UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: October 28, 2014

TO: David L. Hunt, Inspector General

CC: [redacted], Deputy Inspector General

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Investigatory Attorney, [redacted], Investigator

SUBJECT: Investigation into Abuse of Power by FCC Regional Director

Background of Investigation

On December 30, 2013 a written statement was provided to the Office of Inspector General (OIG) in which [redacted] alleges that EB [redacted] Regional Director [redacted] 1) committed perjury and 2) made false statements in [redacted] written statements in ([redacted]), a complaint filed by [redacted] in March 2013 and is still pending before the EEO. [redacted] also alleges that [redacted]'s denial of a 2012 end-of-the-year performance award to [redacted] was in retaliation for his providing testimony in an earlier EEO complaint, [redacted], involving another [redacted] Region employee.

[1] Agent, Federal Communications Commission (FCC) Enforcement Bureau (EB), [redacted] District Office

Case Number:	Case Title:
OIG-1-14-0017	Allegations of Perjury and False Statement in EEO Proceedings by FCC Regional Director

OIG Investigators undertook this investigation to determine whether [redacted] abused [redacted] position as Regional Director by (1) making false statements in an EEO proceeding and/or (2) engaging in retaliation in denying [redacted] a performance award in 2012, the same year [redacted] was deposed in another employee's EEO case. We found no evidence of abuse of authority.

Scope Of Investigation

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

Interviews of

- [redacted], [redacted] Regional Director for the Enforcement Bureau (EB)
- [redacted], EEO Investigator at First Tech hired by the FCC to conduct the Investigation and Interviews of [redacted] v Federal Communications Commission FCC Case Number [redacted]

Background

[redacted] has been the [redacted] Regional Director for the Enforcement Bureau (EB) since January 2003. [redacted] oversees eight offices in the [redacted] Region of the United States including [redacted] directly reports to [redacted], EB Deputy Bureau Chief. [redacted] started at the Commission in 1994 in the Cable Division, and has worked in the Office of General Counsel (OGC) and Office of Engineering Technology (OET).

[redacted] was deposed in the case of [redacted] (EEO Case [redacted]) on June 5, 2012. In March 2013, [redacted] filed an EEO complaint ([redacted]) ([redacted] Complaint) against [redacted] alleging that [redacted]'s decision to deny [redacted] a performance award for the 2012 rating period was in retaliation for [redacted] participation in the [redacted] case[2]

OIG Investigation

[2] [redacted] claims participating in an employment discrimination proceeding, even as a witness is a protected activity.

The OIG investigation focused on two questions concerning potential abuse of power that are essentially intertwined. First, did [redacted] give a false statement to the FCC's investigator in [redacted]'s EEO proceeding when [redacted] explained [redacted] rationale for denying [redacted] a performance award; (2) was [redacted] denial of [redacted]'s performance award in retaliation for [redacted] participation in the [redacted] case.

False Statement Relative to Performance Award

In furtherance of the [redacted] Complaint, [redacted] was interviewed by EEO Contract Investigator [redacted] on or about October 18, 2013. [redacted] explained that, to determine performance awards, [redacted]: (1) conferred with the [redacted] Region District Directors, Deputy Regional Director and Regional Counsel on preliminary recommendations for performance awards of [redacted] Region employees; (2) approved submitted supporting justifications and write-ups for employees in the [redacted] Region offices from recommending officials; (3), approved awards for [redacted] Region employees as the approving official and; (4) submitted the [redacted] Region award paperwork to the Enforcement Bureau Front Office for approval and processing. In this case, the paperwork was submitted to EB's Front Office on July 31, 2012.[3]

Specifically, [redacted] told [redacted] that [redacted], [redacted], consulted with [redacted], [redacted] Region Counsel who, during the 2012 performance period had worked closely with [redacted] and Sr. Agent [redacted] on [redacted] office cases. As part of [redacted] review of every sanction proposed by the [redacted] agents, [redacted] reviewed the Enforcement Bureau Activity Tracking System (EBATS) for sufficiency and completeness of evidence supporting the sanction. (EBATS is the database that stores factual entries, inspection/investigative files and evidence for every case handled within the office). [redacted] did not consult with Acting District Director [redacted], as [redacted] had just been named Acting District Director several days before the award allocations were distributed to the Regions.

According to [redacted] statement in the [redacted] Complaint proceeding, [redacted] and [redacted] discussed and reviewed the criteria, data, analysis and justifications for awards for the [redacted] Office staff. [redacted] also stated that [redacted] discussed and explained the basis and justification for [redacted] receiving no award with [redacted] supervisors.[4]

[3] Page 3, [redacted] Testimony
[4] Page 7, [redacted] Testimony

Case Number:	Case Title:
OIG-I-14-0017	Allegations of Perjury and False Statement in EEO Proceedings by FCC Regional Director

In the [redacted] Complaint proceeding, [redacted] explained that [redacted] did not receive a performance award in 2012 because [redacted] did not meet the criteria. [redacted] stated that [redacted] performance did not improve the efficiency, effectiveness, or economy of the FCC; [redacted] performance was not beyond normal duties, and [redacted] did nothing special or significant warranting recognition.[5] In addition, [redacted] stated that [redacted]'s performance of [redacted] duties and responsibilities was not what was expected of a GS-13 with [redacted]'s level of experience; [redacted] neglected to follow established guidelines and protocols; [redacted] made errors in researching background information, documenting case evidence, and drafting sanctions; and [redacted] had difficulty following instructions.

In [redacted] written response to the EEO investigator, [redacted], addressing a particular case assigned to [redacted], stated:

> [redacted] went out on the case about nine different times, attempting to find the signal, but failed. Because this was a critical infrastructure interference matter, the case had to be reassigned to the Sr. Agent who found the source of the interference [redacted] first time out.[6]

It is this statement that [redacted] alleges to be false.

OIG investigators reviewed the EBATS entries related to the statement in question. In an interview conducted by OIG investigators, [redacted] was specifically asked to clarify and explain the notations found in EBATS, which was supplied by [redacted] in [redacted] original complaint. As noted above, EBATS is a record keeping system in which Enforcement Bureau Agents log their efforts when working a case. During the [redacted] Complaint interview [redacted] stated [redacted] had to "send a senior agent on the case" in question to locate the source of a signal as [redacted] had been unable to do so over a several month period. [redacted] also stated that the senior agent located the source of the signal on the first try.

However, the EBATS history appears to show that the senior agent may have actually

[5] Page 10, [redacted] Testimony
[6] Page 10, [redacted] Testimony

Case Number:	Case Title:
OIG-I-14-0017	Allegations of Perjury and False Statement in EEO Proceedings by FCC Regional Director

gone out three times, as opposed to once as stated by [redacted] in the EEO interview. [7]

[redacted] explained to OIG's investigators that, on March 13, 2012, the senior agent, [redacted], and [redacted] did go out on the case in an attempt to track down the signal. On that same day the signal was tracked to a single block area. No further tracking was completed that day as the agents ran out of time. EBATS shows that [redacted] continued to work the case between March 26, 2012 and May 10, 2012 and visited the general area 9 (nine) times but was unable to locate the specific source of the signal. According to EBATS on May 4, 2012, [redacted] returned to the single block area originally identified and determined the source of the signal to a specific building. Access to all floors of the building was denied on that day for security reasons, but [redacted] and [redacted], another [redacted] Region EB employee, were told by building security that access could be granted in approximately one week. On May 15, 2012, [redacted] and [redacted] were granted access to the building by security and the specific source of the signal was located. [redacted] and [redacted] were able to locate the signal as soon as access was granted.

