

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY
SERVICE**



INSPECTOR GENERAL

REPORT OF INVESTIGATION

15 January 2014

IV-13-0078

Misuse of an Agency Information System to Solicit Business

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 07-01-2019, FOIA Case # 79204 (litigation)
Release: 2019-06

NSA:08587

~~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

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

(b) (3) - IG Act of 1978, Sec 7(b), P.L. 95-452
(b) (3) - P.L. 86-36

(U//~~FOUO~~) On 03 July 2013, the NSA/CSS Office of Inspector General (OIG) received an anonymous allegation that [redacted] misused Agency Information Systems (IS). Specifically, it is alleged that [redacted] used NSA/CSS ISs in providing [redacted] electronic copies of documents to assist [redacted] in planning for an upcoming Request for Proposals (RFP) on the [redacted] procurement and that he did so in an attempt to obtain a teammate position on the upcoming contract should [redacted] win it.

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

(U//~~FOUO~~) In addition to obtaining sworn testimony from [redacted] we obtained a copy of the Agency contract on which he is assigned and relevant emails sent by [redacted] to [redacted] from both his Agency classified OUTLOOK email account and his unclassified [redacted] email account. We also obtained information from the relevant [redacted] program office, and Office of the General Counsel (OGC) in order to confirm that the [redacted] procurement had not been jeopardized by [redacted] actions.

(U//~~FOUO~~) Emails disclosed that [redacted] used the NSA/CSS classified IS to send [redacted] classified and unclassified documents related to the [redacted] program. None of the documents were acquisition sensitive. During his interview with the OIG, [redacted] acknowledged that he used the Agency IS to provide [redacted] background information relevant to [redacted] in order to help the company prepare for the upcoming solicitation; all of the documents were available to contractors with access to NSA/CSS's classified Intranet. According to [redacted] he did this for business development purposes - to try and obtain a teaming opportunity with [redacted] should the company win the [redacted] contract.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused an Agency IS to solicit business, in violation of NSA/CSS Policy 6-4.

(U//~~FOUO~~) A copy of the NSA/CSS OIG report will be forwarded to NSA/CSS Contracting, the NSA/CSS Senior Acquisition Executive (SAE), and the NSA/CSS Office of General Counsel (OGC), Acquisition, Research, and Technology Law (Acquisition Law). Also, a summary of the findings will be forwarded to the NSA/CSS Associate Directorate for Security and Counterintelligence (ADS&CI).

(b) (3) - IG Act of 1978, Sec 7(b), P.L. 95-452
(b) (3) - P.L. 86-36

II. (U) BACKGROUND

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

(U) Introduction

(U//FOUO) [redacted] performs on the [redacted] Technical Task Order [redacted], for which [redacted] is the prime contractor and [redacted] is a subcontractor. In this capacity, [redacted] provides [redacted] [redacted] from his assigned location at NSA Washington (NSAW).

(U//FOUO) [redacted] In a letter dated 28 June 2013, [redacted] self-reported to NSA's [redacted] the company's receipt of Government information from a third party. According to the letter, [redacted] was conducting business planning efforts and potential teaming discussions in preparation for the Agency's anticipated solicitation for the [redacted] contract. In an attempt to assist [redacted] with its business planning and persuade [redacted] to offer him a teammate position should [redacted] with the [redacted] contract, [redacted] provided [redacted] copies of classified and unclassified U.S. Government documents. Although [redacted] claimed that all of the documents were generally available to contractor personnel with access to NSA's classified network, the documents were quarantined from company use by the [redacted] Law Department. On 03 July 2013, the [redacted] referred the matter to the OIG for investigation.

(U) Applicable Authorities

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

(U) NSA/CSS Policy 6-4, Contractor Use of NSA/CSS Information Systems (IS)

(U) Policy

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.

2. (U) Contractors shall not use NSA/CSS ISs to solicit business, advertise products or services, recruit employees, whether from NSA/CSS or other contractor workforces, or otherwise obtain an unfair advantage....

