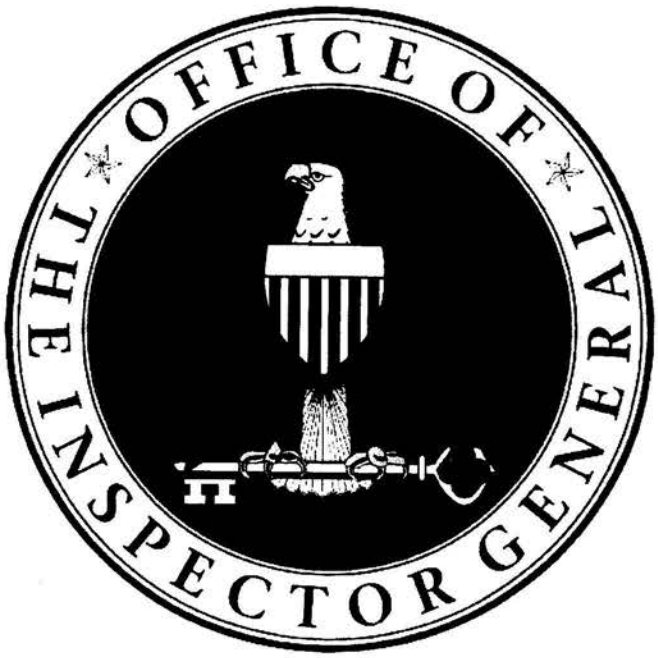
NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



INSPECTOR GENERAL

REPORT OF INVESTIGATION

6 June 2013

IV-12-0114

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

(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.

I. (U) SUMMARY

(U//~~FOUO~~) On 18 June 2012, the IG received a referral from the NSA/CSS Information Systems Incident Response Team (NISIRT), identifying potential computer misuse by a NSA civilian. On 1 October 2012, the IG opened an investigation on [redacted] a civilian employee assigned to the [redacted] alleging the misuse of a NSA/CSS Information System (IS) and U.S. Government resources in May and June 2012. The preponderance of the evidence collected during the investigation substantiated that [redacted] misused his NSA/CSS IS and U.S. Government resources to send sexually explicit emails in violation of the JER 5500.7-R and NSA/CSS Policy 6-6.

(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)

(U) Introduction

(U//~~FOUO~~) employee identification number is a civilian employee assigned to the

(U//~~FOUO~~) NSA/CSS Information Systems Incident Response Team (NISIRT) reviewed unclassified U.S. Government account from 18 May and 14 June 2012. NISIRT detected misuse on account on 29 May, 1 June and 13 June 2012. The NISIRT assigned tracking number to this violation. NISIRT provided the activity report to the Office of the Inspector General on 18 June 2012.

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

(U) Applicable Authorities

(U//~~FOUO~~) DoD Joint Ethics Regulation (JER) 5500.7-R: Subpart 2-301: Use of Federal Government Resources.

> a. Communication Systems. [...] Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only.
>
> > (2) Authorized purposes include brief communications made by DoD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief internet searches; e-mailing directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:
> >
> > ....
> >
> > (d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service)....

(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;

[....]

III. (U) FINDINGS

(U//~~FOUO~~) Did [redacted] a NSA civilian employee, assigned to the [redacted] misuse his Agency IS and U.S. Government resources in violation of the JER 5500.7-R and NSA/CSS Policy 6-6?

(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 send sexually explicit emails in violation of the JER 5500.7-R and NSA/CSS Policy 6-6.

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

(U) Evidence: NISIRT Analysis

(U//~~FOUO~~) NISIRT provided the OIG with details of [redacted] activities on the unclassified NSA/CSS IS. [redacted] was observed sending sexually explicit emails from his personal email account using Government resources. The full NISIRT report can be found as attachment 1.

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

(U) Interview

(U//~~FOUO~~) On 21 May 2013, [redacted] was interviewed and provided the following sworn testimony:

[redacted] admitted to sending sexually explicit emails from his personal email account. He understood the policy governing the use of Government resources but was "not thinking about the monitoring" when he wrote the emails. [redacted] knew "he should not engage in this type of activity from a work computer." [redacted] estimated that from 1 March to 21 May 2013, he spent approximately two to three hours per day on non-work related activities on the internet. [redacted] estimated that from June to October 2012, he spent approximately 1 hour per day on non-work related internet activities.

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

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:

"You are correct. The only thing I would like to say is that, Although I was writing the emails on my unclass email (hotmail account) I did write some inappropriate emails while accessing the account while logged in from work unclassified computer. I do understand this was/is wrong and accept responsibility. I only ask that whatever disciplinary actions there might be, take into account that this is my first offense in the 20plus years I have been working here. I should have known better (I do) and I can promise that it will never happen again. As I told you in the interview. What I did was wrong and the reason I stopped was because I came to the realization that I didn't want to lose everything that I have (work and family). Again my apologies for my mistake and it will not happen again."

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

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

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 in violation of the JER 5500.7-R and NSA/CSS Policy 6-6.

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

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 Employee Relations and Special Actions, ADS&CI for review and any action deemed appropriate.

[redacted]
Deputy Assistant Inspector General
For Investigations

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

Attachment 1

NISIRT report

NISIRT Report

Sample of non-work related activity on the Unclassified IS. Edits were made by the OIG for readability purposes.

(b) (6)

05/29/2012 13:03:11

[redacted]

05/29/2012 14:10:59

[redacted]

05/29/2012 14:57:47

[redacted]

06/01/2012 10:25:39

[redacted]

06/01/2012 11:08:02

(b) (6)

[redacted]

06/01/2012 11:35:51

[redacted]

06/13/2012 10:25:01

[redacted]