Review of the Enforcement Bureau Activity Tracking System (EBATS) for the [redacted] cellphone complaint ([redacted]) referenced by [redacted] and [redacted] indicates that [redacted] went out two (2) times to locate the interference instead of the one (1) time referenced by [redacted]. There is no dispute that [redacted] went out nine (9) times and was unable to locate the interference.

OIG investigators also interviewed [redacted]. The investigator stated that [redacted] did not see any material difference of facts and did not see a need to verify information through additional witnesses. [redacted] had no issue with [redacted]'s veracity in the EEO investigation which would cause the EEO investigator to search for additional evidence.

While in the first instance, it is within the jurisdiction of the EEOC to determine whether [redacted] made a false statement in the [redacted] complaint proceeding, we nevertheless conclude that [redacted]'s explanation of the EBATS notations of the number of visits by the senior agent versus [redacted] comments made to the EEO investigator were reasonable and justified. While the senior agent was physically on the site three times, the explanation by [redacted] of the events/timeline gives credibility to [redacted] response and no falsehood should be associated with [redacted] response.

[7] It is this statement that [redacted] alleges to be false/perjury.

Case Number:	Case Title:
OIG-I-14-0017	Allegations of Perjury and False Statement in EEO Proceedings by FCC Regional Director

Retaliation

In [redacted] interview, [redacted] told OIG investigators that [redacted] had no knowledge of the substance of [redacted]'s deposition in the [redacted] case. Moreover, [redacted] provided OIG no evidence tying [redacted] denial of a performance award to [redacted] participation in the [redacted] case. Rather, [redacted] is, in effect, requesting us to conclude that, because [redacted]'s justification for the award denial included a statement that [redacted] alleges is false, the denial was unjustified, and ergo, was based on retaliation.

We cannot make such a leap. First, as stated above, we conclude that [redacted]'s statement to the EEO investigator was reasonable and justified. Regardless, even if [redacted] statement had been false, [redacted] adequately explained that the reason for not giving [redacted] a performance award was specifically based on the fact that [redacted] did not perform at a level justifying and award and was unable to perform the job based on the standard of the GS13 (not merely on the singular incident upon which the alleged false statement focusses).

Recommendation

Because we found no merit to the allegations presented by [redacted] it is recommended that this case be closed out without further investigation.

UNITED STATES GOVERNMENT
FEDERAL COMMUNCIATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: September 15, 2014

TO: David L. Hunt, Inspector General, Federal Communications Commission

CC: [redacted], Deputy Inspector General, Federal Communications Commission

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Investigator, [redacted], Computer Forensics Investigator

SUBJECT: [redacted]

Background

The Office of Inspector General had received information that [redacted] ([redacted]) an employee in CGB may have been selling items while on official duty hours and that some of the items may have been counterfeit. [redacted] was interviewed by OIG investigators who also conducted a forensic examination of [redacted] computer.

Findings:

The forensic examination found no evidence that [redacted] was engaged in selling any type of merchandise. During the interview, [redacted] was directly asked if [redacted] sells items while at work. [redacted] responded by saying that [redacted] had sold things but that it has been "at least a year" since

Case Number:	Case Title:
OIG-I-14-0011	[redacted]

[redacted] last sold anything. [redacted] explained that [redacted] has sold gloves, hats, candy, wrapping paper and cakes as part of fund raising efforts for a "steppers group" [redacted] and [redacted] sister are involved with, as well as for [redacted] church and for [redacted] nephew's school fund -raising efforts. When asked to quantify the times [redacted] has sold items, [redacted] stated "a million times" over [redacted] forty year career.

[redacted] did not solicit sales throughout the Commission, but would only approach [redacted] friends/coworkers who [redacted] thought may be interested in the products. According to [redacted], none of [redacted] sales were for profit at any time, and [redacted] sales efforts were conducted only during [redacted] lunch period. The merchandise was obtained through various fund raising vendors. [redacted] stated that [redacted] has accepted cash and checks and that the amounts were never over $10.

[redacted] denied ever having sold knock-off/bootlegged/counterfeit items. [redacted] further denied attempting to sell, or selling DVDs or CDs. [redacted] indicated [redacted] was a board member of the FCC Recreation Association (FCCRA) for many years, but was not involved with selecting vendors and claims no association with any of the vendors at any time.

FCC OIG has received allegations that vendors associated with the FCCRA sell counterfeit merchandise, and at least one such vendor has admitted this. Thus, [redacted] was provided a copy of a letter that the Immigration and Customs Enforcement agency provides to individuals regarding possession and/or sale of counterfeit merchandise.

Conclusion

Based on the forensic examination and responses to questions during the interview, we cannot find evidence to suggest that [redacted] is, or was involved in the selling of counterfeit/bootlegged merchandise. However, even though [redacted] admitted to selling fund-raising merchandise in the building, short of time consuming surveillance or evidence provided by employees who purchased goods from [redacted], there is no way to either rebut [redacted] claim that [redacted] engaged in this activity solely during her lunch hour, or whether what [redacted] exceeded acceptable limits of personal activity. We had only a vague allegation from the whistleblower and found no evidence to rebut [redacted]'s statements, and we are not inclined to engage in surveillance in this case.

Recommendations

Based on our findings, we recommend the investigation be closed without taking additional action. [redacted]

Case Number:	Case Title:
OIG-I-14-0011	[redacted]

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: September 16, 2014

TO: David L. Hunt, Inspector General

CC: [redacted], Deputy Inspector General

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Investigatory Attorney, [redacted], Investigator

SUBJECT: Gross Mismanagement And Gross Incompetence By [redacted]

Background of Investigation

On April 3, 2014, a Federal Communications Commission (FCC) employee (WHISTLEBLOWER) in the [redacted] office in the Enforcement Bureau (EB) filed a written complaint with the Office of Inspector General (OIG) alleging "[redacted] ([redacted]), my supervisor at the [redacted] Office is engaged in on-going gross mismanagement and / or abuse and / or waste." On April 7, 2014, WHISTLEBLOWER followed up with an additional email complaint stating, "I'd like to add that [redacted] is a GS-15 and has not and cannot write anything beyond a simple email. [redacted] has never written a technical or legal summary of any sort, cannot recommend a policy, cannot give coherent instructions verbally and much less in writing, and [redacted] cannot review enforcement actions."

Case Number:	Case Title:
OIG-I-14-0020	Gross Mismanagement And Gross Incompetence By [redacted]

Scope Of Investigation:

OIG reviewed the matter and determined the WHISTLEBLOWER's allegations concerned performance/management-related activities and thus more appropriately fell within the jurisdiction of the operating Bureau.in the first instance. On April 8, 2014, Assistant Inspector General for Investigations (AIGI) [redacted] referred the matter to [redacted], Deputy Chief, Enforcement Bureau for action. On July 9, 2014, [redacted] forwarded the matter to [redacted], EB's former Acting Chief of Staff, and [redacted], EB's new Chief of Staff.

