



NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CLOSEOUT MEMORANDUM

Case Number: I11060027

Page 1 of 1

An investigation was initiated when two NSF employees¹ came forward to OIG and reported that their eight year old son had inappropriately used one of their NSF-issued devices (an iPhone) to access and view websites containing adult pornography.²

A forensic review of the iPhone identified that numerous mobile online pornographic websites were visited on three separate dates. The evidence available was not sufficient to prove or disprove what the employees had related had occurred and OIG could not determine the identity of the viewer of the improper sites/content on the iPhone.

A report of investigation, concerning the employee³ whose iPhone was misused, was issued to NSF for action. A counseling memorandum was issued to the employee regarding his/her failure to properly safeguard government property.

Accordingly, this matter is closed.

1
2
3

[REDACTED]



National Science Foundation • 4201 Wilson Boulevard • Arlington, Virginia 22230

Office of the Inspector General

JUN 12 2012

Confidential

To: [REDACTED]

From: Alan F. Boehm, Assistant Inspector General for Investigations *inf/Alan Boehm*

Subject: Report of Investigation (OIG Case No. I11060027)

Please note: This report contains confidential personal information and it should be disclosed only to individuals who must have knowledge of its contents to facilitate NSF's assessment and resolution of this matter. Unauthorized disclosure may result in personal criminal liability under the Privacy Act, 5 U.S.C. § 552a(i)(1).

The attached Investigative Report concerns an NSF employee who reported that her eight year old son used her government-issued iPhone to access and view online pornography.

Based on the facts set out in the Investigative Report, we have concluded:

- Official government property was used to view online pornography; and,
- Official government property was used to access an inappropriate adult online dating and social networking services site
- The NSF employee failed to protect official government property;
- The NSF employee failed to ensure that official government property was used only for authorized purposes;

Please advise me by July 12, 2012 of the actions taken regarding the recommendations contained in our report.

Attachment

cc: Cora Marrett, Deputy Director
Allison Lerner, Inspector General
Gene Hubbard, Office Head & Chief Human Capital Officer, OIRM
Lawrence Rudolph, General Counsel
Clifford Gabriel, Office of the Director's Liaison to OIG

National Science Foundation Office of Inspector General



Confidential Investigation Report Case Number I11060027 June 12, 2012

**This Confidential Report of Investigation is provided to you
FOR OFFICIAL USE ONLY.**

It contains protected personal information, the unauthorized disclosure of which may result in personal criminal liability under the Privacy Act, 5 U.S.C. § 552a. This report may be further disclosed within NSF *only* to individuals who *must* have knowledge of its contents to facilitate NSF's assessment and resolution of this matter. This report may be disclosed outside NSF *only* under the Freedom of Information and Privacy Acts, 5 U.S.C. §§ 552 & 552a. Please take appropriate precautions handling this confidential report of investigation.

Please note: This report contains confidential personal information and it should be disclosed only to individuals who must have knowledge of its contents to facilitate NSF's assessment and resolution of this matter. Unauthorized disclosure may result in personal criminal liability under the Privacy Act, 5 U.S.C. § 552a(i)(1).

Summary

This investigation involves two National Science Foundation (NSF) employees, Employee 1¹ and her husband Employee 2², who came forward and reported to the Office of Inspector General (OIG) that their eight year old son had inappropriately used an NSF-issued iPhone (issued to Employee 1) to access and view websites containing adult pornography.

Both NSF employees were interviewed and denied that either had accessed the websites themselves. OIG then contracted a private company to conduct a forensic review³ of the iPhone issued to Employee 1 and the BlackBerry and iPad issued by NSF to Employee 2. The review determined that the BlackBerry and iPad history files contained no records of visits to inappropriate sites. The iPhone review indicated that numerous mobile online pornographic websites were visited on three separate dates.⁴ The websites were apparently accessed initially by typing in the actual website addresses directly, rather than through a search engine using key words. There was no evidence of misspelled or mistyped words being searched, so the addresses were apparently entered correctly the first time. The two employees were re-interviewed once forensic results were obtained and both again denied any wrongdoing and continued to blame their eight year old son for the inappropriate access to pornographic video websites, an adult chat site, and an adult social network service site.

