

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

---

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY  
SERVICE**



**INSPECTOR GENERAL**

**REPORT OF INVESTIGATION**

**5 September 2014**

**IV-14-0056**

**Misuse of Government Resources**

**WARNING: THIS REPORT MAY CONTAIN GRAPHIC IMAGES  
AND/OR LANGUAGE**

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Approved for Release by NSA on 05-31-2019, FOIA Case # 79204 (litigation)

Release: 2019-05

NSA:08349

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

## **(U) OFFICE OF THE INSPECTOR GENERAL**

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

### **(U) AUDITS**

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

### **(U) INVESTIGATIONS**

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

### **(U) INTELLIGENCE OVERSIGHT**

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

### **(U) FIELD INSPECTIONS**

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

**I. (U) SUMMARY**

(b) (3) - P.L. 86-36  
(b) (6)

(U//~~FOUO~~) On 22 January 2014 the Inspector General (IG) received a referral from the NSA/CSS Associate Directorate of Security and Counter Intelligence (ADS&CI) identifying potential computer misuse by an NSA/CSS contractor, [REDACTED]. On 7 March 2014, the IG initiated an investigation of [REDACTED] use of NSA/CSS Information Systems (ISs). We obtained sworn testimony from [REDACTED]. We also obtained NISIRT records relating to his use of Government resources.

(U//~~FOUO~~) The preponderance of the evidence collected during the investigation substantiates that [REDACTED] misused his unclassified NSA/CSS IS. [REDACTED] used Government resources to access pornographic websites in violation of NSA/CSS Policies 6-4 and 6-6 and the Alaska Language Center (ALC) Computer Network User Agreement. [REDACTED] billed the Government contract for the time he spent viewing pornography, an additional violation of NSA/CSS Policy 6-4. [REDACTED] admitted in testimony that he streamed non-work related material on the unclassified IS in violation of NSA/CSS policy 6-6.

(U//~~FOUO~~) A summary of the findings will be forwarded to the Maryland Procurement Office; Contractor Clearances, ADS&CI; and Special Actions, ADS&CI for review and any action deemed appropriate.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

## II. (U) BACKGROUND

(b) (3) - P.L. 86-36

(b) (3) - P.L. 86-36  
(b) (6)

### (U) Introduction

(U//~~FOUO~~) [redacted] is a contractor affiliate with [redacted] assigned to Associate Directorate for Education and Training (ADET) as a [redacted] at the Alaska Language Center (ALC). He is working under contract number [redacted] on the [redacted] program.

(U//~~FOUO~~) On 21 January 2014, the Alaska Mission Operation Center Information Assurance (AMOC/IA) office notified their security office that [redacted] was suspected of accessing pornographic websites. The unclassified account is on a commercially provided network routed through [redacted]. The EAFB Communications Squadron notified the AMOC/IA office that a number of suspected pornographic website URLs were discovered on [redacted] and listed under [redacted] account.

(b) (6)

### (U) Applicable Authorities

(U//~~FOUO~~) NSA/CSS Policy 6-4, "CONTRACTOR USE OF NSA/CSS INFORMATION SYSTEMS," issued 22 October 2013.

(U//~~FOUO~~) NSA/CSS Policy 6-6, "USE OF UNCLASSIFIED INFORMATION SYSTEMS SUCH AS THE INTERNET," revised 15 October 2013.

(U) See Appendix A for the full text of the applicable authorities.

(b) (3) - P.L. 86-36  
(b) (6)

### III. (U) FINDINGS

(U//~~FOUO~~) Did [redacted] an NSA/CSS contractor, misuse his unclassified NSA/CSS IS to access pornographic websites in violation of NSA/CSS Policies 6-4 and 6-6?

(U//~~FOUO~~) CONCLUSION: **Substantiated.** The preponderance of the evidence supports the conclusion that [redacted] misused his unclassified NSA/CSS IS. [redacted] accessed pornographic websites in violation of NSA/CSS Policies 6-4 and 6-6, and the ALC Computer Network User Agreement. [redacted] billed the Government contract for the time he spent viewing pornography, an additional violation of NSA/CSS Policy 6-4. [redacted] admitted in testimony that he streamed non-work related material on the unclassified IS in violation of NSA/CSS policy 6-6.