Findings:

On July 14, 2014, EB concluded its review of the WHISTLEBLOWER's complaint and forwarded its report to the OIG. EB's findings indicate that there is a "larger, ongoing management conflict between WHISTLEBLOWER and [redacted]." EB management in [redacted] and in DC have been actively working to resolve this conflict.[1]

Conclusion:

OIG has reviewed EB's response and based on its evaluation, finds the allegations are unfounded and no additional action is warranted. EB management is aware of the situation between management and staff in the [redacted] office and is attempting to take proactive steps to mitigate and abate the situation to the satisfaction of the WHISTLEBLOWER, while supporting the mission of EB. Further steps and actions should be address by Labor Relations.

Recommendation:

It is recommended that this case be closed out without further investigation.

[1] Page 1, Enforcement Bureau Response to Office of Inspector General Concerning Grievance filed by Whistleblower

NON-PUBLIC
FOR INTERNAL USE ONLY

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 26, 2014

TO: [redacted], Bureau Chief Public Safety and Homeland Security Bureau, [redacted] Acting Chief Human Capital Officer

FROM: David L. Hunt, Inspector General

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: David L. Hunt, Inspector General

CC: [redacted], Deputy Inspector General

FROM: [redacted], Assistant Ins[redacted] Computer Forensics Investigator, [redacted],

SUBJECT: [redacted]

Overview

On March 12, 2014, [redacted], Chief of the Operations and Emergency Management Division within the Public Safety and Homeland Security Bureau (PSHSB), contacted the Assistant IG for Investigations and reported possible computer misuse (pornography) by one of his employees. On March 15, 2014, the OIG Computer Forensics Investigator 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 Computer Forensics Investigator spoke with [redacted] about the allegations. [redacted] provided an overview of the [redacted] systems operated at PSHSB's facility in [redacted]. [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 probationary employee and that the probationary period ends on April 7, 2014. 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 [redacted] workstation located in PSHSB'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 = [redacted] workstation) and web application = "YouTube."

3. Obtained and reviewed event logs from the [redacted] 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] Center for the March 2014 (log is erroneously marked "Mar 2012").

5. Obtained remote access to the [redacted] workstation using EnCase Enterprise 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 Computer Forensics Investigator obtained and examined log files from the PSHSB [redacted] network, event logs from the [redacted] workstation, Internet browser history screenshots from the [redacted] workstation and employee sign in logs from the [redacted] facility. In addition, the Computer Forensics Investigator obtained remote access to the [redacted] 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 [redacted] 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 [redacted] workstation on March 8, 2014. The Security Event Log for the [redacted] workstation (the other workstation used by [redacted] 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 Computer Forensics Investigator did not find any evidence that [redacted] used the [redacted] 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 [redacted] workstation showed that the Mozilla Firefox browser on the [redacted] 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 Computer Forensics Investigator used a workstation not connected to the FCC network to navigate to the webpages. For those webpages that the Computer Forensics Investigator was able to access[1], the Computer Forensics Investigator 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 Computer Forensics Investigator 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 [redacted] workstation showed that the Mozilla Firefox browser on the [redacted] workstation was used to access a Yahoo Mail account four (4) times on March 8, 2014 . The account name associated with the Yahoo Mail account is [redacted]. The Computer Forensics Investigator 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

[redacted].

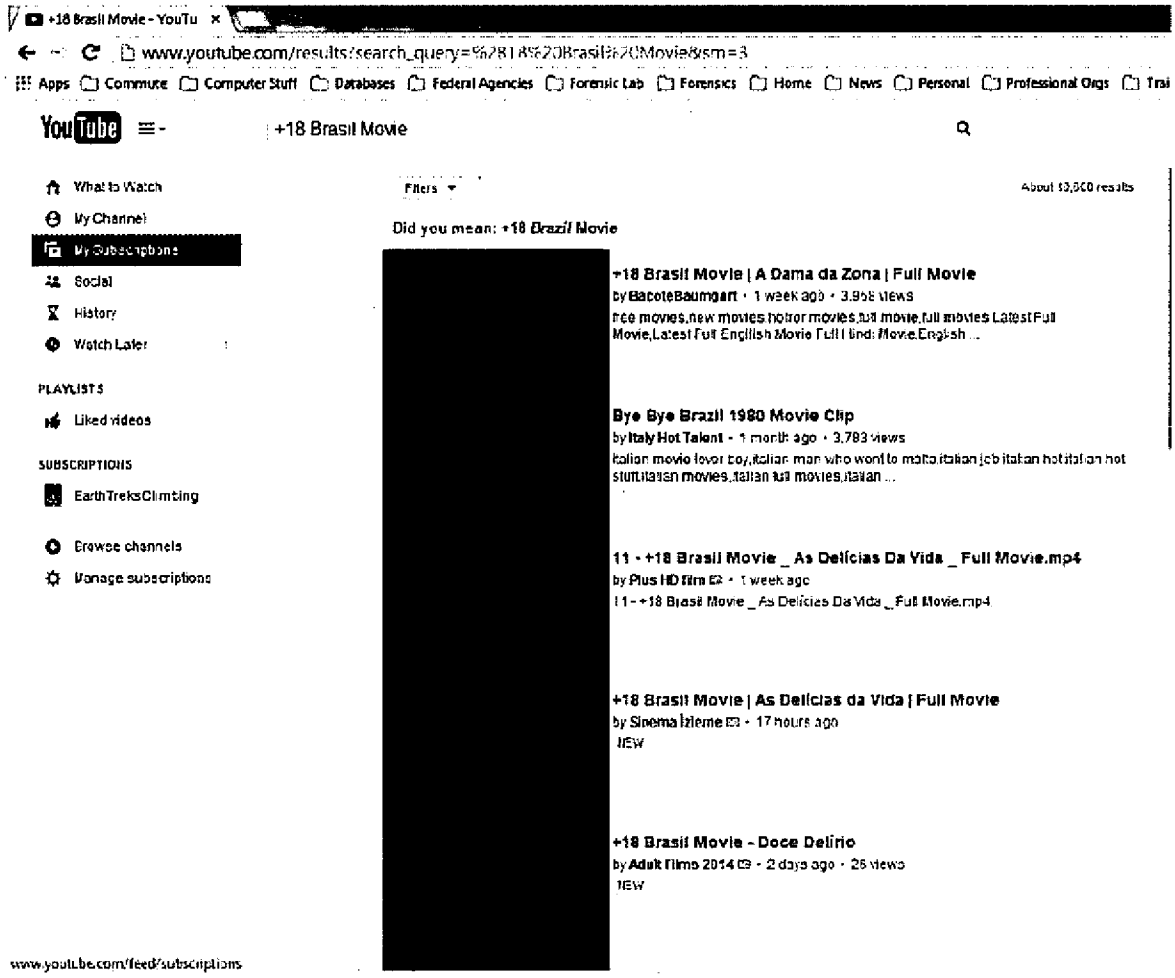
Attachment

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.

