

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY
SERVICE**



INSPECTOR GENERAL

REPORT OF INVESTIGATION

7 June 2013

IV-13-0017

Computer Misuse

This is a PRIVILEGED DOCUMENT. Further dissemination of this report outside of the Office of Inspector General, NSA, is PROHIBITED without the approval of the Assistant Inspector General for Investigations.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Approved for Release by NSA on 03-30-2018, FOIA Case # 79204 (litigation)

~~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-13-0017

I. (U) SUMMARY(b) (3) - P.L. 86-36
(b) (6)

(U//~~FOUO~~) On 10 October 2012, the IG received a referral from the NSA/CSS Information Systems Incident Response Team (NISIRT), identifying potential computer misuse by an NSA contractor. On 15 November 2012, the IG opened an investigation on [redacted] an [redacted] contractor working under contract number [redacted] alleging the misuse of an NSA Information System (IS) and U.S. Government resources in September and October 2012. The preponderance of the evidence collected during the investigation substantiated that [redacted] misused his IS and U.S. Government resources to access adult oriented material, to stream music and to view non-work related videos in violation of NSA/CSS Policies 6-6 and 6-4.

(U//~~FOUO~~) [redacted] was also involved in a prior OIG misuse case. In 2006, [redacted] was detected accessing adult oriented material on the internet. The OIG wrote a summary report of investigation, dated 5 May 2006, and provided that report to [redacted] and the Associate Director for Security and Counterintelligence (ADS&CI). Due to the second detection, the OIG suspended [redacted] Unclassified internet account and access.

(U//~~FOUO~~) Finally, during the course of the investigation, [redacted] confessed to having committed security violations involving computer hardware in April 2013 (See Section III, Interview). This matter is referred to ADS&CI for action as appropriate.

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

Personnel Privileged Information
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Release: 2018-04
NSA: 02717

II. (U) BACKGROUND

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

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

(U) Introduction

(U//FOUO) [redacted] is a contractor affiliate with [redacted] working under contract number [redacted]

(U//FOUO) NSA/CSS Information Systems Incident Response Team (NISIRT) reviewed [redacted] unclassified U.S. Government accounts from 20 September 2012 to 4 October 2012. NISIRT detected misuse on the unclassified account 20 - 21 September 2012, 24 - 28 September 2012 and 1 - 4 October 2012. The NISIRT assigned tracking number [redacted] to this violation. NISIRT provided the activity report to the Office of the Inspector General on 10 October 2012.

(U//FOUO) This is the second computer misuse offense committed by [redacted]. He was previously found to have violated NSA/CSS 6-4 and 6-6 in 2006. The OIG summary report can be found at attachment 1. Due to the second detection, the OIG suspended [redacted] Unclassified internet account and access.

(U) Applicable Authorities

(U//FOUO) NSA/CSS Policy 6-6, "USE OF UNCLASSIFIED INFORMATION SYSTEMS SUCH AS THE INTERNET," revised 20 June 2012:

25. (U) All Users shall:

[...]

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

[...]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0017

(U//~~FOUO~~) NSA/CSS Policy 6-4, "CONTRACTOR USE OF NSA/CSS INFORMATION SYSTEMS," revised 7 June 2007:

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

4. (U) Contractors shall not make personal use of NSA/CSS ISs except for brief, infrequent communications to take care of unavoidable personal matters (e.g., contacting a spouse, dependent, or individual responsible for a dependent's care; scheduling a physician's appointment or car maintenance; etc.). This limited exception to the personal use prohibition applies only when:
 - a. (U) The communication could not have reasonably been made at another time (e.g., the physician is only available during working hours);
 - b. (U) The communication does not adversely affect the Agency mission or reflect poorly on the Agency;
 - c. (U) The communication does not result in other than minimal expense to the Government (e.g., the call is local, toll-free, or charged to a personal telephone calling card);
 - d. (U) Time spent using the NSA/CSS IS for personal use is not billed to the contract; and
 - e. (U) The personal communication is of a non-commercial nature. This exception does not permit the use of NSA/CSS ISs in conjunction with a contractor employee's personal business activity.

....

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

III. (U) FINDINGS

(U//~~FOUO~~) Did [redacted] an [redacted] contractor [redacted] misuse his Agency IS and U.S. Government resources in violation of the NSA/CSS Policies 6-6 and 6-4?

(U//~~FOUO~~) CONCLUSION: **Substantiated.** The preponderance of the evidence supports the conclusion that [redacted] misused his Agency IS and U.S. Government resources. [redacted] used the Government resources to access adult orientation material, to stream media and to view non-work related videos in violation of NSA/CSS Policies 6-6 and 6-4.

