work related use of his FCC-issued computer in violation of FCC Directive 1479.4 and the FCC Cybersecurity Policy. [redacted] has admitted to visiting and viewing pornographic material and adult sites as well as possessing and writing inappropriate written graphic material.

Conclusions: Time and Attendance Issues

Based upon the access control system badge data and [redacted]'s admission that he has arrived later and left earlier then his official tour of duty hours, it is reasonable to conclude the [redacted] has not followed the time and attendance rules relative to his official tour of duty. Analysis of Access Badge Data and payroll records show 152 hours for which [redacted] was paid but was not in the building and was not on authorized leave." NOTE: Human Resources Payroll office could not produce the Time and Attendance Records for Pay Period (PP) 02 (1/27/13 – 2/9/13) and PP03 (2/10/13 – 2/23/13). As a result, we have not included data from these pay periods in the overall calculation.

Recommendations

OIG is referring this matter to [redacted] for review and action as they deem appropriate.

Attachments

Attachment #1 Media Analysis Report, 8/7/13 **(note: graphic images and language)**
Attachment #2 Rules of Behavior (ROB) signed by [redacted] 2/5/07
Attachment #3 Access control badge data analysis spreadsheet
Attachment #4 Telework Agreement for [redacted]
Attachment #5 Memorandum of Interview: [redacted]
Attachment #6 Memorandum of Interview: [redacted]
Attachment #7 Memorandum of Interview: [redacted]

NON-PUBLIC
FOR INTERNAL USE ONLY

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: October 22, 2013

TO: [redacted]

FROM: [redacted]

SUBJECT: [redacted]

Attached hereto, and forwarded with my approval, is a memorandum concluding the Office of Inspector General's inquiry into the above-captioned matter.

Attachment

pornography on a computer workstation (FCC Barcode P020985) assigned to [redacted] in the Consumer and Governmental Affairs Bureau (CGB).

On September 12, 2013, during an examination of access control badge data which shows that a target is present when a computer is used, FCC Investigator [redacted] identified a pattern of access that appears to indicate that [redacted] may be committing time and attendance fraud. As a result of this information an investigation was opened covering the potential child pornography issue as well as time and attendance fraud.

Scope of Investigation

FCC OIG staff conducted interviews and reviewed and analyzed relevant materials as detailed below.

Interviews

- [redacted] (Attachment #4)
- [redacted] (Attachment #5)

Reports/Equipment Reviewed

- Forensic examination of [redacted] FCC-issued computer (Attachment #1 Media Analysis Report)
- Access Control Badge Data Analysis Spreadsheet (Attachment #3)

Findings: Prohibited Use of Government Equipment (Desktop Computer)

1.FCC Directive FCCINST 1479.4, FCC Cyber Security Program, effective May 1, 2011

Subparagraph 7.12 of FCCINST 1479.4 provides that users must:

- Read, sign indicating acceptance of, and comply with the FCC Computer System User Rules of Behavior;
- Use FCC information system resources only for authorized FCC business purposes, except as provided by the FCC's limited personal use policy

2. FCC Cybersecurity Policy v3.1
Office of the Managing Director (OMD)

forensics investigator also found one (1) Adobe Acrobat document containing graphic descriptions of sexual activity and one (1) Microsoft Office document containing an inappropriate image. Further, the computer forensics investigator identified seven (7) video files depicting graphic violence. The computer forensics investigator determined that [redacted] used the FCC network to obtain some of the pornographic and inappropriate material.

In an interview, [redacted] admitted to using his FCC issued desktop for "other than official government work." [redacted] offered that he may have music on his computer, as well as pictures of videogames, cars, shoes, women in bikinis as well as "naked women, but nothing under 18 or 21." He admitted that he was getting these pictures from message boards or from Facebook pictures. These message boards also include topics related to sports and politics. He visits these message boards daily and thought he might have approximately 80 to 90 pornographic pictures. [redacted] informed [redacted] that during the computer forensic examination, 248 pornographic pictures and 22 pornographic videos were found. After additional questioning [redacted] ultimately admitted to downloading pictures and knowing that he had pornographic videos on his Commission-issued computer.