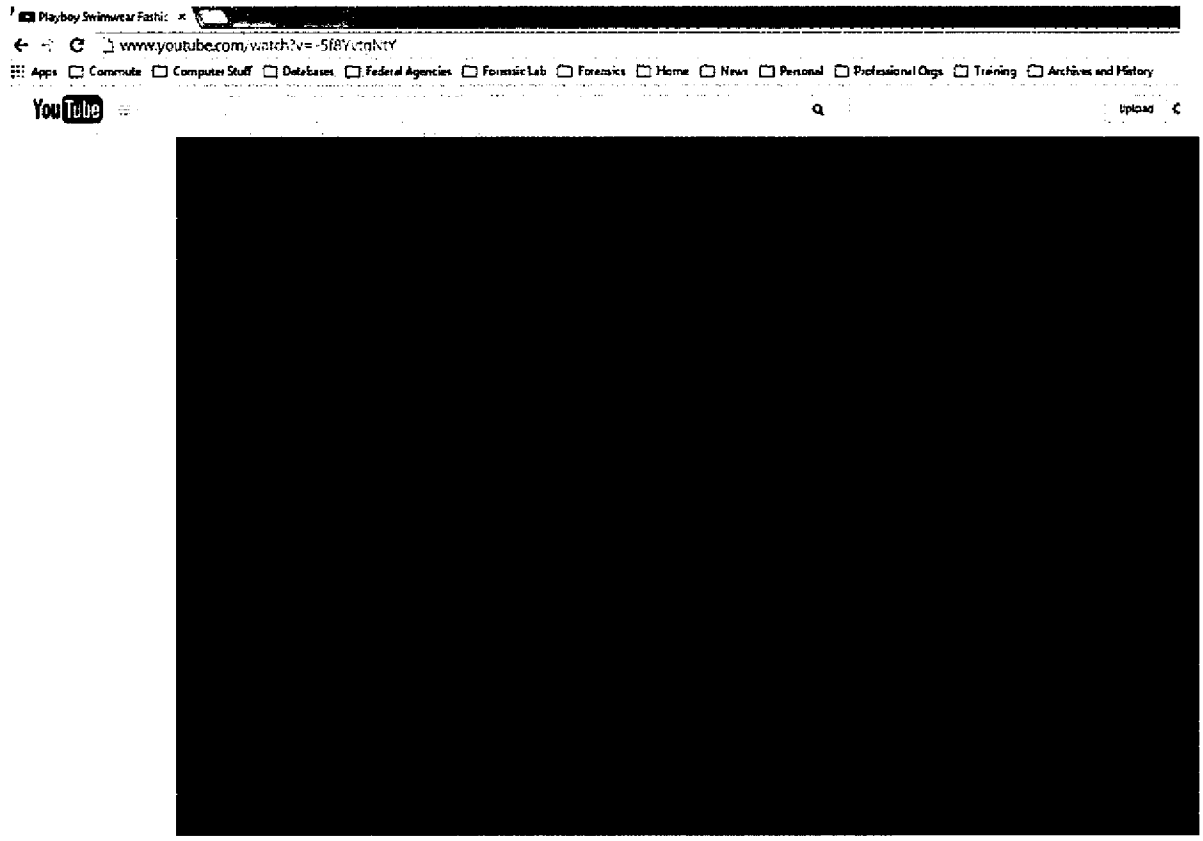
Appendix - Detailed results of the examination of webpages with screenshots showing video content

Date/Time	Webpage	Name
3/8/2014 7:42:22 AM	http://www.youtube.com/watch?v=XmlN-SKzgQo	▶ +18 Brasil Movie - Doce Delírio - YouTube



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

Date/Time	Webpage	Name
3/8/2014 9:47:19 AM	http://www.youtube.com/watch?v=-5f8YvtgNtY	▸ Playboy Swimwear Fashion Show - Miami Beach - YouTube



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

Date/Time	Webpage	Name
3/8/2014 9:47:35 AM	http://www.youtube.com/watch?v=0tS9I-oOUJ8	▶ TOPLESS MODEL SHOOT - YouTube

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

Date/Time	Webpage	Name
3/8/2014 9:49:38 AM	http://www.youtube.com/watch?v=I8RJuf6yb2c	Sexy Bikini Girls! 'Mexico' - YouTube

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

Date/Time	Webpage	Name
3/8/2014 9:51:42 AM	http://www.youtube.com/watch?v=g-COifO1shk	▶ Happy Boob Year 2010! - YouTube

Case Number:	Case Title:
OIG-I-14-0018	

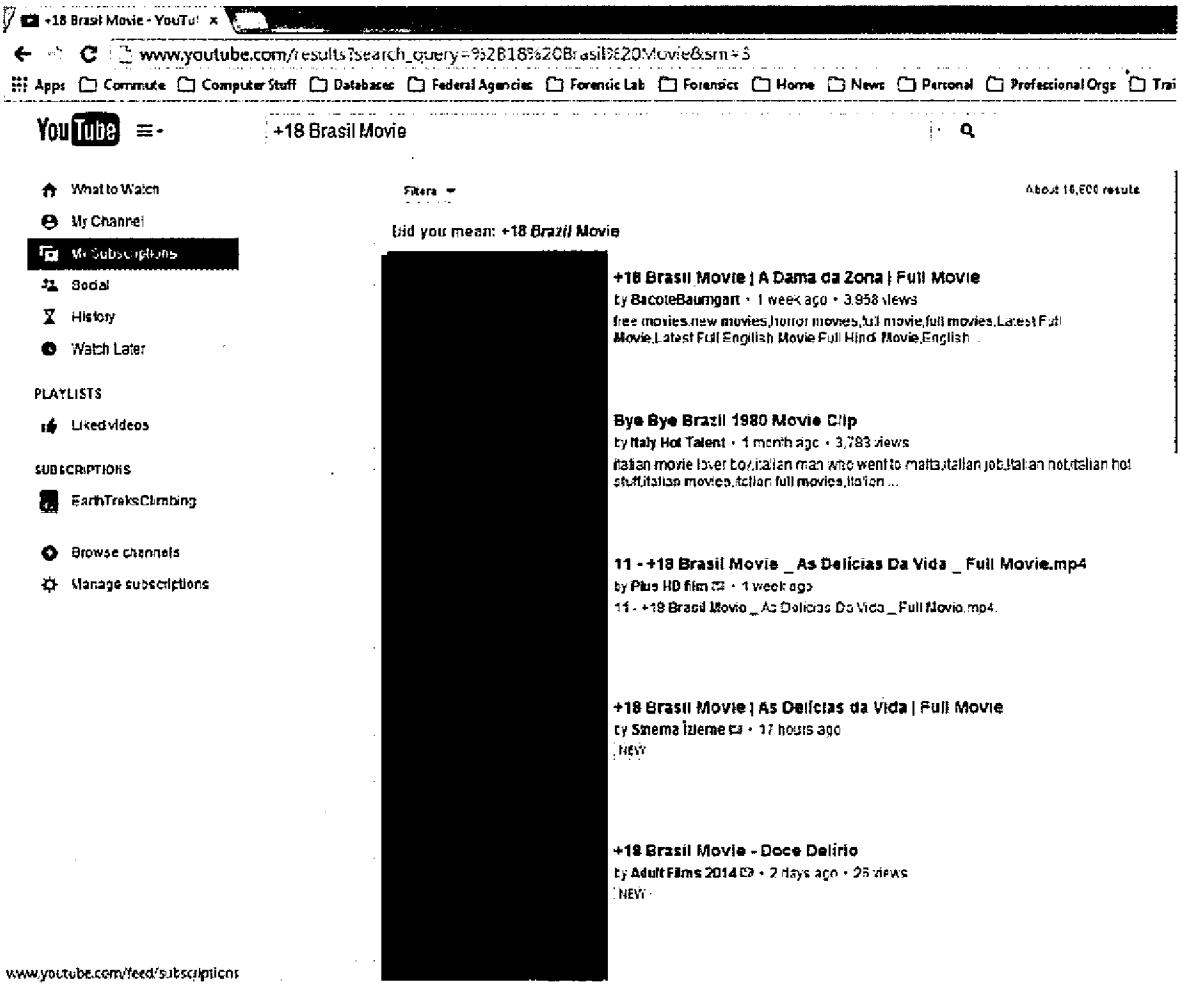
Date/Time	Webpage	Name
3/8/2014 9:51:54 AM	http://www.youtube.com/watch?v=3KkXS4IGZoA	▸ phim sex chồng đi vắng vợ ở nhà một mình ngoại tình 2014 - YouTube