A review of all sites visited determined that some non-pornographic sites were visited less than a minute before, or directly between, the visits to pornographic websites. These sites included Facebook, Yahoo!, and a government website www.chcoc.gov (determined to be the website for the Chief Human Capital Officers Council in which a news transmittal about General Schedule within-grade increases was reviewed).⁵ OIG tried to determine if the Facebook and Yahoo! sites accessed on the iPhone, were the personal sites belonging to the subject, however the data for these sites proved inconclusive in making a determination of the identity.

¹ [REDACTED] (Employee 1).

² [REDACTED] (Employee 2).

³ TAB 1 - Access Data Group, LLC Forensic Report and Mobile Analysis Data; TAB 1A:- iPhone Safari History, TAB 1B - iPad Safari History and TAB 1C - Blackberry browser URLs.

⁴ TAB 2 - List of websites visited on June 17, 2011, June 20, 2011, and June 23, 2011.

⁵ TAB 3 - List of non-pornographic sites visited. TAB 3A - Copy of news transmittal from website www.chcoc.gov.

OIG's review of work emails, R drive⁶ files and C drive⁷ files for Employee 1 found no instances of inappropriate use. OIG's review of the work emails, R drive files and C drive files for Employee 2 found no instances of inappropriate use.

The available evidence is not sufficient to either prove or disprove the version of events related by Employees 1 and 2 as to the identity of the viewer of the improper content on the iPhone device. The available evidence supports the conclusion that Employee 1 breached her ethical duty to protect and conserve the government property entrusted to her care, thereby leading to the misuse of the property.

OIG Investigation

A. Background

Two NSF employees, Employee 1 and Employee 2, came forward to NSF OIG and reported that their eight year old son had improperly obtained and used the iPhone issued to his mother (Employee 1) to access and view inappropriate websites containing pornographic material/videos.

A review of the iPhone history identified 34 instances in which 13 different inappropriate websites were visited. The data shows that Employee 1's iPhone was used to visit 11 pornographic video websites on about 30 different instances, along with 2 visits to a phone chat site and 2 visits to an adult online dating and social network services site, during the late evening/early morning hours on three separate dates.

A review of all sites visited determined that some non-pornographic sites were visited less than a minute before, or directly between, the visits to pornographic websites. These sites included Facebook and Yahoo!.

B. Applicability of NSF Policy

Pursuant to NSF policy regarding *Personal Use of NSF's Technology and Communication Resources* contained in NSF Bulletin 08-18 ("Personal Use Policy"),⁸ NSF staff members are authorized to use NSF technology and communication resources for occasional personal use. However, this policy creates express limitations on personal use, which are similar to those cited in the Federal CIO Council's 1999 Model Policy/Guidance on "Limited Personal Use" ("Model Policy"),⁹ as examples of inappropriate uses.

⁶ The R drive is a designated network drive assigned to each NSF employee/user for individual use/storage of data and accessible only by the individual employee/user and/or OIRM/DIS technical staff.

⁷ The C drive is the employee's desktop computer drive.

⁸ See TAB 4 - NSF Bulletin 08-18.

⁹ See TAB 5 - Copy of Federal CIO Council's 1999 Model Policy/Guidance on "Limited Personal Use."

According to Section IV of the Model Policy:

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate. Misuse or inappropriate use of government office equipment includes: Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public . . . and . . . the creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.

OIG obtained information that both employees completed NSF Information Technology security training.¹⁰ This training includes NSF's IT Security "User Responsibilities-Rules of Behavior."¹¹ NSF users acknowledge and agree that they will comply with the rules on appropriate use, some of which are as follows:

- I may be provided with electronic tools such as computers, cell phones, and personal electronic devices to accomplish my official duties. I will use only the systems, software and data which I am authorized to use.
- I understand that I am responsible for proper use of all IT resources, and for any misuse of such IT resources. I understand that personal use is authorized only in accordance with NSF policy.
- I will not seek, transmit, collect, or store defamatory, discriminatory, harassing, or intimidating material that could discredit NSF or damage its public reputation.
- I will not seek, transmit, collect, or store obscene, pornographic, or sexually inappropriate material.