[redacted] stated he is not passing pictures to FCC or other federal employees via his FCC.GOV email address, nor does he share articles he finds on the message boards via his FCC.GOV email address or visit adult web sites. [redacted] admitted to using his FCC computer to transfer pictures from his phone to a Zip or thumb drive, and saved pornographic pictures and videos to his C:\ drive on his computer.

[redacted] offered that during the forensic examination, 7 videos of violence were found. [redacted] stated that he hasn't viewed it in a long time, "maybe 3,4, 5 years ago." He admitted to finding these photos on YouTube or WorldStar. He stated "I'm not searching for it."

Findings: Suspected Marijuana Use

1.Executive Order 12564 of September 15, 1986 Drug-Free Federal Workplace
Section 1 provides that:
(a) Federal employees are required to refrain from the use of illegal drugs.
(b) The use of illegal drugs by Federal employees, whether on duty or off duty, is contrary to the efficiency of the service.
(c) Persons who use illegal drugs are not suitable for Federal employment.

(A) assignments to tours of duty are scheduled in advance over periods of not less than 1 week;
(B) the basic 40-hour workweek is scheduled on 5 days, Monday through Friday when possible, and the 2 days outside the basic workweek are consecutive;
(C) the working hours in each day in the basic workweek are the same;
(D) the basic nonovertime workday may not exceed 8 hours;
(E) the occurrence of holidays may not affect the designation of the basic workweek; and
(F) breaks in working hours of more than 1 hour may not be scheduled in a basic workday.

2. 5 USC Chapter 63, Subchapter I – Annual and Sick Leave

5 USC § 6302 - General provisions
(a) The days of leave provided by this subchapter are days on which an employee would otherwise work and receive pay and are exclusive of holidays and nonworkdays established by Federal statute, Executive order, or administrative order.

According to the Federal Communications Commission's Employee Handbook, page 16, "Tours of duty will be established by the supervisor to cover an eight and one-half hour period, including lunch, and will begin between 7:00 a.m. and 10:00 a.m. and end between 3:30 p.m. and 6:30 p.m."

[redacted] tour of duty is from 8am until 4:30pm. He does not telework or work a compressed work schedule. [redacted] admitted that he "usually gets in the office around 8-8:30 and leaves around 3:45-4:00pm." [redacted] stated that "[redacted] okays me coming in 5 -10 minutes late, and he [redacted] is okay if I have to leave early." He stated that if he is missing more than 2 hours of work, he would put in a leave slip, but for 30 minutes to an hour he does not.

[redacted] R informed [redacted] S's that his badge access data from July 12, 2013 to September 11, 2013 shows that he is short by 55 hours. [redacted] stated that 4 -5 months ago he had to "duck out early" for some personal things. When [redacted] explained the time period reviewed covered two months, not just a few days in which he may have left early, [redacted] offered that [redacted] begs me to take leave." [redacted] also stated that "I have the leave to cover the hours, just take it." [redacted] showed [redacted] the spreadsheet and asked if he had any

[4] [redacted]

Attachment #1 Media Analysis Report dated 9/6/2013**(note: graphic images and language)**
Attachment #2 Rules of Behavior (ROB) signed by [redacted] 1/5/07
Attachment #3 Access control badge data analysis spreadsheet
Attachment #4 Memorandum of Interview: [redacted]
Attachment #5 Memorandum of Interview: [redacted]

Case Number:	Case Title:
OIG-I-13-0041	[redacted]

NON-PUBLIC
FOR INTERNAL USE ONLY

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 26, 2014

TO: [redacted]

FROM: [redacted]

SUBJECT: [redacted]

Attached hereto, and forwarded with my approval, is a memorandum concluding the Office of Inspector General's inquiry into the above-captioned matter.