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

Date/Time	Webpage	Name
3/8/2014 10:40:32 AM	http://www.youtube.com/watch?v=LqrTYafxsbM	Mil Sexos Tiene La Noche Pelicula Completa +18 - YouTube

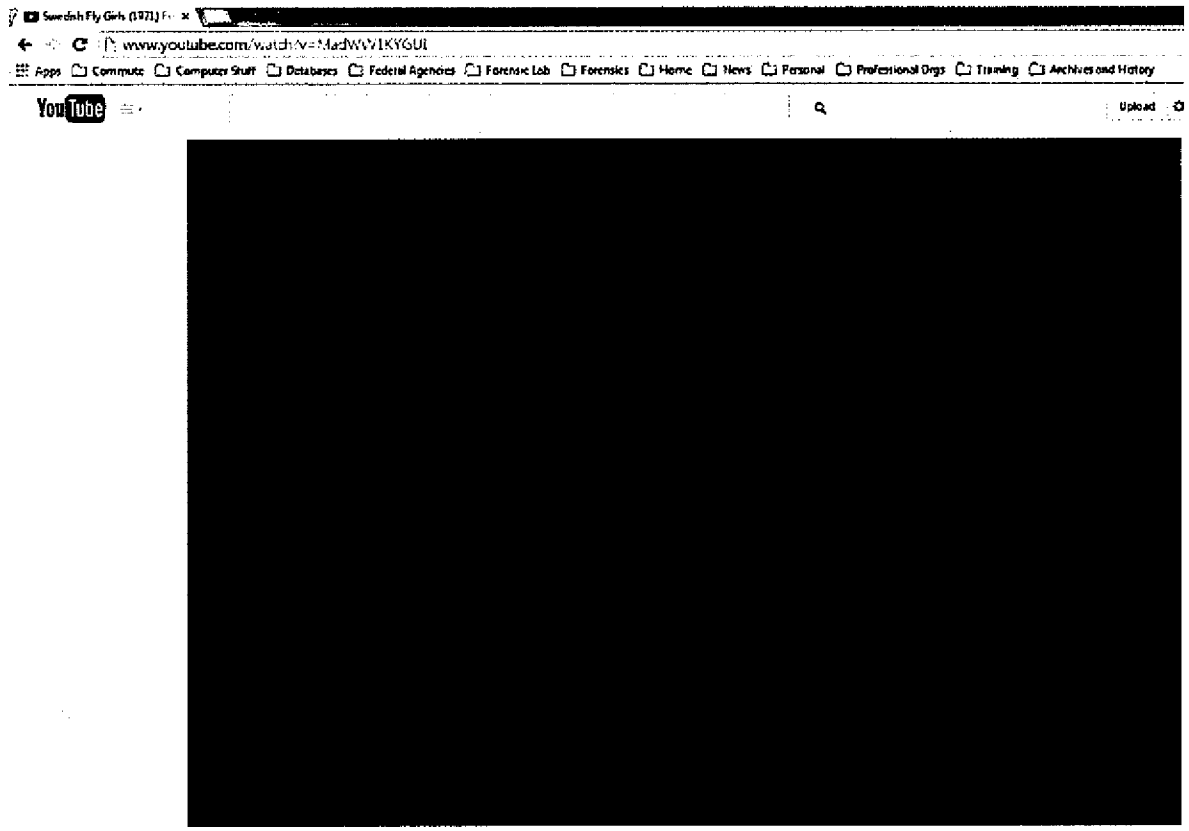
Case Number:	Case Title:
OIG-I-14-0018	[redacted]

Date/Time	Webpage	Name
3/8/2014 10:43:25 AM	http://www.youtube.com/watch?v=V6ZFJC9KGbA	▸ +18 Brasil Movie	A Dama da Zona	Full Movie - YouTube



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

Date/Time	Webpage	Name
3/8/2014 10:57:48 AM	http://www.youtube.com/watch?v=MadWW1KYGUI	▸ Swedish Fly Girls (1971) Full Movie 17+ - YouTube

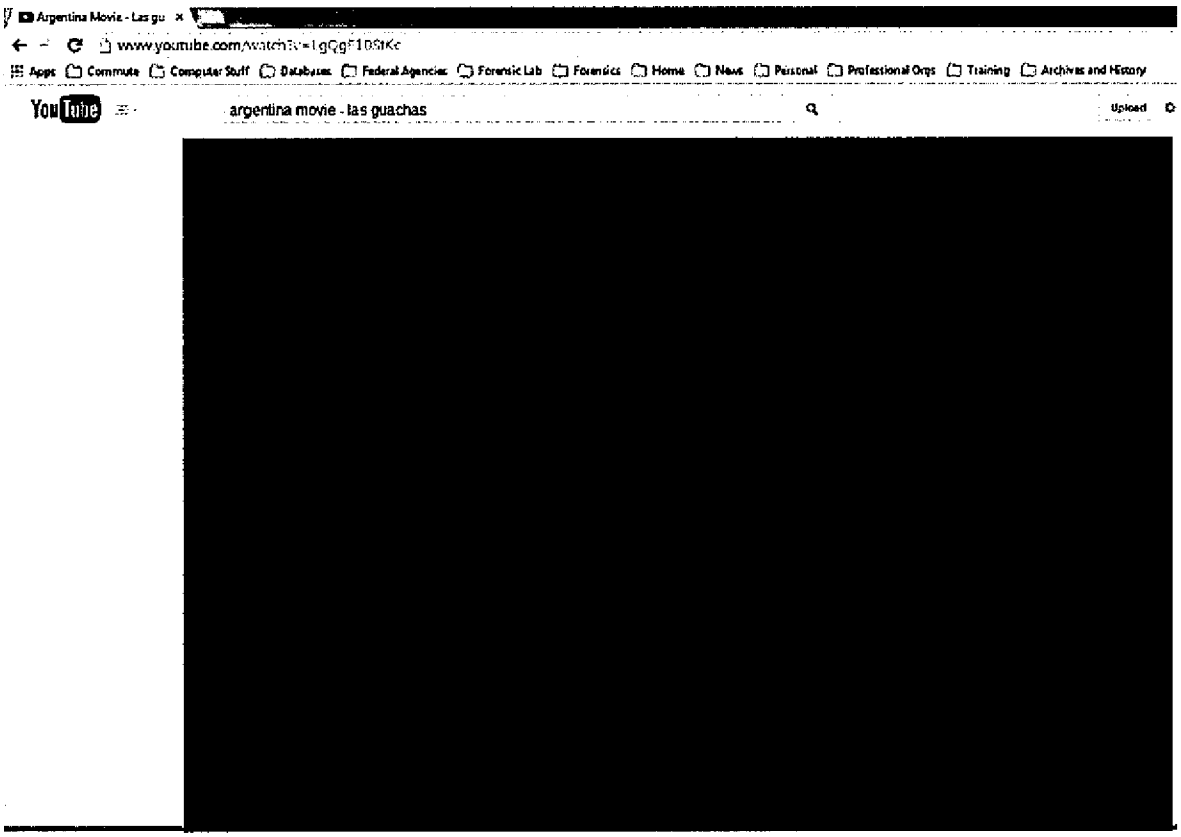


Case Number:	Case Title:
OIG-I-14-0018	[redacted]