NSF users also acknowledge and agree with the individual accountability statement as follows:

"I understand that failure to comply with the Rules of Behavior or other requirements of NSF policy may result in disciplinary action, sanctions, personal liability, and/or civil or criminal penalties."

C. Interviews of the NSF Employees

The employees were interviewed by representatives from OIG in reference to the misuse of the iPhone by their eight year old son who allegedly accessed and viewed websites containing pornographic material.

Prior to the individual interviews, OIG provided each of the employees with a copy of *Weingarten* and *Garrity* Warnings, which they each read and signed.

¹⁰ See TAB 6 - Training dates for Employee 2 and TAB 7 - Training dates for Employee 1.

¹¹ See TAB 8 - Copy of NSF IT Security "User Responsibilities-Rules of Behavior."

Employee 1 Interview¹²

On July 20, 2011, Employee 1 was interviewed and explained that she was issued an iPhone for home and office use because she often handles calls and requests after hours in the evenings and over the weekends for her division. She said she did not sign any forms when these devices were issued to her. She explained that on June 23, 2011 she woke up at around 2:30AM and noticed the light was on in her son's room. She said that her eight year old son tends to stay up late or wake up in the middle of the night. She said she went to his room and asked him what he was doing and as she began to walk towards the closet in his room he moved in front of her. She said she opened the closet and found her NSF iPhone on the floor and saw the screensaver on. She said she began reviewing either the internet history or bookmarks and found pornographic websites had been visited and she noticed some were from seven days earlier. She said she does not remember the website names. She said she did view one site in which a man was having oral sex with a woman.

Employee 1 said she woke her husband up and told him about what she found and told him that he may want to check his NSF-issued iPad and BlackBerry to see if their son had used them to look at porn sites. She said she is not sure if her husband checked his BlackBerry or iPad; he did not tell her but she believes he might have checked them and found nothing.

Employee 1 explained that her son probably got her iPhone out of her pocketbook while she was asleep. She said she sometimes lets her son use her iPhone but that she enters the passcode and hands it to him. She said he might have looked over her shoulder and seen the passcode and remembered it; she is not sure how he would have her passcode. She explained that she uses the same PIN or passcode for all her devices – both she and her husband usually use birthdates and change the passcodes every 90 days or so. She said when she lets her son use her NSF iPhone he generally goes to game websites. She sees nothing wrong with letting her son use her NSF iPhone to play games.

Employee 1 explained that about three years ago, when her son was five years old, she caught him looking at pornography on their home computer. She said she scrolled through the drop down history and saw the recent sites he had visited. She said that he is just a curious child and probably entered search words like "police" and "mom" and "sex," after which the search engine provided results including porn sites. She said that he likes going on the internet. She explained that sometimes her husband takes their son to the house of one of his single male friends, and that this friend probably has adult magazines around or things on his computer that their son may have seen or picked up and was curious about. While his father and friend watch television or play games, her son usually spends time on the friend's computer.

Employee 1 was asked if her husband had [REDACTED]

[REDACTED]. She was asked if it was possible that maybe her husband had accessed

¹² TAB 9 - Memorandum of Investigation (MOI) - Interview of Employee 1, dated July 20, 2011 along with affidavit and TAB 9A - *Weingarten* and TAB 9B - *Garrity* Warning signed by Employee 1.

the home computer three years ago, not her son who was five years old at the time, and that her son had just merely clicked on the visited sites. She said that she did not believe so.

Employee 1 was asked whose idea it was to come to NSF OIG with the devices (her iPhone, her husband's NSF-issued BlackBerry and iPad) and she said she did not know but thinks it was her idea. She denied that her husband was the actual visitor to the porn sites, and denied that she and her husband had fabricated this story about the son to cover up the husband's misuse. She said her husband would not use her phone to access porn sites.

Employee 1 was asked if she and her husband had checked their home computer and their personal devices to see if their son had used those to access porn sites. She said that they had not. She was further asked if she uses her iPhone for personal calls and internet searches, and she explained that she does when her personal Droid phone is dead. She said that she uses the iPhone for emails, and goes to Facebook, the Target store website, and other sites, and does not consider this an issue.