#### (U) Documentary Evidence

(b) (3) - P.L. 86-36

(U) Security Incident Write up: Email dated 21 January 2014 sent from [redacted] to Q23

(U//~~FOUO~~) On 21 January 2014, the EAFB Communications Squadron notified the AMOC/IA office that a number of suspected pornographic website URLs were discovered on [redacted] and listed under [redacted] account. The AMOC/IA office notified the site's special security officer. [redacted] was interviewed by the special security officer and he admitted to accessing 'adult pornography' sites on the unclassified network during the afternoon of 20 January 2014. He claimed this incident was the first and only time he accessed pornography from a Government computer. He viewed the images online but denied downloading files to the Government computer. [redacted] knew at the time his actions were against policy and struggled to stop. Over the course of a couple hours, he viewed numerous different pornography sites (more than 10 sites). During this period of misuse, [redacted] would stop and re-focus on work, but then found himself drawn back to view the pornography. He contemplated walking away from the computer terminal altogether in effort to stop but was overcome by his desire to view pornography.

(U) See Appendix B for the full text of email referral.

#### (U) Alaska Language Center (ALC) Computer Network User Agreement

(U) On [redacted] [redacted] signed the user agreement which states "I understand that I am not to access or attempt to access Internet sites that portray or promote pornographic images or text. Such accesses or attempts thereof constitute a violation of policy. Accessing or attempting to access such sites will result in a formal report to the Office of the Inspector General."

(U) See Appendix C for a copy of the signed user's agreement.

(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

**(U) Testimonial Evidence**

(b) (6)

(U) On 20 February 2014, [redacted] was interviewed, by telephone, and provided the following sworn testimony:

(U//FOUO) [redacted] checks his personal email account and completes his timesheet using the unclassified Government IS. He stated that his personal email use is very minimal. He also admitted to listening to classical music by using Google to search for different classical artists then playing YouTube music videos while working. [redacted] claimed that he researched material [redacted] and sometimes listened to music or videos in that language. On 20 January 2014, [redacted] admitted to accessing adult pornography websites and viewed multiple adult pornography images. It was the Martin Luther King holiday and he was in the office alone (a rare occurrence). He clicked on links found on websites to view images from various sources but did not remember what actions he performed that resulted in him initially viewing pornographic images. [redacted] viewed pornography intermittently for approximately 2 hours that day. He would view pornographic images then would stop, redirect himself and go back to work. [redacted] claimed that this was the only time he ever engaged in this type of activity at work. He billed his time to the Government contract. [redacted] knew viewing pornography on a Government system was not allowed.

(b) (3) - P.L. 86-36  
(b) (6)**(U) Analysis and Conclusions**

(U//FOUO) Contractor's use of Agency IS for personal use is extremely limited. [redacted] use of resources to access and view pornography was not authorized by contract, and it clearly reflects negatively on the Agency as described in NSA/CSS Policy 6-4. The fact that [redacted] billed the Government contract for the time spent viewing pornography is an additional violation of NSA/CSS Policy 6-4.

(U) According to the AMOC/IA office, the incident was a onetime isolated event. Site security was immediately notified of the incident (the next day) and [redacted] was interviewed. [redacted] admitted he viewed pornography on a Government system and billed the time he spent viewing the pornographic images to the Government contract. [redacted] knew he was not allowed to view pornography on a Government system.

(U//FOUO) [redacted] use of the NSA/CSS IS also violated Policy 6-6. [redacted] actions to view pornographic images demonstrated a lack of good judgment and common sense. Additionally, [redacted] admission that he streamed non-work related media (classical music) is an additional violation of NSA/CSS Policy 6-6.

(U//FOUO) Lastly, [redacted] violated his computer network user agreement when he accessed pornographic images. The user agreement specifically stated that attempting or assessing "Internet sites that portray or promote pornographic images or text" will be a violation of policy and would be reported to the OIG.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

*IV-14-0056*

(U) Documentary evidence, combined with [redacted] own testimony, supports the conclusion that he misused his unclassified NSA/CSS IS to view pornography.

⋮

(b) (3) - P.L. 86-36  
(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

**IV. (U) RESPONSE TO TENTATIVE CONCLUSION(S)**

(b) (3) -P.L. 86-36  
(b) (6)

(U//~~FOUO~~) [redacted] was provided the tentative conclusions on 19 August 2014. On 4 September 2014, he responded stating:

The report conclusion is accurate concerning the one-time incident of the misuse of an unclassified NSA/CSS computer. This incident never occurred prior and has not and will not occur ever again. I regret and feel ashamed of such behavior as it contradicts my personal and professional values, ethics, and morals.