Date/Time	Webpage	Name
3/8/2014 11:10:27 AM	http://www.youtube.com/watch?v=076YTYe4g-I	▶ Reformatório das Depravadas | Full Movie - YouTube

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

Date/Time	Webpage	Name
3/8/2014 11:10:50 AM	http://www.youtube.com/watch?v=krsuYeO8gXM	Argentina Movie - Las guachas - YouTube



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

Date/Time	Webpage	Name
3/8/2014 11:12:40 AM	http://www.youtube.com/watch?v=JBz-ab-BCPg	▸ USA Movie - Confessions of a Young American Housewife - YouTube

[redacted] [redacted]

FCC Computer System
User Rules of Behavior

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.

YOU ARE RESPONSIBLE FOR ALL ACTIONS PERFORMED WITH YOUR PERSONAL USER ID.

- UserIDs and passwords are for your individual use only, and are confidential FCC information.
- Your UserID and password must be used solely to access computer resources for the performance of your official FCC job functions. (Refer to 5 CFR Part 2635, "Standards of Ethical Conduct for Employees of the Executive Branch.")

POLICY, STANDARDS, AND PROCEDURES MUST BE FOLLOWED.

- Use of all computer resources, including personal computers, laptops, all parts of the FCC Network, communication lines, and computing facilities are restricted to FCC-authorized purposes only.
- You must be aware of, and abide by the "Computer Fraud and Abuse Act of 1986" (Public Law 99-474), the civil and criminal penalties of the Privacy Act, the Trade Secrets Act (18 U.S.C. 1905), and other Federal Regulations applying to unauthorized use of FCC files, records, and data. Training will be provided to educate you about your responsibilities under these statutes.
- Be aware that all computer resources assigned, controlled, accessed, and maintained by FCC employee and contractor personnel are subject to periodic test, review, and audit.

ACCESS TO INFORMATION MUST BE CONTROLLED.

- Access only the information for which you are authorized, and have "need to know/access."
- Do not leave computers logged on and unattended. Log off, use "lock workstation" feature, or use access control software (i.e., Screen Saver with password) during unattended use.
- If you know that a person, other than yourself, has used or is using your userID, you must report the incident immediately to your supervisor and the Computer Security Officer.
- Take steps necessary to maintain security of computer files and reports containing FCC information.

YOU ARE RESPONSIBLE FOR THE PROPER USE OF YOUR COMPUTER RESOURCES.

- Only use FCC-approved software, and comply with vendor software license agreements.
- Back up your programs and data on a regular basis, and do not store sensitive or mission-critical data on your PC's hard drive.
- All FCC computer resources, including hardware, software, programs, files, paper reports, and data are the sole property of the FCC.

USER CERTIFICATION

I certify that I have read the above statements, fully understand my responsibilities, and agree to comply.
I recognize that any violation of the requirements indicated above may be cause for disciplinary actions.

Name (please print): [redacted] Bureau/Office: PS HSB

Signature: [redacted] Date: 04/08/13

Return Form to: TW-C417

Form A-201
Revised January 2006

UNITED STATES GOVERNMENT
FEDERAL COMMUNCIATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: April 28, 2014

TO: David L. Hunt, Inspector General, Federal Communications Commission

CC: [redacted], Deputy Inspector General, Federal Communications Commission

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Investigator, [redacted], Computer Forensics Investigator

SUBJECT: [redacted], [redacted], [redacted], [redacted], [redacted]

Background

On February 3, 2014 a written statement was provided, by a person who requested anonymity, to the Office of Inspector General in which the writer outlines various allegations concerning six (6) individuals who work in the FCC Reference Information Center. The allegations included:

1. "Sleeping at their respective desks"

2. "No to minimal work production (with evidently, no accountability) with the only exception of tending to plants located on the window sill."

3. "Arguing with one another and the use foul language."

4. "Constantly printing personal items of interest."

Case Number:	Case Title:
OIG-I-14-0022	[redacted]

5. "Using the phones of others and at the RIC counter to make personal calls to creditors, etc."

6. "Falsifying time."

7. "Selling of products i.e. Avon, Bootleg DVDs, Clothing, Perfume, etc."

8. "Sitting together in chairs and looking out the window."

9. "Talking to the Guard"

[redacted] (GS-11) is alleged to have committed time and attendance fraud by working fewer hours than [redacted] tour of duty required, and spending considerable time while on official duty away from [redacted] work area, copying numerous personal documents and talking and arguing on the phone for long periods of time. The writer observed a general lack of any FCC-related work performed by, or work product produced by [redacted].

[redacted] (GS-9) is alleged to often sleeping in her chair, selling Avon products and staring out the window. The writer observed a general lack of any FCC-related work performed by, or work product produced by [redacted].

[redacted] (GS-12) is alleged to never do anything other than tending to the plants on the window and collecting personal items from the printer as well as staring out the window.

[redacted], (GS-9) who is physically located in the [redacted], is alleged to sleep at [redacted] desk, play computer games or argue on the phone. [redacted] will frequent the Resource Information Center to discuss topics of interest with other employees and does not appear to perform any FCC-related work.

[redacted] (GS-10) is alleged to travel back and forth to the lunch room and "hang-out" at the guard's station. The writer observed on at least one occasion that [redacted] stayed at the guard station for the entire guard shift. The writer observed a general lack of any FCC-related work performed by [redacted].

The 6th person named in the statement is [redacted] (GS-11) who was the subject of a separate investigation that has since been forwarded to the Bureau.

Time and Attendance Rules

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 non-overtime 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 non-workdays established by Federal statute, Executive order, or administrative order.

According to the Federal Communications Commission's Employee Handbook[1], 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] **Findings: Time and Attendance Issues**

[1] http://intranet fcc.gov/docs/omd/hrm/employee_handbook/OMDEmployeeHandbook.pdf

On February 3, 2014 and April 8, 2014 Building Access Control Records were obtained and reviewed for [redacted] covering the period from October 27, 2013 through April 7, 2014, which for this specific review, equaled 83 days of badge data. This review showed that [redacted] amassed a total of 27.45 hours that can be attributed to leaving before [redacted] regular tour of duty.

On February 4, 2014 and April 8, 2014 Time and Attendance (T&A) records from the FCC payroll office were obtained and reviewed for [redacted] covering the same period. An excel spreadsheet (attachment 1) was created showing arrivals and departures from the FCC Headquarters building as well as any leave taken during the period reviewed. The review indicated that [redacted] did not request leave for the 27.45 hours that [redacted] worked less than [redacted] tour of duty.

