



This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

MEMORANDUM

November 26, 2008

To:

(b)(7)(C)

From:

H. David Kotz
MDK
Inspector General

Re:

Referral of Report of Investigation; Case OIG-503;
Misuse of Government Computer Resources and Official Time at (b)(7)(C)

Attached is our report of investigation into misuse of government computer resources and official time (b)(7)(C)

This report is being referred to management for disciplinary action, up to and including dismissal. In order to ensure that we have the information necessary to comply with our reporting responsibilities, please advise us within 45 days what disciplinary action is taken, if any, in response to this report.

Please understand that this report is confidential in nature and should be treated in a secure manner. We request that, when you are finished with the report, you either shred it or return it to us.

If we can be of further assistance to you, please do not hesitate to contact (b)(7)(C) or me.

Attachment

cc:

(b)(7)(C)

**OFFENSIVE MATERIAL
MAY CONTAIN**

WARNING:

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

A July 2, 2003 memorandum from the Executive Director on the proper use of the Internet states, "The SBC considers inappropriate use of the Internet to be an extremely serious matter." It further provides that misuse or inappropriate use of government equipment includes, among other things, "accessing sexually explicit materials."

Government-wide Standards of Ethical Conduct

Under 5 C.F.R. § 2635.704 (Use of Government property), government employees are prohibited from using government property "for other than authorized purposes." 5 C.F.R. § 2635.705 provides that employees "shall use official time in an honest effort to perform official duties."

The Commission's Rules of the Road

The Commission's "Rules of the Road," SECRC 24-04.A01, are intended to help

employees and contractors "use the agency computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these resources to everyone within the Commission. All SBC users (i.e., Federal employees, interns, contractors, and anyone else who is granted access to SBC systems) must follow the Rules of the Road when using SBC Information Technology (IT) resources, except as described in the "Exceptions and Waivers" section...."² The Commission's Rule of the Road #2 instructs employees not to "engage in any activity that would discredit the SBC, which includes,

but is not limited to: creating, seeking, transmitting, collecting, downloading, uploading, viewing, or storing... pornographic, sexually explicit or offensive materials."

Finally, Rule of the Road #2 puts SBC employees on notice that "[t]o monitor policy compliance, assesses system performance, or conduct troubleshooting, access logs are reviewed on a periodic basis. Access logs capture the date, time, and address of sites visited by any workstation using the SBC network. Because Internet and Intranet access is for authorized users only, individuals using the system without authority or in excess of their authority may be subject to disciplinary action."³

² SECRC 24-04.A01, "SBC Rules of the Road."

³ The Commission provides IT security awareness and training to ensure that each employee is aware of policies, procedures, and guidelines related to the IT Security Program. The OIT Security Group has developed a Security Awareness and Training program in order to verify that all employees are adequately trained on their individual IT security responsibilities. The program consists of both security awareness and specialized training programs. Commission records reflect that during the same period he was viewing and storing pornography to his SBC computer hard drive, [b] successfully completed the 2008 IT Cybersecurity Awareness Training, on August 25, 2008. [b] also successfully completed the Rules of the Road Courses and Certifications On April 5, 2006 and May 16, 2007. See attachment A.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

Relevant Case Law

The Merit Systems Protection Board (MSPB or Board) has previously found that disciplinary action for an employee's misuse of a government computer to view pornography is warranted to promote the efficiency of the service. *See, e.g., Johnson v. Dep't of Veterans Affairs*, 2007 MSPB LEXIS 190 (M.S.P.B. Jan. 10, 2007); *Martin v. Dep't of Transportation*, 103 M.S.P.R. 153 (2006); *Quillen v. Dep't of Treasury*, 96 M.S.P.R. 154 (2004), *aff'd without op.*, 134 Fed. Appx. 449 (Fed. Cir. 2005). For example, in *Johnson*, 2007 MSPB LEXIS 190 at *2, the Board upheld the removal of a supervisory auditor who engaged in inappropriate internet usage, including accessing numerous internet sites containing sexually explicit photographs and other materials. The employee's misuse occurred during periods when he should have been engaged in agency business and was in violation of his employer's computer security policy. *Id.* The Board observed that, in selecting the penalty of removal, the deciding official had considered the following factors: "[t]he appellant's offense was serious; it occurred both before and after his appointment to a supervisory position; his misconduct reflected poorly on his judgment; and it negatively impacted the employer-employee relationship"

Results of the Investigation

I. Analysis of the Logs and Forensic Analysis

Our review of (b)(7) internet usage log for the 17 business-day period from August 11, 2008 to September 2, 2008 disclosed that he received approximately 1880 access denials for pornographic websites including, among others, www.tgirlhotspot.com, www.ladyboyjuice.com, www.ladyboys-xxx.com, www.trannyit.com, www.anal-sims.com, and www.fuck-my-wife.com. These access denials were received during (b)(7) normal work hours.