Furthermore, I understand my responsibility regarding the use and protection of government computer systems and the oath that I took to safeguard and use it properly. I renew this commitment to do so with no reservations.

Please, consider my otherwise clean record and trustworthy character. This is not a pattern of behavior or activity that is part of my work or personal life. It was a one-time incident and a mistake that I regret and will never return to.

Thank you for your time and consideration in this matter.

(U//~~FOUO~~) The conclusion of this investigation remains unchanged.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

### V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused his unclassified NSA/CSS IS. [redacted] accessed pornographic websites in violation of NSA/CSS Policies 6-4 and 6-6 and the ALC Computer Network User Agreement. [redacted] billed the Government contract for the time he spent viewing pornography which is an additional violation of NSA/CSS Policy 6-4. [redacted] also violated NSA/CSS policy 6-6 by streaming non-work related media (classical music) on the unclassified IS.

[redacted]  
(b) (3) - P.L. 86-36  
(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

### VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A summary memorandum will be provided to the Maryland Procurement Office; Contractor Clearances, ADS&CI and Special Actions, ADS&CI for review and any action deemed appropriate.

[Redacted Signature]

Senior Investigator

(b) (3) - P.L. 86-36

Concurred by:

[Redacted Signature]

Deputy Assistant Inspector General  
For Investigations

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

## APPENDIX A

### (U) Applicable Authorities

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**(U//~~FOUO~~) NSA/CSS Policy 6-4, "CONTRACTOR USE OF GOVERNMENT INFORMATION SYSTEMS," Policy Section (dated 22 October 2013):**

1. (U) Contractors shall only use NSA/CSS ISs to perform tasks that are authorized by contract, approved by the Contracting Officer (CO), and permitted by this policy.

[...]

8. (U) Contractors shall not use NSA/CSS ISs or telephone services for personal use except for brief, infrequent communications to deal with urgent matters. This limited exception to the personal use prohibition applies only when:

- a. (U) Unavoidable personal matters arise such as, but not limited to, contacting a spouse, dependent family member, or other individuals responsible for a dependent's care; scheduling a physicians appointment; or vehicle maintenance;
- b. (U) The communication does not adversely affect the NSA/CSS mission or reflect poorly on NSA/CSS;
- c. (U) The communication does not result in other than minimal expense to the Government (e.g., the call is local, toll-free);
- d. (U) Time spent using the NSA/CSS IS or resource is not billed to the contract; and
- e. (U) The use is not associated with personal business activities outside the scope and purpose of the contract.

[...]

**(U//~~FOUO~~) NSA/CSS Policy 6-6, "USE OF UNCLASSIFIED INFORMATION SYSTEMS SUCH AS THE INTERNET," Responsibilities Section (revised 15 October 2013):**

25. (U) All Users shall:

[...]

n. (U) Use good judgment and common sense when accessing and/or communicating on unclassified ISs;

[...]

**(U) Annex - Prohibited Applications**

(U) The following applications are prohibited for other than work-related purposes:

[...]

4. (U) Streaming media

[...]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

**APPENDIX B**  
**(U) Email referral**

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

**From:** [redacted]  
**Sent:** Wednesday, January 22, 2014 2:08 PM  
**To:** [redacted]  
**Cc:** [redacted]  
**Subject:** FW: (U) Misuse of IT System - Contractor (AMOC [redacted])  
 Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

[redacted]  
 Could you please review the following and let me know if this is something you would look into? Due to the system he was on, I was unsure if this would be able to be reviewed by the IG.  
 Thanks, [redacted]

[redacted]

This email may contain information protected by the Privacy Act of 1974

(b) (3) - P.L. 86-36

**From:** [redacted]  
**Sent:** Wednesday, January 22, 2014 1:54 PM  
**To:** [redacted]  
**Cc:** [redacted]  
**Subject:** FW: (U) Misuse of IT System - Contractor (AMOC [redacted])  
 Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Hi [redacted] sent this to [redacted] but I am not sure if he got it as there is something weird about the date of the message so I have copied him as well - please see below. [redacted] told me that he walked this guy out of the SCIF and took his badge yesterday for viewing pornography on NSA computers.