[redacted] Findings: Inappropriate Activities During Official Tour Of Duty

After reviewing the other alleged activities it has been determined that those issues, while serious, are more appropriately addressed by Bureau Management, in the first instances, as managers are best positioned to observe, and evaluate their employees' on- the- job performance and take appropriate remedial action if necessary.

[redacted] Conclusion:

Based upon the access control system badge data as well as the time and attendance data, it is reasonable to conclude that [redacted] has not followed the time and attendance rules relative to [redacted] official tour of duty. However the other claims of inappropriate activity while on official government time should be considered by Bureau management with appropriate action taken as necessary to ensure performance.

[redacted], [redacted], [redacted], [redacted] Findings:

After reviewing the alleged activities, it has been determined that those issues, while serious, are more appropriately addressed by Bureau Management, in the first instances, as managers are best positioned to observe, and evaluate their employees' on- the- job performance and take appropriate remedial action if necessary.

Case Number:	Case Title:
OIG-I-14-0022	[redacted]

Recommendations

[redacted]

Case Number:	Case Title:
OIG-I-14-0022	[redacted]

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: August 27, 2014

TO: David L. Hunt, Inspector General

CC: [redacted], Deputy Inspector General

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Computer Forensics Investigator

SUBJECT: FCC [redacted], Violation of 5 C.F.R § 2635.704 (Use of Government Property)

Background of Investigation

In April 2014, the Office of Inspector General received allegations that [redacted], was using the Commission's computer network to perform work related to several outside tax and accounting businesses.

Scope of Investigation

The objective of this investigation was to determine if [redacted] used the Commission's computer network to perform work related to several outside tax and accounting businesses. To conduct the investigation, FCC OIG investigators performed the following steps.

1. Obtained and reviewed FCC Directive FCCINST 1479.4, entitled "FCC Cyber Security Program" and effective May 1, 2011. This Directive establishes policy and assigns

responsibilities for assuring optimal levels of protection required for FCC data and information systems.

2. Obtained and reviewed the Commission's Cyber Security Policy, version 3.5 promulgated by the Office of the Managing Director and effective June 20, 2013. This policy 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.

3. Obtained and reviewed FCC Form A-201, entitled "FCC Computer System User Rules of Behavior" revised in January 2006.

4. Obtained and reviewed [redacted]'s FCC Outlook Mailbox.

5. Obtained and reviewed [redacted]'s network share.

Conclusions:

Our investigation did not substantiate the allegations. Specifically, we did not find any evidence that [redacted] used the Commission's computer network to perform work related to several outside tax and accounting businesses. In fact, we found correspondence between [redacted] and the Office of General Counsel (OGC) that demonstrates an effort of [redacted]'s part to ensure that there is no conflict of interest related to [redacted] work for the outside businesses. Further, we conducted a keyword search of the digital evidence using the names of the outside businesses and did not identify any relevant email correspondence, Microsoft Office documents, Excel Spreadsheets, or any other files.

Recommendations

Based on our findings, we would recommend no further investigation into this issue at this time.

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: August 18, 2014

TO: David L. Hunt, Inspector General

CC: [redacted], Deputy Inspector General

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Computer Forensics Investigator, [redacted], Investigator

SUBJECT: FCC Employee [redacted], Prohibited Use of Government Issued Credit Card-

---

Background of Investigation

On June 18, 2014 [redacted], Labor Relations, called [redacted], AIGI, and informed [redacted] that [redacted] office had been working on a case involving [redacted]. Subsequently [redacted] had been informed by [redacted], agency program coordinator for travel, Financial Operations that a notification was sent by J.P. Morgan/Chase Bank to the FCC indicating "possible suspicious activity" on a government travel card issued to [redacted], [redacted], [redacted], International Bureau. On June 19, 2014, FCC OIG initiated a preliminary investigation

Scope of Investigation

Case Number:	Case Title:
OIG-1-14-0028	[redacted]

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

Interview of [redacted]:

On June 19, 2014 a telephone interview was conducted with [redacted]. On Wednesday June 11, 2014, [redacted] received an email from the J.P. Morgan/Chase fraud section indicating a possible fraud alert for the travel card belonging to FCC employee [redacted]. According to J.P. Morgan/Chase three (3) cash advances were taken using the travel card on June 3, 2014 and June 4 2014 for a total amount of $480.11. The travel card was deactivated on June 5, 2014. According to [redacted] J.P. Morgan/Chase will not be pursing this issue as a fraud case as it appears to be a case of "user misuse".

After receiving the fraud alert [redacted] sent an email to [redacted]'s supervisor and [redacted], Assistant Bureau Chief for Management – IB, explaining the report of suspicious activity on the card and asking [redacted] to call [redacted]. To date [redacted] has not responded to [redacted]'s request.

[redacted] contacted [redacted]'s [redacted] who confirmed that [redacted] is not on official travel and should not be using [redacted] travel card. [redacted] further confirmed that the bureau is currently working with the FCC Labor Relations office in regard to issues they are having with [redacted] and indicated [redacted] has not been in the office in recent weeks. [redacted] voluntarily provided a copy of [redacted]'s J.P. Morgan/Chase travel card statement and spreadsheet (attached) showing attempted use of the card.

Interview of [redacted]:

[redacted] is the [redacted] Bureau, Federal Communications Commission. Since approximately January 2014 [redacted] along with [redacted], supervisor to [redacted], has been working with the FCC's Office of Labor Relations regarding issues with [redacted]. According to [redacted], [redacted] has been listed as AWOL intermittently since January 2014.

[redacted] advised that [redacted] is currently on administrative leave and is not being allowed into the building, due to a possible medical condition, and is being required to bring in a doctor's note before [redacted] will be allowed to come back to work.

[redacted] confirmed that [redacted] is not on official government travel and that [redacted] has not responded to attempts to contact [redacted] regarding the suspicious charges on [redacted] travel card.

Case Number:	Case Title:
OIG-I-14-0028	[redacted]

Several attempts were made to contact J.P. Morgan/Chase fraud department in an effort to determine if CCTV footage from any of the locations at which withdrawals were made would be available for review. No response was received from J.P. Morgan/Chase. Additionally an attempt to contact [redacted] by telephone was made but no response was received from [redacted].

Conclusions:

Based on the information provided by [redacted] and [redacted] along with a review of the travel card information and spreadsheet it appears that [redacted] may have used the card without authorization. However there is no monetary loss to the government as the employee is responsible for the debt and the card has been cancelled eliminating any future possibility that the card can be used. It appears that [redacted]'s management is dealing with other employment related issues concerning [redacted] and can include the misuse of the travel card in any action they deem warranted.