....4. (U) Contractors shall not make personal use of NSA/CSS ISs except for brief, infrequent communications to take care of unavoidable personal matters.... This limited exception to the personal use prohibition applies only when:...

...b. (U) The communication does not adversely affect the Agency mission or reflect poorly on the agency:...

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

IV-13-0078

...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.¹

¹ NSA/CSS Policy 6-4 was updated on 22 October 2013. This report of investigation uses the version of NSA/CSS Policy 6-4 (issued 16 April 2003 and revised 07 June 2007) that was in effect at the time of the events.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

III. (U) FINDINGS

(U//~~FOUO~~) Did [redacted] misuse an Agency IS to solicit business?

(U//~~FOUO~~) **CONCLUSION:** Substantiated. The preponderance of the evidence supports the conclusion that [redacted] misused an Agency IS to solicit business, in violation of NSA/CSS Policy 6-4.

(U) Documentary Evidence

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

(U//~~FOUO~~) The OIG obtained a copy of the contract, [redacted] to which [redacted] is assigned. Page 26, Section H, Special Contract Requirements, Paragraph H.33, 352.290-9014 Contractor Use of Government Information Systems (May 2007), of the contract reads as follows:

(U) Contractors that require access to NSA/CSS Government Information Systems (GIS) shall comply with the NSA/CSS Policy 6-4, Contractor Use of Government Information Systems. The GIS includes any equipment owned, leased, controlled, or operated on behalf of NSA/CSS through contract as defined within the policy. NSA/CSS Policy 6-4 is applicable to all NSA/CSS contractors, subcontractors, and their personnel that use, implement, maintain, or have access to GIS. A copy of NSA/CSS Policy 6-4 can be accessed via the Acquisition Resource Center (ARC) (www.nsaarc.net) by clicking the "Acquisition News" link.

(U//~~FOUO~~) The OIG reviewed [redacted] classified OUTLOOK email account for relevant emails. Additionally, [redacted] provided copies of [redacted] classified and unclassified email correspondence with company personnel. Emails revealed that on 19 March 2013, [redacted] contacted four [redacted] personnel using his unclassified [redacted] email account. [redacted] indicated that he had used the NSA/CSS Acquisition Resource Center (ARC) business registry database to obtain their names as points of contact (POCs) for [redacted] and would be "interested in talking to whomever at [redacted] would be interested in the [redacted] Market Survey [redacted] [redacted]". Subsequent emails revealed that [redacted] arranged to meet with the [redacted] [redacted] on 21 March 2013.

(U//~~FOUO~~) On 19 April 2013, [redacted] used his NSA classified email account to identify an [redacted] employee's "dropbox" to which he could forward concept briefings related to [redacted] [redacted]. Between 19 April 2013 and 23 April 2013, [redacted] shared over 20 [redacted] background documents with [redacted] by either email or dropbox. He also used his NSA classified email account to write to an [redacted] employee, educating him on [redacted] hardware, providing background on [redacted] difficulties, and suggesting improvements that could be implemented through [redacted]. On 25 and 26 April 2013, [redacted] provided [redacted] the original source for each of the individual documents he had sent earlier. He noted that every document was available to anyone with an NSA net, IWICS, or SIPRNet account." He also

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

provided a link to [redacted]
[redacted] homepage of the Intranet.

(U//FOUO) Emails revealed that [redacted] Program Office) personnel reviewed the documents [redacted] released to [redacted] and determined that they would not damage the integrity of the procurement process. Further, upon consultation with OGC Acquisition Law, the [redacted] concurred. According to the [redacted] most of the information [redacted] provided to [redacted] was out of date. Additionally, none of it involved procurement data (such as Statements of Work, Acquisition Strategy, and Functional Requirements) that would cause harm to program acquisitions.