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

(U) Evidence: NISIRT Analysis

(U//~~FOUO~~) NISIRT provided the OIG with an analysis of [redacted] activities on the unclassified NSA/CSS Information System (IS). [redacted] was observed accessing adult oriented material, streaming media and watching non-work related videos. The full NISIRT report can be found at attachment 2.

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

(U) Interview

(U//~~FOUO~~) On 14 May 2013, the OIG interviewed [redacted] admitted to performing non-work related activities on the unclassified network for 2 hours per workday for the last 5 years. [redacted] admitted to conducting inappropriate internet activity to include accessing sport news, music and personal emails. He also admitted to performing searches for adult oriented material. He has received [redacted] blocking him from pornography websites and admitted that he would continue to try other sites. [redacted] admitted that he knew that his activity is against policy.

(U//~~FOUO~~) During questioning [redacted] initially stated he had no prior security incidents but later admitted to having multiple incidents the month prior. The security incidents involved [redacted]

[redacted]

(U//~~FOUO~~) Forensic evidence combined with [redacted] testimony supports the allegation that he misused his Agency IS and U.S. Government resources.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0017

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//~~FOUO~~) [redacted] was provided the tentative conclusions on 4 June 2013. [redacted] responded to the tentative conclusion stating:

“I agree.”

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

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused his unclassified Agency IS and U.S. Government resources for approximately two hours each workday from 2007-2012, in violation of NSA/CSS Policies 6-6 and 6-4.

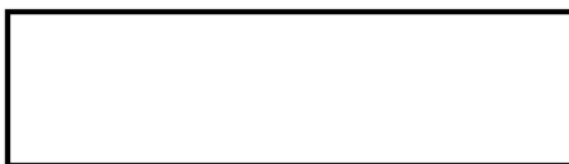
[redacted]
(b) (3) - P.L. 86-36
(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0017

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report of investigation will be maintained in the case file. 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.



Deputy Assistant Inspector General
For Investigations

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0017

Attachment 1

OIG report

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



**OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE**

To: Chief, D14

Date: 5 May 2006

From: AIC [redacted]

Subject: Computer Misuse (b) (3) - P.L. 86-36

File No: [redacted]

Precedence: Routine

Purpose: (U) To provide a summary report of investigation and to refer this matter to Special Actions in the Associate Directorate for Security and Counterintelligence (ADS & CI) for review and any action deemed appropriate. A copy of this memorandum will be forwarded to the Director of Human Resources, [redacted]

Details:

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

I. (U) Background:

(U//FOUO) [redacted] is an NSA contractor affiliate assigned to [redacted]. Routine monitoring of the NSA/CSS unclassified network detected [redacted] account accessing adult-oriented material on unclassified Internet web pages. The activity was initially detected on 10 January 2006. On at least one other occasion (13 January 2006), similar activity was detected on his account. Computer Logs revealed that [redacted] was logged-in at the times the inappropriate activity was detected: [redacted]

(U//FOUO) NSA/CSS Computer Security/Virus Incident Report (CSIR) [redacted] was issued 6 February 2006. The tracking number for this violation was assigned to the NSA/CSS Information Security Incident Response Team (NISIRT) [redacted]

II. (U) Issue(s):

(U//FOUO) Did [redacted] misuse his Agency computer and unclassified Internet account by intentionally accessing adult-oriented web sites?

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0017

III. (U) Applicable Standard(s):**(U) NSA/CSS Policy 6-6, "USE OF UNCLASSIFIED INFORMATION SYSTEMS SUCH AS THE INTERNET," Responsibilities Section:**

25. (U) All Users shall:

...

- e. (U) Report to the SHO or the Office of Inspector General (OIG), any potential or actual abuses of NSA/CSS-sponsored accounts on unclassified ISs as soon as they become aware of any known or suspected problem;
- h. (U) Report all cases of misdirected web page access to inappropriate web sites to the SHO immediately, and to the appropriate ISSO or ISSPM for the particular Internet host;

...

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

....

(U) NSA/CSS Policy 6-4, "CONTRACTOR USE OF GOVERNMENT INFORMATION SYSTEMS," Policy Section:

3. (U) Personal use of Government ISs by contractor personnel is prohibited except for brief, infrequent communications to take care of unavoidable personal matters (e.g., contacting a spouse, dependent, or individual responsible for their care; scheduling a physician's appointment or car maintenance; etc.). This limited exception to the personal use prohibition applies only when

- a. the communication could not have reasonably been made at another time (e.g., the physician is only available during working hours),
- b. the communication does not adversely affect the Agency mission or reflect poorly on the Agency,
- c. the communication does not result in other than minimal expense to the Government (e.g., the call is local, toll-free, or charged to a personal telephone calling card),
- d. time spent using the Government IS for personal use is not billed to the contract, and
- e. the communication is of a non-commercial nature.