Recommendations

It is recommended that [redacted]

Attachments

Case Number:	Case Title:
OIG-I-14-0028	[redacted]

UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: August 21, 2014

TO: David L. Hunt, Inspector General

CC: [redacted], Deputy Inspector General

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Computer Forensics Investigator, [redacted], Investigator

SUBJECT: FCC Employee [redacted], Violations of the Hatch Act, 5 U.S.C. §§ 7321-7326

Background of Investigation

On June 21, 2014, the Office of Inspector General received an anonymous letter from "A concern (sic) employee" alleging Hatch Act violations by [redacted], Enforcement Bureau (EB). The letter states that [redacted], a former attorney with EB, recently resigned from the Commission to run for the office of the [redacted]. The letter alleges that certain FCC employees, including [redacted], who are "friends of [redacted]" have been "engaged on a daily basis in personal activities during the work day by surfing the internet using their FCC computers to search for news about [redacted]'s candidacy" and "using the FCC email network to send emails to colleagues at the FCC about [redacted]'s candidacy." The letter further alleges that when [redacted] sends an email message about [redacted], '[redacted] emails contain [redacted] electronic signature showing [redacted] official position and title at the FCC."

Case Number:	Case Title:
OIG-1-14-0029	[redacted]

Scope of Investigation

The objective of this investigation was to determine if [redacted] used the Commission's computer network to engage in "partisan political activity" in violation of the Hatch Act and Commission policies and directives. To conduct the investigation, FCC OIG investigators performed the following steps.

1. Obtained and reviewed the Hatch Act as contained in 5 U.S.C. §§ 7321-7326.

2. Obtained and reviewed the FCC Office of General Counsel (OGC) ETHICSgram from October 2011 addressing the Hatch Act.

3. Obtained and reviewed FCC Directive FCCINST 1479.4, entitled "FCC Cyber Security Program" and effective May 1, 2011. This Directive establishes policy and assigns responsibilities for assuring optimal levels of protection required for FCC data and information systems.

4. Obtained and reviewed the Commission's Cyber Security Policy, version 3.5 promulgated by the Office of the Managing Director and effective June 20, 2013. This policy 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.

5. Obtained and reviewed FCC Form A-201, entitled "FCC Computer System User Rules of Behavior" revised in January 2006.

6. Obtained and reviewed [redacted]'s FCC Outlook Mailbox.

Conclusions:

Our investigation did not substantiate the allegations. We found one email message that included a link to a fundraising page for [redacted] that [redacted] received from the [redacted] campaign. [redacted] responded to that email by requesting that [redacted] work email address be removed from the site. We found several email messages from [redacted] to FCC colleagues that included links to articles about the campaign. However, we do not believe that this activity (either using the Commission's network to search for articles on the campaign or forwarding links to these articles) violates the Hatch Act or the Commission's personal use policy. Thus, we did not find evidence that [redacted] sent any email message that could be construed as violating the Hatch Act

(e.g., soliciting contributions, allowing official title to be used in fund raising activities, engaging in political activity, etc.).

We shared our conclusions with [redacted], Senior Legal Advisor (Ethics), Office of General Counsel (OGC). [redacted] agreed with the OIG conclusions.

Recommendations

Based on our findings, we would recommend no further investigation into this issue at this time.

UNITED STATES GOVERNMENT
FEDERAL COMMUNCIATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

TO: David L. Hunt, Inspector General, Federal Communications Commission

CC: [redacted], Deputy Inspector General, Federal Communications Commission

FROM: [redacted], Acting Assistant Inspector General for Investigations, [redacted], Investigator

SUBJECT: [redacted] (FCC Employee Time and Attendance)

DATE: September 8, 2014

Background

An anonymous allegation was made to [redacted], who in turn passed the allegation to the OIG, alleging that [redacted], CGB, has been given preferential treatment regarding time off during [redacted]. According to [redacted], [redacted] currently maintains a "high leave balance" despite the fact that [redacted] was not at work for approximately three (3) months.

Findings

Review of time and attendance records as well as building access control badge records were completed covering the period from September 26, 2013 to December 31, 2013. The access control record show that [redacted]'s badge was used a total of 17 times in the above stated period. There was no badge activity from September 22, 2013 through December 31, 2014 except for

Case Number:	Case Title:
OIG-I-14-0035	[redacted]

two days in November. The time and attendance records show that [redacted] used a total of 474 hours of approved leave in the period using a combination of annual leave (176 hours), sick leave (146 hours) and time-off award leave (152hours).

It should be noted that for the 17 days of badge activity found, [redacted] did not complete [redacted] full tour of duty by 17 hours and 33 minutes. (See attached excel spreadsheet)

Conclusion

Based upon the time and attendance records reviewed, it is reasonable to conclude that [redacted] appropriately followed the rules governing leave. Thus, the allegation of preferential treatment is without merit. However, based on the access control records, it appears that [redacted] did not complete [redacted] official tour of duty in the period under review.

Recommendations

Based on our findings, [redacted].

UNITED STATES GOVERNMENT
FEDERAL COMMUNCIATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: June 30, 2014

TO: David L. Hunt, Inspector General, Federal Communications Commission

CC: [redacted], Deputy Inspector General, Federal Communications Commission

FROM: [redacted], Assistant Inspector General for Investigations, [redacted], Investigator

SUBJECT: [redacted]

Background

On April 6, 2014 a written statement was provided to the Office of Inspector General Hotline in which the writer, a former Commission employee, outlines various allegations involving what [redacted] feels are "serious management problem[s] at the FCC dealing with excessive and unreasonable delays in regulatory actions that address new sources of spectrum interference" and ask the Office of Inspector General to investigate "why [the] FCC has been so slow in resolving serious problems with interservice radio interference" in two rulemaking proceedings.

Case Number:	Case Title:
OIG-I-14-0021	[redacted]

Findings

On April 9, 2014 a redacted copy of the letter was forwarded by [redacted] to [redacted], [redacted] and [redacted] asking for their assessment of the allegations. A response was requested within 60 days.

On June 11, 2014 a response was received from [redacted], Deputy Bureau Chief, Enforcement Bureau. The response indicated that management from the Enforcement Bureau, Office of Engineering and Technology and Wireless Telecommunications Bureau reviewed the complaint and provided the following:

> At this time management believes no specific action by the FCC is needed to address the complaint. The complaint alleges a number of harms to consumers and industry as the result of two rulemaking proceedings; however, it provides no substantiated facts to support those allegations, nor does it provide any evidence of waste, fraud or abuse by Commission employees involved in this rulemaking.
>
> In any event, the Commission acted appropriately in both proceedings in balancing the effects of specific actions on licensees, manufacturers and the public. Specifically, the complaint does not accurately reflect the situation regarding signal boosters as it evolved over time. CTIA submitted a white paper detailing several specific interference events that were investigated by carriers and found to be attributable to non-compliant equipment. At the same time, the Enforcement Bureau, working with CTIA, established a hotline for any additional interference complaints that were investigated and resolved as the Commission became aware. All of the instances of interference were found to be the result of equipment not authorized by carriers or non-compliant equipment.
>
> Subsequently, in response to Petitions from the industry, the Commission opened a rulemaking proceeding to craft a set of rules that would provide for much needed signal boosters to provide service to rural areas while also protecting the wireless networks from interference. This proved to be a very contentious and complex undertaking. In seeking solutions, the Commission engaged all parties, which ultimately resulted in a collaborative process to resolve the issues to all parties' satisfaction. Experience has shown that such a process may be lengthy, but ultimately yields the best result and generally takes less time as it minimizes the potential for reconsideration petitions and court appeals.

Conclusion

Based on the information contained in the response from the Bureaus involved with the issue it appears that prudent, appropriate measures were taken to deal with, and ultimately resolve, the complex policy and technical issues that were raised in the complaint.

Recommendation

It is recommended that no further action be taken in this case.