Employee 1 then provided a written affidavit and written consent for OIG to review her NSF iPhone.

We subsequently contacted Employee 1 via telephone¹³ to request the power cord for the iPhone device, and she asked when the forensic review would be completed. Employee 1 expressed an interest in finding out the truth about the misuse of her iPhone.

Employee 2 Interview¹⁴

On July 20, 2011, Employee 2 was interviewed and he explained that on June 23, 2011 he either woke up at around 3:00 AM or his wife woke him, and told him that she caught their son with her iPhone looking at porn sites. He said he did not review his wife's iPhone. He said he accepted his wife's conclusion that the sites were inappropriate and did not need to look at it.

Employee 2 said that his son had never done this before. He said this is the first time that he is aware that his son has been caught viewing porn sites. He said he did not know whether his wife had caught their son looking at inappropriate sites prior to this incident.

He said he did not use his wife's iPhone and that he does not know the passcode. He said he does not use birthdates as his passcodes.

Employee 2 said he does not know how his son accessed his wife's iPhone or how he knew the passcode. He explained that his son is usually up at night watching cartoons. He said that both his son and his wife usually stay up late.

He explained that their old PC died months ago and that they just purchased a laptop right after this incident. Their son does not use the laptop – he has been punished. Employee 2 said that he

¹³ TAB 9C – MOI - Record of Conversation with Employee 1 on July 22, 2011.

¹⁴ TAB 10 - Memorandum of Investigation (MOI) – Interview of Employee 2, dated July 20, 2011 along with a written statement, and TAB 10A - *Weingarten* and TAB 10B - *Garrity* Warning signed by Employee 2.

had checked the old PC before it broke to review the sites visited and found nothing that concerned him. He said both the old PC and TV have parental controls. He said that he is aware that if someone mistypes words it may take you to a wrong site.

Employee 2 denied having used his wife's iPhone to visit porn sites. He said he did not use his BlackBerry or iPad to access inappropriate sites. He explained that his job involves being available after hours for emergencies and he therefore takes both devices, his BlackBerry and iPad, home because he sometimes may have to work after hours.

Employee 2 said he never gave his son the passcode to his BlackBerry or iPad. He explained that he went to the browser on his BlackBerry to check the device and saw no inappropriate sites that he or his son would have accessed intentionally, but that he didn't check the history. He said he did not check the iPad.

He said he asked his son about all his devices and whether he had used them and he said "no."

Employee 2 declined to provide a written affidavit. He did however provide a written statement saying that the government has the right to scan/review his NSF issued BlackBerry and iPad.

Forensic Results

The forensic report and Safari browser data provided by the forensic contractor indicates that the iPhone issued to Employee 1 had numerous site visits to inappropriate pornographic websites on two separate dates, June 17, 2011 and June 23, 2011. The report indicates that an adult online dating and social network services site at www.ashleymadison.com was visited but not logged into on June 17, 2011 at 1:35 AM, in between access times to video porn sites.¹⁵ This adult social network service site requires membership and payment (a credit card) in order to log onto. On June 23, 2011, at 2:15:13 AM, the website www.chcoc.gov, determined to be the website for the Chief Human Capital Officers Council, was accessed and a news transmittal about General Schedule within-grade increases was reviewed. Access to this site occurred between access to two separate pornographic websites (at 2:14:13 AM and 2:15:49 AM) in a span of time lasting slightly more than 90 seconds.

Subsequently, it was noted that access to a pornographic website, www.brazzersmobile.com, also occurred on June 20, 2011 at around 11:47:25 PM.¹⁶

2nd Interview of NSF Employee 1¹⁷

On September 30, 2011, Employee 1 was interviewed for a second time and told that a forensic analysis was conducted on her NSF-issued iPhone, and her husband's NSF-issued BlackBerry

¹⁵ See TAB 1. Note: NSF OIG was not able to subpoena information and determine if Employee 1 or Employee 2 has a membership with AshleyMadison.com, because the company has its headquarters office in Canada.

¹⁶ See TAB 1.

