NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

OFFICE OF THE INSPECTOR GENERAL

REPORT OF INVESTIGATION

26 July 2013
IV-13-0018

Misuse of Government Resources

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 02-28-2018, FOIA Case # 79204

Release: 2018-03
NSA: 02188
(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 ensure 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 23 August 2012 the Office of the Inspector General (OIG) 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 OIG initiated an investigation of use of NSA/CSS Information Systems (IS). The preponderance of the evidence collected during the investigation substantiates that between June and October 2012 misused her NSA/CSS IS to plan a company recruiting event. These activities violate NSA/CSS Policies 6-4, 6-6 and 6-12.

(b)(3) - P.L. 86-36
(b)(6)
II. (U) BACKGROUND

(U) Introduction

(U//FOUO) Ms. ______________ working under the contract


(U) Applicable Authorities

(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.
(U//FOOU) 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;

[....]

(U//FOOU) NSA/CSS Policy 6-12

1. (U) Users shall use collaboration tools and collaboration services on classified NSA/CSS ISs for work-related purposes. ... Contractors also shall follow NSA/CSS Policy 6-4, "Contractor Use of NSA/CSS Information Systems". Accordingly, posted material is subject to review, and violations of policy may result in user administrative and/or disciplinary action.
III. (U) FINDINGS

(U/FOUO) Did misuse NSA/CSS IS in violation of NSA/CSS Policies 6-4, 6-6 and 6-12?

(U/FOUO) CONCLUSION: Substantiated. The preponderance of the evidence supports the conclusion that [redacted] misused her Unclassified and Top Secret NSA/CSS IS. [redacted] used the Government resources to plan a recruiting event for [redacted] in violation of NSA/CSS Policies 6-4, 6-6 and 6-12.

(U) Documentary Evidence

(U) NISIRT Report

(U/FOUO) The NISIRT provided the OIG with an analysis of [redacted] activities on the Unclassified and Top Secret NSA/CSS IS. [redacted] was observed planning a recruiting event. The full NISIRT report can be found at Appendix A.

(U) Print logs

(U/FOUO) The OIG obtained the print logs for [redacted]. A review of unclassified printer logs revealed that she printed 34 documents, totaling 101 pages, with titles related to recruiting event planning between June and September 2012. The print log of these specific items can be found at Appendix B.

(U) Testimonial Evidence

(U/FOUO) On 16 May 2013, [redacted] was interviewed and provided the following sworn testimony:
admitted to sending “a couple” of personal emails on the unclassified internet. She did not feel the admitted activity was excessive. She uses chat on the Top Secret IS to communicate with individuals both work related and non work related but felt those activities were mostly work related. She stated, I know I have done some things on there [the internet] I shouldn’t have done. I’m only supposed to use Government resources for Government use. After receiving the email requesting an interview with the OIG, she thought to herself “why did I do that Google search?” She attributed her actions to a “complete lapse of judgment.”

was asked by her company to recruiting event. She planned for this event from June to September 2012. denied printing flyers using the Agency printer but did admit that she used the unclassified and classified computers to plan this event.

On 17 June 2013, was interviewed again and provided the following sworn testimony:

stated again that she did not print the flyers for the event using Government resources but when asked if she printed any documents relating to the event, she could not recall. However, when confronted with the print logs she admitted that the titles would be consistent with items a person would need to assist in planning such an event. did not deny that she printed these items; just that she had forgotten that she printed them in her earlier interview.

(U) Analysis and Conclusions

The NISIRT report and the print logs combined with own admission of personal use supports the conclusion that she misused her Unclassified and Top Secret NSA/CSS IS.
IV. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//FOOU) was provided the tentative conclusions on 4 June 2013. responded to the tentative conclusion stating:

"I acknowledge the drafted report and I acknowledge that I mis-used my government computer system. I would like to make it clear that I did not knowingly do this at the time. As I stated in my interview, I did not realize that the emails I was sending were wrong at the time. I see now why it should not have been done and for that I apologize. I would also like to state for the record that along with my time sheets I provided a detailed list of email transactions, how long those emails were, and how long they may have taken me. All together including emails and working on documents I spent at the most 3 hrs during work hours using a government computer to do company related work. My detailed list was provided to the investigator as well as my company management team. I have not used my government computer system for anything other than timesheets since the beginning of this investigation and do not intend to use it for anything else in the future. I know that this does not change what I have done but it is a way to correct my actions and to ensure this never happens again. I thank you for your time and consideration."

(U//FOOU) 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] mishandled her Unclassified and Top Secret NSA/CSS ISs to plan a company recruiting event in violation of NSA/CSS Policies 6-4, 6-6 and 6-12.

(b)(3) - P.L. 86-36
(b)(5)
VI. (U) DISTRIBUTION OF RESULTS

(U//FOO) A copy of this report of investigation will be maintained in the case file. A summary memorandum will be provided to the NSA Senior Acquisition Executive, 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
Appendix A

NISIRT report
Appendix B

breakdown of event related documents printed on an unclassified printer

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