

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY
SERVICE**



**INSPECTOR GENERAL
REPORT OF INVESTIGATION**

14 May 2013

IV-12-0119

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~~

~~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~~

I. (U) SUMMARY

(U//~~FOUO~~) On 17 August 2012, the IG received a referral from the Associate Directorate for Security and Counterintelligence (ADS&CI), identifying potential computer misuse by an NSA contractor. On 22 August 2012, the IG opened an investigation on [redacted] a [redacted] contractor assigned to the [redacted] alleging the misuse of an NSA Information System (IS) and U.S. Government resources starting in August 2012. The preponderance of the evidence collected during the investigation substantiated that [redacted] misused his NSA/CSS IS and U.S. Government resources to transfer non-work related material to the classified NSA/CSS IS in violation of NSA/CSS Manual 5-23 and NSA/CSS Policy 6-4.

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

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

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 or affiliate with [redacted] assigned to the [redacted]

(U//~~FOUO~~) ADS&CI notified the OIG of detected misuse on [redacted] account beginning in August 2012. NSA/CSS Information Systems Incident Response Team (NISIRT) confirmed that they had provided ADS&CI a report of detected misuse. The NISIRT assigned tracking number [redacted] to this violation. ADS&CI transferred the computer security incident report to the OIG on 17 August 2012.

(U//~~FOUO~~) ADS&CI determined [redacted] committed a major security violation for deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information in March 2012.

(U) Applicable Authorities

(U//~~FOUO~~) NSA/CSS Manual 5-23, "PHYSICAL SECURITY REQUIREMENTS FOR CONTROLLED AREA MANUAL," revised 23 June 2010.

(U) Chapter Nine: Introduction of Electronic & Information Technology Equipment:

4. (U//~~FOUO~~) Commercially produced CDs and DVDs, normally silver in color with the manufacturer's artist label, are permitted for use in personal CD or DVD players inside NSA/CSS spaces. Personally produced music or speaking audio CDs and DVDs are permitted for use inside NSA/CSS spaces. Personally produced music or speaking audio CDs and DVDs must meet the following criteria:

- a. (U) A supervisor has approved the use of CDs/DVDs in the office;
- b. (U) The CD/DVD is clearly marked "Unclassified Personal Music" with indelible ink so it is easily recognized as an unclassified music CD/DVD;
- c. (U) The CD/DVD is a write once type and finalized, so that no additional data can be added;
- d. (U) The CD/DVD contains only music or speaking audio files;

e. (U) The CD/DVD must remain in the workplace and be disposed of via special burn when no longer needed (does not apply to commercially recorded media);

f. (U) The CD/DVD must only be played in a personally owned CD/DVD player; and

g. (U) The CD/DVD player has no record capabilities or microphone.

(U) Chapter Ten: Prohibited/Restricted Items

5. (U//~~FOUO~~) Restricted items may be brought through the vehicle gates and maintained in a personal vehicle, but cannot enter NSA/CSS facilities. They include the following personally-owned items:

...

j. (U) CDs/DVDs, other than those permitted by paragraph 4, Chapter Nine, "Introduction of Electronic and Information Technology Equipment."

7. (U//~~FOUO~~) Personally owned media or equipment shall not be connected to any classified or unclassified NSA/CSS automated information system or network.

....

(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.

d. (U) Time spent using the NSA/CSS IS for personal use is not billed to the contract; and

....

III. (U) FINDINGS

(U//~~FOUO~~) Did [redacted] a contractor affiliate with [redacted] assigned to the [redacted] misuse his Agency IS and U.S. Government resources in violation of the NSA/CSS Manual 5-23 and NSA/CSS Policy 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] introduced non-work related material to the classified network in violation of NSA/CSS Manual 5-23. [redacted] also violated NSA/CSS Policy 6-4 by using Government resources for activities other than that authorized by contract or approved by the Contracting Officer.