(U) Testimonial Evidence

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

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

(U//FOUO) [redacted]

(U//FOUO) On 18 July 2013, [redacted] was interviewed and provided the following sworn testimony:

(b) (6)

(U//FOUO) He is aware of [redacted] because it involves [redacted] a field in which he has worked for [redacted] years. Everyone in his field at NSA is aware of the [redacted] related procurement efforts. However, [redacted] is the only such effort [redacted]. Because of his work experience, [redacted] is seeking to team with another company on [redacted]. Therefore, in spring 2013 he reached out to [redacted] about possible teaming opportunities.

(U//FOUO) Because the [redacted] team in charge of the [redacted] procurement process is not knowledgeable of [redacted] used NSA computer systems to provide [redacted] relevant electronic documents to "bring them up to speed" on [redacted]. All of the documents were available to any NSA contractor with classified Intranet access. Most of them could be found in the electronic library of the ARC under business development. Others were from outside agencies and could be found through JWICS and SIPRNet. [redacted] denied providing [redacted] acquisition sensitive information or any information that they otherwise could not have found themselves. He simply saved [redacted] research time. None of the documents were acquisition, [redacted] or [redacted] sensitive. [redacted] has no involvement in NSA's procurement process and does not have access to acquisition information.

(U//FOUO) Although [redacted] had not read the contract on which he worked in its entirety, he was familiar with the restrictions on contractor use of GISs as listed on page 26 of the contract. He knew that contractors were expected to follow NSA/CSS Policy 6-4. [redacted] was also aware that he could not charge the Government for time spent conducting business development tasks and did not do so. He acknowledged that by sending business development emails to [redacted] personnel, he had violated Policy 6-4's prohibition against using Agency ISs to conduct personal business activity.

(U//FOUO) In his effort to team with [redacted] [redacted] had also met with [redacted] personnel to educate them further about [redacted]. However, they expressed concern when they learned that he was a subcontractor on [redacted] at NSA. [redacted] explained to [redacted] that his work

was completely unrelated to acquisitions and even sourced the documents he had provided so that [redacted] would know that they were available to everyone with access to the classified Intranet. However, when [redacted] sent [redacted] an email in approximately June 2013 asking whether he was going to be a member of [redacted] team, he received no response.

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

(U) Analysis and Conclusions

(U//~~FOUO~~) [redacted] acknowledged having used an Agency IS for personal business development purposes; he wanted to be a teammate with [redacted] on the [redacted] effort. Further, he acknowledged having done so even though he was aware of the requirement to adhere to NSA/CSS Policy 6-4. [redacted] testimony was corroborated by emails, which disclosed that he not only misused an Agency IS to access the ARC and identify POCs within [redacted]. he then continued to misuse the Agency IS to educate the [redacted] team on [redacted] in an effort to make the team more competitive on [redacted] and to demonstrate his value as a potential team member.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused an Agency IS to solicit business, in violation of NSA/CSS Policy 6-4.

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

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//~~FOUO~~) On 07 January 2014, the OIG sent [redacted] the tentative conclusion reached in the investigation. On 15 January 2014, [redacted] provided his response. In his response, [redacted] said that he provided [redacted] documents from an Agency IS in order to educate them about [redacted] and demonstrate his knowledge in the field. [redacted] stressed that the information he provided to [redacted] was already available to [redacted] affiliates with access to NSA/CSS's classified Intranet and did not include sensitive program information. [redacted] also said that he regretted his actions. Because [redacted] provided no new information requiring further investigation, our preliminary conclusion became final.

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

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

V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused an Agency IS to solicit business, in violation of NSA/CSS Policy 6-4.

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

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report of investigation will be provided to NSA/CSS Contracting, the SAE, and OGC Acquisition Law. Also, a summary of the findings will be forwarded to the ADS&CI.

Concurred by:

[Redacted Signature] Senior Investigator

[Redacted Signature] Assistant Inspector General for Investigations

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