The OIG's analysis of the websites that (b) attempted to access on his SEC computer revealed several images of transgendered women. There were numerous images of what appeared to be transgendered women performing sex acts.⁴ The OIG also reviewed the images retrieved by OIT Security as having been stored on the hard drive of (b)(7) SEC computer under "My Documents." These images were of transgendered women, some performing sex acts.

II. (b)(7) Sworn Testimony

The OIG took (b)(7) sworn, on-the-record testimony on November 7, 2008. (b) admitted under oath that he used his SEC-assigned computer to access and attempt to access Internet web sites containing pornography and other sexually explicit material

⁴ Because of the extremely graphic nature of these images and the ones obtained from his computer, we are not attaching them to the report, but will make them available upon request.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

during work hours. Testimony Transcript of (b)(7)(X) (b)(7)(X) attached hereto as Exhibit B, at p. 24. (b)(7)(X) recalled trying to access a web site and having it blocked due to pornography "numerous times." Id. at 15. (b)(7)(X) also testified that he saved numerous images to the hard drive of his SEC computer, and that he considered the images to be pornographic in nature and inappropriate for work. Id. at 21, 23-24. (b)(7)(X) acknowledged that he viewed these saved images from time to time during work hours. Id. at 24.

(b)(7)(X) testified that he looked at pornography sometimes up to twice a day, and that it was a "fairly frequent occurrence." Id. at 22-23. When asked how long he has been viewing pornography at work, (b)(7)(X) replied that it had "probably occurred for a long time," that his usage was "cyclical in nature" and that his increased attempts to access pornographic materials on his SEC computer were proportionately related to the increase of the stress of his job. Id. at 24-25. (b)(7)(X) testified:

It's kind of one of those things where I felt really stressed, and it was kind of there. And I, you know, I guess I didn't necessarily have the self-control not to look at it.

Id. at 21-22.

(b)(7)(X) further admitted that there were times when his searching for and viewing pornography during work hours may have interfered with his work, causing him to bring work home. Id. at 26-27.

(b)(7)(X) acknowledged that in attempting to access pornographic and sexually explicit materials on the internet, he turned off and/or lowered the protection on the search filter on www.MSN.com, and he had also done so on www.Yahoo.com before doing so was prevented by OIT. Id. at 29. (b)(7)(X) admitted that he had personal accounts with pornographic websites, and stated that he did not recall accessing those personal accounts from his SEC computer, but if he did, it was once or twice over his entire work history with the Commission. Id. at 30. (b)(7)(X) also acknowledged that he accessed pornography from his SEC computer while on travel. Id. at 32.

(b)(7)(X) denied that anyone else at the SEC was aware that he was accessing pornography. Id. at 30. (b)(7)(X) however, acknowledged that although he was in a private office, it would be possible for someone to see the pornographic images on his computer screen if the door was open. Id. at 32. (b)(7)(X) stated that he could not recall viewing pornographic material with his office door open. Id. at 31.

(b)(7)(X) testified that he was aware of the standards of ethical conduct governing the use of government property and official time. Id. at 34. (b)(7)(X) testified that he was aware that the materials he was searching for and viewing on his SEC computer were pornographic in nature and were inappropriate for work. Id. at 23. (b)(7)(X) apologized for viewing this material. Id. at 36.

This document is subject to the provisions of the Privacy Act of 1974, and may require redaction before disclosure to third parties. No redaction has been performed by the Office of Inspector General. Recipients of this report should not disseminate or copy it without the Inspector General's approval.

III. Interview of [redacted]

In connection with this investigation, [redacted] supervisor, [redacted] was interviewed on November 18, 2008. [redacted] described [redacted] [redacted] Notes of Interview of [redacted] attached hereto as Exhibit C at p. 1. [redacted] was unaware that [redacted] had been using his SBC computer to view inappropriate material, but noted that [redacted] does spend time playing video games on his SBC computer. *Id.* However, [redacted] stated that he considered [redacted] sophisticated computer skills to be an asset to the office, and that in this regard [redacted] has "contributed greatly" to the data analysis work done by the office. *Id.*

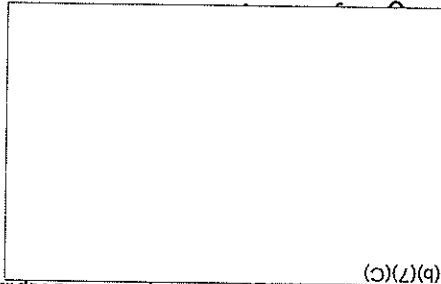
IV. Review of [redacted] OHR Files

A review of [redacted] OPF and his conduct file revealed that he had no prior disciplinary actions. Our examination of his time and attendance records did not reflect any unusual absences from work. [redacted] most recent Standard Form 50 indicated that he is a [redacted] [redacted] [redacted] [redacted]

Conclusion

The evidence established that [redacted] inappropriate use of the Internet violated Commission policy and rules. This is a serious matter – one which could have easily discredited the SBC. The matter is being referred to [redacted] the Associate Executive Director for Human Resources, the Associate General Counsel for Litigation and Administrative Practice, the Ethics Counsel, and the Director of the Office of Equal Employment Opportunity for disciplinary action, up to and including dismissal.