¹⁷ See TAB 11 Memorandum of Investigation (MOI) – 2nd Interview of Employee 1, dated September 30, 2011, along with a written affidavit and TAB 11A - *Weingarten* and TAB 11B - *Garrity* Warning signed by Employee 1.

and iPad. She was told that no inappropriate sites or material were found in her husband's BlackBerry or iPad.

The review of her iPhone did confirm that inappropriate sites were visited on June 17, 2011 and June 23, 2011 in the early morning hours. We explained that the sites were not accessed via any type of search engine such as Google. The sites visited were typed in and accessed directly. She was shown the log info and shown the websites that were visited and associated times. She was shown that the website for AshleyMadison.com was accessed within minutes of the porn sites. We explained that the site is used by married adults (or those in a relationship) who seek to meet and engage in affairs with other married adults (or those in relationships). She said that she did not know what the site is and denied having membership with the website. She was told that the analysis indicates that someone went to the site and went to the page where one would log on. She again denied she had membership.

Employee 1 was asked if she would provide her personal email addresses and she agreed and did so. She cooperated fully and asked if her passwords were needed, to which she was told that they were not needed at this time. She also provided a written affidavit.

2nd Interview of NSF Employee 2¹⁸

On September 30, 2011, Employee 2 was interviewed and told that a forensic analysis of his NSF-issued BlackBerry and iPad found no evidence of inappropriate sites visited. He was told that the forensic analysis of his wife's NSF iPhone indicated numerous visits to inappropriate websites, specifically early in the morning of June 17, 2011 and June 23, 2011. The review indicates site addresses were typed in rather than launched from keyword Google searches. We pointed out that in between visits to porn sites, within a couple of minutes, the website for AshleyMadison.com was visited and someone went to the login page. He said he did not know what the AshleyMadison.com site is, and said he is not a member and that he did not use his wife's iPhone to view porn sites.

Employee 2 was asked if he would provide his personal email addresses and he declined. He was asked if he would provide a voluntary written affidavit and he declined.

Review of All Websites Accessed¹⁹

A review of all sites visited determined that some non-pornographic sites²⁰ were visited less than a minute before, or directly between, the visits to pornographic websites. These sites included Facebook and Yahoo!.

On June 20, 2011, at 8:07:08 PM the mobile Facebook site was accessed, then the Craigslist site was accessed and a search for cars and trucks was conducted. A few hours later, at 11:48:05 PM, the mobile porn site www.brazzersmobile.com was accessed. Then on June 21, 2011 at

¹⁸ See TAB 12- Memorandum of Investigation (MOI) – 2nd Interview of Employee 2, dated September 30, 2011 and TAB 12A - *Weingarten* and TAB 12B - *Garrity* Warning signed by Employee 2.

¹⁹ See TAB 1A.

²⁰ See TAB 3 - List of non-pornographic sites visited.

1:12:27 AM, about 24 minutes later, the Yahoo.com website was accessed and a search conducted.

Review of Invoices and Call and Data Detail Reports for the iPhone²¹

A review of the iPhone call and data detail usage was conducted and no calls or text messages appear to have been made or received around the dates and times when inappropriate pornographic sites were visited. A review of the call data activity determined that many of the calls made and received throughout the time period of February 2011 to June 2011 appear to be of a personal nature.

Review of Ethical Conduct Rules and Regulations

The NSF Personnel Manual (Manual 14, section 143) states that:

NSF employees are expected to adhere to basis standards of integrity and decency. NSF employees must not engage in criminal, dishonest, immoral or any other conduct that is prejudicial to the Government.

Ethics regulations promulgated by Office of Government Ethics and based on the ethical principles in Executive Order 12674 state:²²

(9) Employees shall protect and conserve Federal property and shall not use it for other than authorized activities.

Furthermore, the ethics regulations also state, in pertinent part:²³

(14) Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part.

The specific regulatory standard implementing principle (9) extends the principle to misuse by others (emphasis added):²⁴

(a) Standard. An employee has a duty to protect and conserve Government property and shall not use such property, *or allow its use*, for other than authorized purposes.

OIG concludes that the two NSF employees have a duty to abide by these and other ethical conduct standards.