(U) Evidence: NISIRT Analysis

(U//~~FOUO~~) NISIRT provided first ADS&CI then the OIG with an analysis of [redacted] activities on the classified NSA/CSS IS. [redacted] was detected transferring movie and TV files from a DVD/CD to the hard drive on his workstation. The full NISIRT report can be found as attachment 1.

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

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

(U) Interview

(U//~~FOUO~~) On 7 March 2013, the OIG interviewed [redacted] has been working in NSA spaces since 2009 as a contractor. When [redacted] was asked his understanding of policies governing his use of Government resources, he stated he was not permitted to use the IS for "personal use." [redacted] admitted using his NSA/CSS IS to access personal email.

(U//~~FOUO~~) [redacted] works under [redacted] [redacted] was informed that he was detected introducing movies, mp3, etc to the classified network. [redacted] did not deny the allegation. He admitted he is not a Data Transfer Agent and does not have the authority to introduce the files into the network. He explained that he burns his own copies of movies on DVDs at home and then brings them into NSA spaces. Some of these movies were purchased movies and others are downloaded from the internet but he reported all were obtained from legitimate sources. [redacted] claimed that he virus scanned the DVDs before uploading them to the network. [redacted] testified that his intent was to "keep my mind occupied and focused at

~~Unclassified//For Official Use Only~~

IV-12-0119

work." [redacted] said no one else knows what he is doing. Currently there are a "handful" of movies on a local drive.

(U//FOUO) After the interview, [redacted] was provided information in an email regarding the current policy and guidance. See attachment 2 for the OIG policy email sent to [redacted]. He was asked to respond to the OIG acknowledging the requirement to comply with the policies in the future. On 8 March 2013, [redacted] responded, stating "I have reviewed the policy in detail and will adhere to it."

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

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

~~Unclassified//For Official Use Only~~

~~Unclassified//For Official Use Only~~

IV-12-0119

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

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

(U//~~FOUO~~) [redacted] was provided the tentative conclusions on 3 May 2013. [redacted] responded to the tentative conclusion, stating:

As I had originally stated, the media that was imported was done so with the utmost care and concern for security; any content of that media was original media from my own library, and checked multiple times with multiple virus, malware and rootkit detection tools. The media was then sent to special burn per agency policy. The files themselves were kept on an unused drive on my local workstation, so as not to interfere with anything else, period.

Yes, I introduced 'non-work related' materials to NSANet. I think I've admitted as much. And I believe I explained exactly why I did so; having background noise of a familiar nature allows me to focus better on the work and tasks at hand. It was never a matter of 'non-work' - it had always been about enhancing my work flow, as early in my career I had found certain things to aid my focus and allow me to essentially tune out the rest of the noise and goings on in the office and have solid focus and a keen amount of concentration to the tasks at hand.

I suppose that the conclusion that you have drafted is technically correct, however given what I have explained, I believe that the wording and technicality of the conclusion alludes to something more improper than what I believe is the case here; I was extremely careful and exceedingly precise about what I did, and I had no intent of malice. I did so to essentially enhance my performance given what I have learned over the course of many years in the IT industry, and as a security practitioner.

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

~~Unclassified//For Official Use Only~~

~~Unclassified//For Official Use Only~~

IV-12-0119

V. (U) CONCLUSION

(U//FOUO) The preponderance of the evidence supports the conclusion that [redacted] misused his classified NSA/CSS IS and U.S. Government resources in violation of NSA/CSS Manual 5-23 and NSA/CSS Policy 6-4.

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

~~Unclassified//For Official Use Only~~

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) This report of investigation will remain 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 their information and any action deemed appropriate.