[redacted]

\*\*\* PRIVACY SENSITIVE. This e-mail contains information protected by the Privacy Act. Any misuse or unauthorized access may result in disciplinary action. \*\*\*

**From:** [redacted]  
**Sent:** Wednesday, January 22, 2014 1:43 PM  
**To:** [redacted]  
**Subject:** FW: (U) Misuse of IT System - Contractor (AMOC [redacted])

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

IV-14-0056

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

FYSA.

From: [redacted]  
 Sent: Wednesday, January 22, 2014 4:16 PM  
 To: [redacted]  
 Cc: [redacted]  
 Subject: RE: (U) Misuse of IT System - Contractor (AMOC [redacted])  
 Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

[redacted] Please see e-mail below.

From: [redacted]  
 Sent: Tuesday, January 21, 2014 8:01 PM  
 To: [redacted]  
 Cc: [redacted]  
 Subject: (U) Misuse of IT System - Contractor (AMOC [redacted])  
 Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (3) - P.L. 86-36

We had a security incident involving one of the [redacted] contractors providing language instruction at the Alaska Language Center. Please see the below write-up of the incident. Also included is the original approval for access from [redacted] dated Apr 2012. I see [redacted] has moved offices, so I'm sending this to you for your information/action. Please forward as required.

SUBJECT: [redacted]  
 Unit of Assignment: Alaska Language Center (ALC) located at the Alaska Mission Operations Center (AMOC)  
 Nature of Concern: Misuse of Government Information Technology Systems - Accessing Pornography  
 Date of Event: 20 January 2014  
 Date event reported: 21 January 2014

(b) (3) - P.L. 86-36  
(b) (6)

(U//~~FOUO~~) Background:

- On 21 Jan 14, the AMOC Information Assurance (IA) office notified the security office that SUBJECT was suspected of accessing pornographic websites using [redacted] account in his name.
  - o The account is on a commercially provided lowside network routed through the [redacted]
  - o The EAFB Communications Squadron notified the AMOC IA office that a number of suspected pornographic website URLs were discovered on [redacted] and listed under SUBJECTS account data.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

- A review of Account User Agreement documents on file in the IA office disclosed SUBJECT read and signed an agreement not to access pornography sites from government IT systems.
- The [redacted] elected to restrict SUBJECT from further access to the AMOC SCIF, pending the results of investigation and security determinations.
  - o [redacted] SUBJECT's SCIF access badge was withdrawn, and he was provided a new badge limiting his access.
  - o SUBJECT's NSAnet, NIPRnet, and [redacted] accounts were disabled.
  - o IA removed the laptop SUBJECT used, and provided it to the security office for safekeeping.
  - o SUBJECT is able to access the AMOC Compound and his office space in the unclassified area of the ALC (outside the SCIF).
  - o SUBJECT [redacted] in the ALC.
- At the time SUBJECT's SCIF access badge was withdrawn, he asked to 'openly discuss' the matter with the security representative.
- No publicity is expected to occur.

(b) (6)

(b) (3) - P.L. 86-36

(U//~~FOUO~~) SUBJECT verbally provided essentially the following: He admitted to accessing 'adult pornography' sites using his [redacted] account on the unclassified commercial network in the afternoon of 20 Jan 14. He's had an off & on desire to view pornography on the internet for several years, and asserted while he's accessed pornography from his personal computer, the incident on 20 Jan 14 was the first [and only] time he accessed pornography from a government computer. He viewed the images online, and didn't download any files to the computer. He knew at the time his actions were against policy, yet he struggled within himself to stop. Over the course of a couple hours, he viewed many different pornography sites (more than 10). During this period, he would stop and re-focus on work, but then soon find himself drawn back to view the pornography again and again. He contemplated walking away from the computer terminal altogether in effort to stop, but was overcome by desire.

(U//~~FOUO~~) Security Representative Notes: SUBJECT openly discussed this matter in detail, and seemed genuinely sorry and ashamed of his behavior. He was very cooperative, and didn't attempt to deny or avoid taking responsibility in any way. He claimed he felt compelled to self-report before it was discovered, but didn't for unknown reasons. He desires to continue to be forthright and honest to see this matter through.

(U) Please let me know if you have any questions.