Attachment

UNITED STATES GOVERNMENT
FEDERAL COMMUNCIATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 26, 2014

TO: [redacted]

CC: [redacted]

FROM: [redacted]

SUBJECT: [redacted]

Overview

On March 12, 2014, [redacted], contacted the [redacted] and reported possible computer misuse (pornography) by one of his employees. On March 15, 2014, the [redacted] contacted [redacted] to obtain additional information related to the allegations. [redacted] suggested contacting [redacted], the direct supervisor for the person suspected of computer misuse. On March 18, 2014, the [redacted] spoke with [redacted] about the allegations. [redacted] provided an overview of the [redacted] operated at [redacted]'s facility in [redacted] explained that, because of the unique nature of the work being performed, the workstations used in the [redacted] facility are not built on the standard FCC baseline image. [redacted] further explained that [redacted] employees use a shared account on a shared workstation to access the FCC network for Internet access and to check Outlook email.

Case Number:	Case Title:
OIG-I-14-0018	[redacted]

shared workstation to access the FCC network for Internet access and to check Outlook email. Lastly, [redacted] explained that the employee suspected of computer misuse, [redacted], is a [redacted] and that the [redacted] 4. Based on the allegations, OIG initiated an investigation of [redacted]. Specifically, OIG investigated allegations that [redacted] used a shared FCC computer to view pornography.

Our investigation found evidence that [redacted] used an FCC computer to view pornographic material in violation of the Commission's directive and policies governing cyber security.

Investigation

To investigate this matter, OIG investigators performed the following steps:

1. Obtained and reviewed screenshots of Mozilla browser history purportedly from the HFDFADMIN2-HP workstation located in [redacted]'s facility in [redacted]. OIG received two (2) pages of browser history screenshots showing activity for the period from March 7, 2014 at 7:16 am EST through March 9, 2014 at 7:51 am EST.

2. Obtained and reviewed Blue Coat firewall log for the period 3/8/2014 between the hours of 7:00 am and 3:00 pm for client IP = 165.135.251.252 (HFDFADMIN2-HP workstation) and web application = "YouTube."

3. Obtained and reviewed event logs from the HFDFADMIN2-HP workstation for the period from 8/13/12 at 2:04 pm through 3/14/14 at 3:34 pm.

4. Obtained and reviewed the employee sign in log for the [redacted] for the March 2014 (log is erroneously marked "Mar 2012").

5. Obtained remote access to the HFDFADMIN2-HP workstation using [redacted] and performed a limited scope forensic examination of the workstation.

Finding: Prohibited Use of Government Equipment (Desktop Computer)

Our investigation found evidence that [redacted] used an FCC computer to view pornographic material in violation of the Commission's directive and policies governing cyber security.

FCC Directive FCCINST 1479.4, entitled "FCC Cyber Security Program" and effective May 1, 2011, establishes policy and assigns responsibilities for assuring optimal levels of protection required for FCC data and information systems. Section 7.12 of the directive, entitled "Authorized Network/Workstation System Users", states that Users must:

- Read, sign indicating acceptance of, and comply with the FCC Computer System User Rules of Behavior;
- Use FCC information system resources only for authorized FCC business purposes, except as provided by the FCC's limited personal use policy;
- Be aware of their responsibilities to comply with this directive;

The Commission's Cyber Security Policy, version 3.5 promulgated by the Office of the Managing Director and effective June 20, 2013, establishes the security policies, consistent with Federal regulations, mandates, and directives for the protection of FCC data and information systems using a risk-based approach. Section 2.0.2 of the Cyber Security Policy, entitled "Broad Organizational Policies", states the following:

- Staff must adhere to the security policies contained in FCCINST 1479.4, this policy document, and the FCC Computer System User Rules of Behavior (FCC Form A-201).
- Staff using FCC information systems or accounts must not participate in unethical, illegal or inappropriate activities such as: for-profit commercial activities, pirating software, stealing passwords, stealing credit card numbers, and viewing/exchanging inappropriate written or graphic material (e.g., pornography).