²¹ See TAB 13 - AT&T Invoices. TAB 13A - AT&T Call and Data Detail Reports and TAB 13B - MOI: Call Detail Report Review/Analysis.

²² 5 C.F.R. sec. 2635.101(b)(9). See also NSF Manual 15 (Conflicts of Interest and Standards of Ethical Conduct), section 3 (principle 9).

²³ 5 C.F.R. sec. 2635.101(b)(14). See also NSF Manual 15, section 3 (principle 14).

²⁴ 5 C.F.R. sec. 2635.704(a).

OIG Analysis

Based on the information contained in this report OIG concludes that the iPhone issued to NSF Employee 1 was used to visit inappropriate websites to view various pornographic videos, adult chat sites, and an adult online dating and social network services site, all inappropriate and of a sexual nature.

A forensic analysis identified 34 instances in which a total of 13 different inappropriate websites were visited. There were a total of 30 website pages accessed that contained pornographic material/videos, along with access to a phone chat site, and access to an adult online dating and social network services site but no apparent login into the site. In one instance, a government website was accessed between visits to two separate pornographic websites, all of which occurred in slightly more than 90 seconds.

Date	Time(s)	Pornographic or improper sites visited
6/17/2011	Between 1:25 AM and 1:36 AM	26 different web page visits on 11 websites: http://moviebox.com (1 visit) http://m.moviebox.com (3 visits) http://enter.mobile.moviebox.com (2 visits) http://cdn.dvdcn.com (2 visits) http://enter.brazzersmobile.com (2 visits) http://static.mofos.com (1 visit) http://m.mofos.com (1 visit) http://static.brazzers.com (2 visits) http://redtube.brazzersmobile.com (8 visits) http://redtube.phonemates.com (live private chat site – 2 visits) http://www.ashleymadison.com (adult social network site- 2 visits)
6/20/2011	11:47:25 PM	1 web page visit on 1 website: http://www.brazzersmobile.com (1 visit)
6/23/2011	Between 2:03 AM and 2:16 AM	7 different web page visits on 3 websites: http://www.redtube.com (1 visit) http://redtube.brazzersmobile.com (4 visits) http://cdn.dvdcn.com (2 visits)

According to the browser history, non-pornographic sites such as Facebook, Craigslist, and Yahoo! were also accessed, in some instances between the pornographic websites or within less than a minute of access to a pornographic site.

It is unlikely that an eight year old would seek access to a government website and review a news transmittal. It is also unlikely that an eight year old would seek access to an adult online dating and social network services site, particularly one that requires membership and payment to login.

With the above listed information, OIG has been unable to locate evidence that would prove whether Employee 1 or 2 viewed the inappropriate websites. It does appear that the evidence is

sufficient to find that Employee 1 failed to carry out her ethical duty to protect, conserve, and ensure the appropriate use of government property pursuant to the standard set forth in 5 C.F.R. section 2635.704(a). Based on the information known to her (a son who had previously used a computer to search for pornography and who probably saw pornography when visiting his father's friends with his father; [REDACTED]

[REDACTED]; and a household temporarily without a family computer), Employee 1 could reasonably have foreseen that allowing either the son or the husband to use the NSF iPhone for personal purposes could expose the device to misuse in violation of the ethics regulation and the NSF personal use policy. The casual loaning of the iPhone to either the child or the husband, or the failure to adequately secure the iPhone to prevent the use of the device by either the child or the husband without Employee 1's knowledge, amounts to a breach of Employee 1's ethical duty. Any NSF employee who allows a third party to use his or her NSF handheld device assumes the risk that the device can be misused by the third party. Employee 1, through annual IT security training, has acknowledged and agreed with the IT Security policies and "Rules of Behavior". As such, she agreed to bear responsibility for the proper use of IT resources and for the misuse of NSF IT resources, as occurred in this case.

OIG Conclusions

Employee 1 failed to safeguard government property, which resulted in its misuse in violation of federal ethics standards and NSF IT policy.

OIG Recommendations

Based on the conclusion outlined above, we recommend that the National Science Foundation proceed with administrative actions that are appropriate under HRM and IT policies to address the misconduct of Employee 1.