Submitted:



Concur:

Date:

11/20/08

Date:

Nov. 26, 2008

Approved:

[Signature]

Date:

November 26, 2008

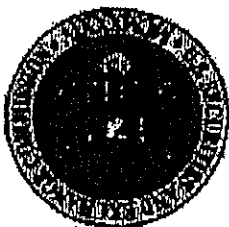
H. David Kotz



A



U.S. Securities and Exchange Commission



Course Developed by:

Foreign Service Institute
U.S. Department of State

This certificate is awarded to:

(b)(7)(c)

on August 25, 2008

In recognition of successful completion of Cybersecurity Awareness.

This certificate also is used as an acknowledgement of your agreement to comply with the SEC "Rules of the Road" as part of your annual IT Security Awareness and Training. You further certify that you understand your responsibilities regarding access and use of SEC IT resources as set forth in the "Rules of the Road" and Cybersecurity Awareness and affirm that you will comply with the statements, terms, and conditions set forth therein. You understand that violating these responsibilities may lead to revocation of your network access and/or disciplinary action.

Certification Number: (b)(7)(c)

Version 3.1, SEC.1



Re: IT Training Certification

(b)(7)(C)

From: (b)(7)(C)

Sent: Wednesday, November 05, 2008 3:51 PM

To: (b)(7)(C)

Subject: RE: IT Training Certification

Importance: High

Attachments: (b)(7)(C)

As requested, here is the training data for 2008, 2007 and 2006 for (b)(7)(C) (b)

208 Cyber Security Awareness Training Certification Information: Expiration Date - 08/25/2009 12:50:16 PM					
Registration Date:	08/25/2008	Course Start Date:	08/25/2009	Course Completion Date:	08/25/2008
Exam Start Date:	08/25/2008 12:50:22 PM	Exam Completion Date:	08/25/2008 12:51:56 PM	Exam Attempt(s):	1

Email History:		Subject		Email Date		System	
(b)(7)(C)		Cyber security Awareness Invitation		07/19/2008 10:00:23 AM		System	
(b)(7)(C)		Cyber security Awareness Reminder		08/09/2008 10:01:51 AM		System	
(b)(7)(C)		Cyber security Awareness Reminder		08/24/2008 10:00:57 AM		System	

Exam History:							
Registration Date	08/25/2008	Exam Version	5	Exam Attempt	1	Start Date	08/25/2008 12:50:22 PM
End Date	08/25/2008 12:51:55 PM	Exam Score	10/10	Exam Passed	Y		

Login History:		Email Address		Login Date	
(b)(7)(C)		(b)(7)(C)		08/25/2008 12:19:42 PM	

2007 SEC IT Security Awareness and Training data call for - (b)(7)(C)							
Certificate ID	8157	Email Address	(b)(7)(C)	FIRSTNAME	(b)(7)(C)	LASTNAME	(b)
Course ID	ROR2007	Date of Comp	5/16/2007	Course Name	Rules of the Road Certification	Division/Company Id	(b)(7)(C)
Course	Refreshers Course	Course	2007	Course	2007	SEC G	
Certificate ID	8163	Email Address	(b)(7)(C)	FIRSTNAME	(b)(7)(C)	LASTNAME	(b)
Course ID	UPDATE07	Date of Comp	5/16/2007	Course Name	Refreshers Course	Division/Company Id	(b)(7)(C)
Course	Refreshers Course	Course	2007	Course	2007	SEC G	

Re: IT Training Certification

2006 SEC IT Security Awareness and Training data call for - (b)(7) (b)(7)(C)

Certificate ID	Email Address	FIRSTNAME	LASTNAME	Course ID	Date of Comp	Course Name	Division / Office	Compan Id
11235	(b)(7)(C)	(b)(7)	(b)	ROR2006	4 /5 /2006	Rules of the Road, Part 1 of 4	(b)(7)(C)	SEI
11239	(b)(7)(C)	(b)(7)	(b)	CSB2006	4 /5 /2006	Computer Security Basics, Part 2 of 4	(b)(7)(C)	SEI
11241	(b)(7)(C)	(b)(7)	(b)	UR2006	4 /5 /2006	User Responsibilities, Part 3 of 4	(b)(7)(C)	SEI
11242	(b)(7)(C)	(b)(7)	(b)	GCSP2006	4 /5 /2006	Good Computer Security Practices, Part 4 of 4	(b)(7)(C)	SEI

Respectfully,

Principal
 Information Assurance Division
 Security & Systems Engineering Services
 SRA International, Inc
 (b)(7)(C)

From: (b)(7)(C)
 Sent: Wednesday, November 05, 2008 3:23 PM
 To: (b)(7)(C)
 Subject: RE: IT Training Certification

I don't have access to it but I can get it.

Please provide the cert for (b)(7)(C) for 2007. Please make this a priority. Thanks.

U.S. Securities and Exchange Commission
 Office of Information Technology Security
 (b)(7)(C)



B