Deputy Assistant Inspector General
for Investigations

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

~~Unclassified//For Official Use Only~~

IV-12-0119

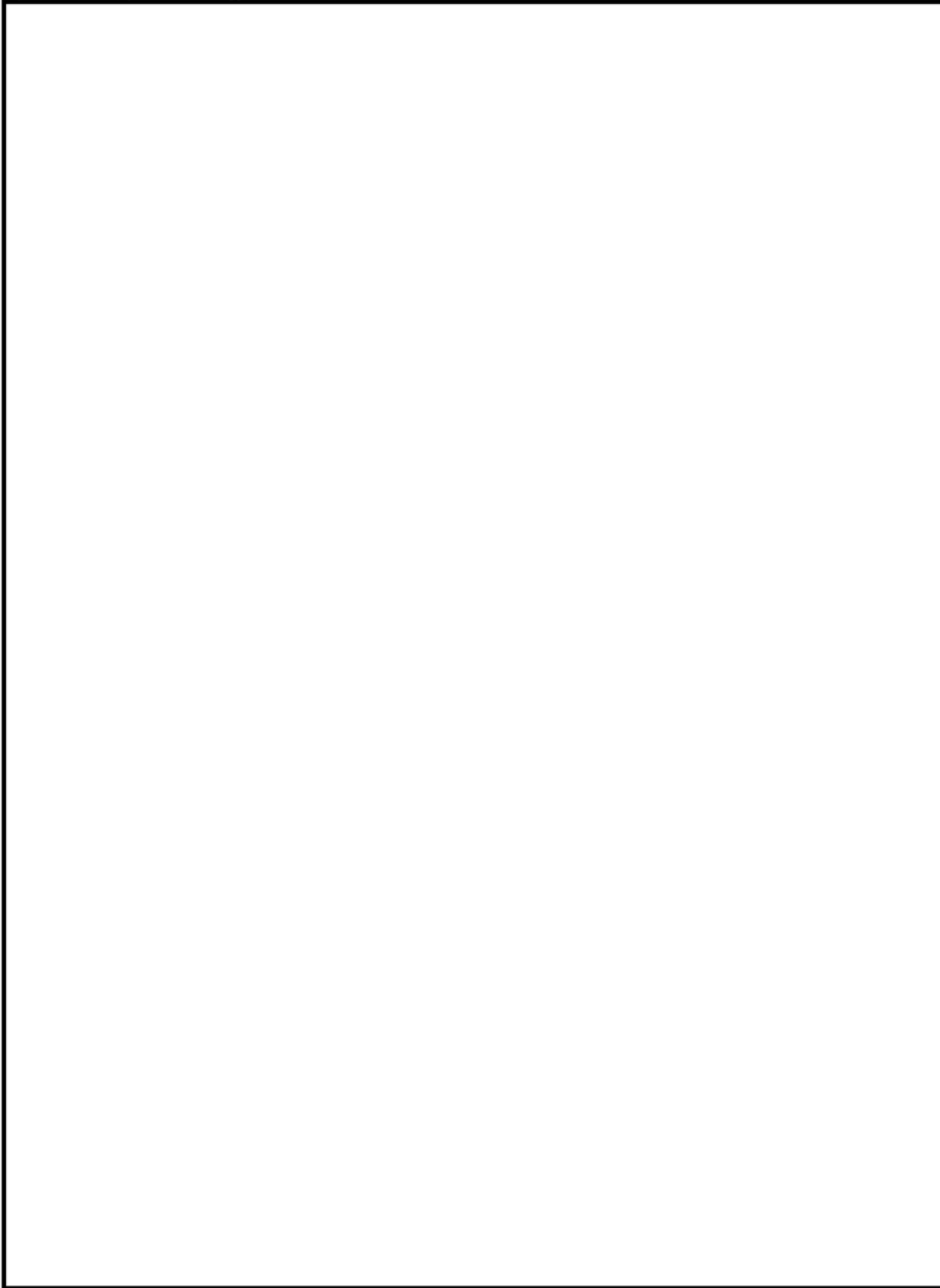
Attachment 1

NISIRT report

~~Unclassified//For Official Use Only~~

NISIRT Report

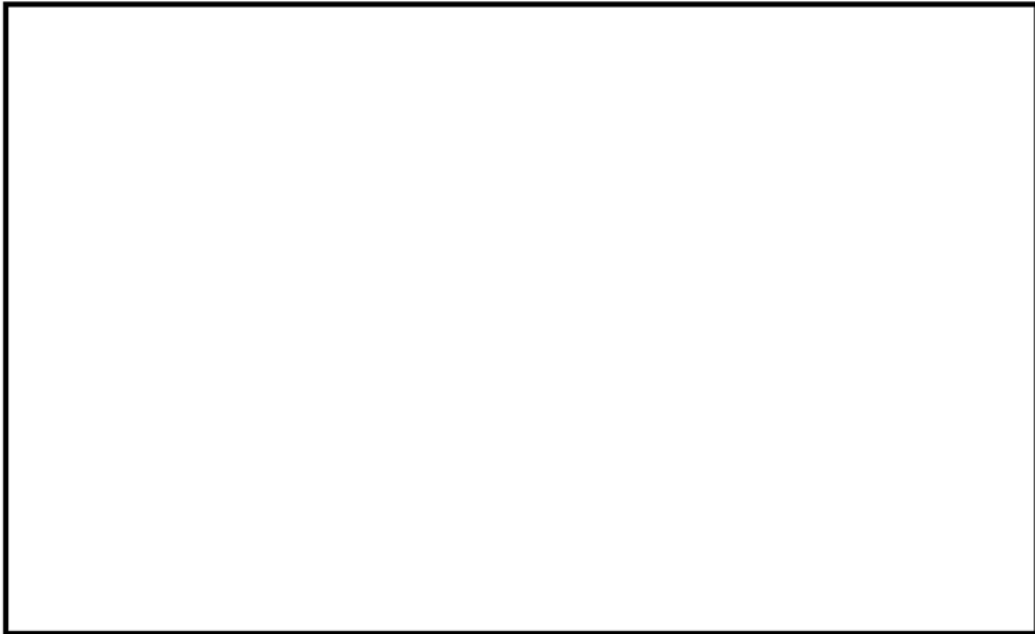
(U//~~FOUO~~) On 7 August 2012, the user transferred the following files from a DVD to NSAnet.



(b) (6)

~~Unclassified//For Official Use Only~~

IV-12-0119



(b) (6)

(U//~~FOUO~~) On 9/4/12, the user transferred the following onto NSAnet:



~~Unclassified//For Official Use Only~~

~~Unclassified//For Official Use Only~~

IV-12-0119

Attachment 2

Policy email

~~Unclassified//For Official Use Only~~

~~Unclassified//For Official Use Only~~

IV-12-0119

From: [Redacted]
Sent: Thursday, March 07, 2013 1:30 PM
To: [Redacted]
Subject: (U) Followup from our interview

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

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

To follow-up on the policy details we discussed during our interview. Please read the below information.

4. (U//~~FOUO~~) Commercially produced CDs and DVDs, normally silver in color with the manufacturer's artist label, are permitted for use in personal CD or DVD players inside NSA/CSS spaces. Personally produced music or speaking audio CDs and DVDs are permitted for use inside NSA/CSS spaces. Personally produced music or speaking audio CDs and DVDs must meet the following criteria:
- a. (U) A supervisor has approved the use of CDs/DVDs in the office;
 - b. (U) The CD/DVD is clearly marked "Unclassified Personal Music" with indelible ink so it is easily recognized as an unclassified music CD/DVD;
 - c. (U) The CD/DVD is a write once type and finalized, so that no additional data can be added;
 - d. (U) The CD/DVD contains only music or speaking audio files;
 - e. (U) The CD/DVD must remain in the workplace and be disposed of via special burn when no longer needed (does not apply to commercially recorded media);
 - f. (U) The CD/DVD must only be played in a personally owned CD/DVD player; and
 - g. (U) The CD/DVD player has no record capabilities or microphone.

7. (U//~~FOUO~~) Personally owned media or equipment shall not be connected to any classified or unclassified NSA/CSS automated information system or network.

You are required to review policy listed below and send me an email acknowledging that you have reviewed the policy and will adhere to it in the future. If the link does not work, you can type "Go Policy" on NSAnet and look it up.

PHYSICAL SECURITY REQUIREMENTS FOR CONTROLLED AREAS MANUAL

[Redacted]

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

~~Unclassified//For Official Use Only~~