We also recommend that NSF evaluate the need to update the personal use policy, and to enact new policy or revise any applicable existing policy, to strengthen the guidance for employees about the use of handheld IT equipment, particularly as it relates to personal use by members of households and other third parties. Employee 1 appeared to have a very casual attitude about the use and handling of the iPhone, and its availability for personal use, and the possibility for similar events to occur with other NSF employees with such devices is a strong possibility. The opportunity for abuse under these conditions is substantial.



National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

Date: July 16, 2012

To:

From:

Subject: Counseling Memorandum

The purpose of this memorandum is to counsel you regarding your failure to properly safeguard your government issued blackberry—which resulted in the misuse of official government property—and to warn you that similar behavior will not be tolerated in the future.

On July 20, 2011, you were interviewed by the Office of the Inspector General (OIG) concerning information that you provided in connection with the misuse of your government-issued iPhone by your eight year old son. You explained that when you awoke on June 23, 2011 at or around 2:30am, you noticed the light on in your eight year old son's bedroom. You went on to say that when you entered your son's room to ask why he was awake; he attempted to block his closet door where you found your NSF iPhone on the floor. When you asked your son why he had your phone, he ran from the room and you immediately reviewed your internet history. A quick search of your phone revealed that he had potentially visited several sexually inappropriate websites.

A review of your phone by OIG confirmed several site visits to inappropriate, sexually explicit websites on three separate dates: June 17, 2011; June 20, 2011; and June 23, 2011. When asked to explain how your son would have had access to your NSF issued phone, you replied that he had probably taken it out of your purse while you were sleeping. With regard to how your son could have known the password for your phone, you explained that you sometimes allowed him to use your phone and would often enter the password before handing it to him. You mentioned the possibility that he had looked over your shoulder on one occasion and remembered your password.

Because you did not adequately secure the your NSF cell phone or safeguard its password, you failed to prevent inappropriate access to your government issued iphone, which resulted in an unauthorized user seeking obscene, pornographic, and sexually inappropriate material on a device for which you are the only authorized user. When you acknowledged and agreed with the IT Security policies and "Rules of Behavior", through the annual IT security training, you agreed to bear the responsibility for the proper use of IT resources. While I commend you for bringing this matter to the attention of OIG, I find your carelessness concerning the use and handling of your phone by members of your household troubling. Furthermore, the fact that you did not see an issue with using your IT equipment for personal calls and internet searches when questioned by OIG is also cause for concern. You should have used better judgment before this situation occurred.

As an [REDACTED], you are expected to [REDACTED] and must be cognizant of your actions, particularly any which violate (or appear to violate) NSF policy.

In the future, I expect you to be much more sensitive to your surroundings by locking and properly storing your mobile device when it is not in use. You may also want to consider if there is a need for you to take your mobile device home as often or if you can do without it some days. You are held responsible for activities on your mobile device. If you leave it unattended and someone uses it to go to on an inappropriate site, you are responsible.

This memorandum is not a disciplinary action and will not be filed in your Official Personnel Folder (OPF). The purpose of this memorandum is to counsel you regarding the inappropriateness of your recent behavior. However, you are advised that if there is a recurrence of this misconduct, I may consider initiating a formal disciplinary action against you such as a Letter of Reprimand, suspension, or removal from the Federal service.

If you are experiencing health or personal problems that may be impacting your job, I encourage you to contact the Employee Assistance Program (EAP) at 1-800-869-0276. The EAP has qualified counselors available 24 hours a day, 7 days a week who can provide expert guidance and counseling. The EAP is a confidential, free, and voluntary service. Your discussions with an EAP counselor will not be disclosed to anyone, including me, without your permission, and your participation will not be noted in your Official Personnel Folder (OPF).

If you have any questions or wish to discuss this matter further, please let me know.

[Redacted]

[Redacted]

National Science Foundation

Please sign to acknowledge receipt of this notice in the space provided below. Your signature does not indicate your agreement or disagreement with this action; it only represents receipt of this notice on the date signed. Your failure to sign will not void the content of this memorandum.

Acknowledgement of Receipt

[Redacted Signature Area]

— Signature

Date

7/20/12