(U) This exception does not permit any personal commercial use of Government ISs (e.g., use in conjunction with a contractor employee's personal business activity for financial or other gain).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) [redacted] Internet Account User Agreement, dated 05 January 2000 - Version 9:

(U) The use of [redacted] resources constitutes your consent to monitoring:

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

...
(U//FOUO) This [redacted] Conduct business accordingly.

...
(U) YOU are accountable for the proper use and protection of YOUR account.

...
(U) Violation of the terms of this agreement may result in loss of access and/or other disciplinary action....

IV. (U) Investigative Activity:

A. (U) NISIRT Forensic Analysis

(U//FOUO) A NISIRT Network Analyst provided the OIG with an analysis of activities on [redacted] Internet account. The following is an OIG summary of that analysis.

(U//FOUO) On 10 January 2006, the user [redacted] performed a Google Search for [redacted]. The user then accessed several adult-oriented websites including graphic images and videos. The user accessed several adult-oriented websites, which included:

(b) (6)

[redacted] (website contains [redacted]) (website contains information, links, images, and videos of sexually explicit material). Similar activity was noted on 13 January 2006. Approximately 35 adult-oriented videos were accessed during these two dates of inappropriate activity.

B. (U//FOUO) Notification to Subject [redacted]

(U//FOUO) On 14 February 2006, the OIG sent [redacted] an email stating that his account was detected accessing adult-oriented material, and he was provided the links to the relevant policies and OIG Exec message to review. [redacted] was required to respond to this email, and affirm his intention to adhere to the applicable policies in the future. Later that day, he responded, stating: "Good morning, I have reviewed the policy [sic] and will definitely adhere to them in the present and the future."

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

V. (U) Analysis and Conclusion:

(U//FOUO) Forensic evidence indicates that [redacted] misused his Agency computer and his unclassified Internet account. [redacted] failed to exercise good judgment in his usage of the NSA unclassified system, and therefore violated NSA/CSS Policy 6-6. Furthermore, [redacted] violated

NSA/CSS Policy 6-4 in that his personal use of Government information systems reflects poorly on the Agency. Finally, by virtue of his misuse, [redacted] violated his NSA User Agreement.

VI. (U) Recommendation(s):

(U//~~FOUO~~) In accordance with the above, this case should be closed and this summary memorandum provided to Special Actions in ADS & CI for review, and any action deemed appropriate. A copy of this memorandum will also be provided to the Director of Human Resources, Eagle Alliance.

cc:

- 1 - [redacted]
- 1 - ADS & CI (Q234)
- 1 - OGC (D23)
- 1 - [redacted] (Human Resources)

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

*** (U//~~FOUO~~) This report is property of NSA and may not be disseminated further without specific approval of NSA Office of General Counsel (OGC). Furthermore, the information in this report cannot be used in affidavits, court proceedings, subpoenas, or for other legal or judicial purposes without the prior approval of the NSA OGC. You should contact the NSA OGC directly at [redacted] for approval to use this information in any legal proceeding.**

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0017

Attachment 2

NISIRT report

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Excerpts from the NISIRT report

User was observed going to web sites of a sexual nature and trying to access porn sites. He was also streaming music and going to [redacted] video site. A small sample of activity and sites accessed is listed below. This user has a very low volume of traffic on his classified account during this time while his traffic was high on the unclassified network.

URLs accessed or attempted:

- 2012/09/20 11:42AM
[redacted]
- 2012/09/21 07:43AM
[redacted]
- 2012/09/24 11:44AM
[redacted]
- 2012/09/24 12:37PM
[redacted]
- 2012/09/25 07:48AM
[redacted]
- 2012/09/26 07:59AM
[redacted]
- 2012/09/27 02:07PM
[redacted]
- 2012/09/28 7:28AM
[redacted]
- 2012/09/28 09:20AM
[redacted]
[redacted]
[redacted]
- 2012/10/01 08:18AM
[redacted]
- 2012/10/01 02:10PM
[redacted]

(b) (6)

~~UNCLASSIFIED//TOP OFFICIAL USE ONLY~~

IV-13-0017

(b) (6)

2012/10/01 08:16AM

[Redacted]

2012/10/02 07:02AM

[Redacted]

2012/10/02 10:50AM

[Redacted]

2012/10/03 10:15AM

[Redacted]

2012/10/03 10:56AM

[Redacted]

2012/10/03 11:27AM

[Redacted]

2012/10/04 12:20PM

[Redacted]

2012/10/04 11:36AM

[Redacted]

2012/10/04 11:35AM

[Redacted]

2012/10/04 11:22AM

[Redacted]

~~UNCLASSIFIED//TOP OFFICIAL USE ONLY~~