V/r

[redacted]

(U//~~FOUO~~)

[redacted]

[redacted]  
 Alaska Mission Operations Center  
 Elmendorf AFB, Alaska  
 NSTS: 654-6530



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

*IV-14-0056*

**APPENDIX C**

**(U) ALC User Agreement**

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

(b) (3) - P.L. 86-36  
(b) (6)

(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**ALASKA LANGUAGE CENTER (ALC) COMPUTER NETWORK USER AGREEMENT**

The instructor  is assigned the following username

As a user of the ALC computer network, I acknowledge my responsibility to conform to the following requirements and conditions established by  Standard Operating Procedure for Computer Security. I understand that failure to sign this acknowledgment will result in denial of access to the ALC computer system.

I understand that the ALC computer network is an unclassified system. I will NOT introduce, store, pass or process classified data on it.

I understand the need to protect my password and any other system passwords. I will NOT share my password and/or account or use anyone else's password.

I understand that the ALC computer network is to be used for unclassified open source research and may not be used for intelligence gathering activities.

I understand that I am not to access or attempt to access Internet sites that portray or promote pornographic images or text. Such accesses or attempts thereof constitute a violation of policy. Accessing or attempting to access such sites will result in a formal report to the Office of the Inspector General.

I understand I am responsible for all actions taken under my account. I will not attempt to hack, crack, or gain unauthorized access to the ALC network or any other network or computer on the Internet, or to gain access to data for which I am not specifically authorized, or exceed the scope of any authorized access granted.

I understand that it is my responsibility to maintain the non-attributional status of the ALC network. I agree to not give out my ALC account name.

(b) (3) - P.L. 86-36

I acknowledge my responsibility to use the ALC computer network only for official government business as an obligation under the Standards for Ethical Conduct of Employees of the Executive Branch 5 CFR Part 2635 dated 2 August 1992 and DOD Directive 5500.7 "Joint Ethics Regulation", DOD 5240.1-R "Procedures Governing the Activities of DOD Intelligence Components That Affect U.S. Persons" and any subsequent revisions.

I acknowledge my responsibilities under NSA/CSS Regulation 10-63 "NSA/CSS Prepublication Review Procedure" ensuring that protected information is not publicly disclosed and reporting suspected violations of this regulation.

I understand that in an attempt to keep the ALC computer network non-attributional, that I must not access any account requiring a log-in and password.

I understand that I am NOT to use the ALC computer network to attempt to post to any outside Internet newsgroup, that I am not to sign web visitor logs, send web feedback, register for any service or function, subscribe to any service or in any other way use this account to attempt to make active postings or feedback.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~202712~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

I acknowledge my responsibility NOT to run any unauthorized software on the ALC computer network, and that any software downloaded from the Internet is subject to the procedures outlined in NSA/CSS Regulation 130-2 "Computer Virus Prevention Policy".

I agree not to transfer magnetic media between the ALC computer network and any internal NSA system without going through the proper computer security procedures.

I understand that all NSA/CSS Telecommunications and Automated Information Systems and related equipment are for the communication, transmission, processing and storage of U.S. Government information only. These systems and equipment are subject to monitoring to ensure proper functioning, and to protect against improper or unauthorized access, and to verify the presence or performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored on this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel. I expressly consent to such monitoring. I understand that the System Administrator and Computer Security Officer, or their designees, are responsible for such monitoring.

I acknowledge my responsibility to conform to the requirements set forth in this agreement. I acknowledge that I will abide by all policies as set forth in NSA/CSS manual 130-1 and NSA/CSS Regulations 130-2.3.05 and the Operations Directorate Internet Access Policy. I also acknowledge that failure to comply with these SOPs may constitute a security violation resulting in denial of access to ALC computer network and that such violations will be reported to appropriate authorities for further action as deemed appropriate.

By signing this document, you acknowledge and consent that when you

Access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.
- You consent to the following conditions:
  - The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations. At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.
  - Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.
  - Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.
  - Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and may be modified or eliminated at the government's discretion.

Printed Name:   
Signature:

Date:  (b) (6)

(b) (3) - P.L. 86-36  
(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056

**APPENDIX D**

**(U) Sample of pornographic images [redacted] viewed on 21 January 2014**

[redacted]  
⋮  
[redacted]  
(b) (3) - P.L. 86-36  
(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056



ACCESSED SITE. DATE TIME



ACCESSED SITE DATE TIME



ACCESSED SITE DATE TIME



ACCESSED SITE DATE TIME



(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-14-0056



ACCESSED SITE . . . . . DATE TIME



(b) (6)

ACCESSED SITE DATE TIME



ACCESSED SITE DATE TIME



ACCESSED SITE DATE TIME



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~