Section 2.8 of the Cyber Security Policy, entitled "Policy Violation and Disciplinary Action", states that "Cyber security-related violations are addressed in the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR Part 2635); FCC employees may be subject to criminal, civil, or disciplinary action for failure to comply with the FCC security policy."

Section 2.11 of the Cyber Security Policy, entitled "Internet Usage", states that "You must not use the Internet to view or download pornography."

FCC Form A-201, entitled "FCC Computer System User Rules of Behavior" revised in January 2006, states that "Use of all computer resources, including personal computers, laptops, all parts

of the FCC Network, communication lines, and computer facilities are restricted to FCC-authorized purposes only. A copy of FCC Form A-201 signed by [redacted] on April 8, 2013 is included as Attachment #1 to this Report of Investigation.

To investigate the allegation, the [redacted] obtained and examined log files from the [redacted] network, event logs from the HFDFADMIN2-HP workstation, Internet browser history screenshots from the HFDFADMIN2-HP workstation and employee sign in logs from the [redacted] facility. In addition, the [redacted] obtained remote access to the HFDFADMIN2-HP workstation and extracted and reviewed Mozilla Firefox browser artifacts.

The employee sign in log from the [redacted] facility in [redacted] shows that [redacted] and [redacted] were in the [redacted] facility during the day shift (7:00 am to 3:30 pm) on March 8, 2014 (the date of the alleged activity).

The Security Event Log for the HFDFADMIN2-HP workstation shows that the workstation was used to access the Outlook mailbox for the account [redacted] on March 8, 2014 at 7:00:01 am EST. The log also shows that no other Outlook mailboxes were accessed from the HFDFADMIN2-HP workstation on March 8, 2014. The Security Event Log for the HFDFADMIN1-HP workstation (the other workstation used by HFDF employees to access the Internet and Outlook) shows that the workstation was used to access the Outlook mailbox for account [redacted] on March 8, 2014 at 7:04:09 am EST. The [redacted] tigator did not find any evidence that [redacted] used the HFDFADMIN1-HP workstation to access his Outlook mailbox on March 8, 2014.

The browser history screenshots, Blue Coat log files, and Mozilla Firefox history file obtained from the HFDFADMIN2-HP workstation showed that the Mozilla Firefox browser on the HFDFADMIN2-HP workstation was used to access eighteen (18) webpages that appear to contain pornography based on the title of the webpage. To determine if the webpages contained pornographic material, the [redacted] used a workstation not connected to the FCC network to navigate to the webpages. For those webpages that the [redacted] was able to access[1], the [redacted] briefly previewed the video file and took screenshots showing video content. The detailed results of the examination of webpages including screenshots showing video content are included in the Appendix to this

[1] The [redacted] was not able to access all eighteen (18) of the video files that appear to contain pornographic material. Some of the video files were marked private and others had been removed from YouTube. Private video files can only be seen by the person uploading the file and those persons designated by the person uploading the file.

Report of Investigation.

In addition to showing access to webpages that appear to contain pornographic material, the browser history screenshots, Blue Coat log files, and Mozilla Firefox history file obtained from the HFDFADMIN2-HP workstation showed that the Mozilla Firefox browser on the HFDFADMIN2-HP workstation was used to access a Yahoo Mail account four (4) times on March 8, 2014[2]. The account name associated with the Yahoo Mail account is [redacted]. The [redacted] did not subpoena account information from Yahoo to determine conclusively that this Yahoo Mail account is associated with [redacted]. However, the Computer Forensics Investigator believes that this Yahoo Mail account is associated with [redacted] based on the account name.

Conclusion

Our investigation found evidence that [redacted] used an FCC computer to view pornographic material in violation of the Commission's directive and policies governing cyber security.

Recommendations

OIG is referring this matter to [redacted] and [redacted] for review and action as they deem appropriate.

Attachment

Attachment #1 FCC Computer System User Rules of Behavior signed by [redacted] on April 8, 2013

[2] The [redacted] Yahoo Email account was accessed at 07:07 hours, 09:34 hours, 11:47 hours, and 13:06 hours on March 8, 2014.