

~~SECRET//REL TO USA, FVEY~~



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

**To:** Chief, D14 [redacted] **Date:** 1 May 2015

**From:** [redacted]

**Subject:** [redacted] Unauthorized Disclosure of PII

**File No:** IV-15-0028

**Precedence:** Routine

**Purpose:** To provide a summary report of investigation, and to recommend that this case be closed.

**Details:** (b) (3) - P.L. 86-36

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

**I. (U) Background**

(U//FOUO) On 22 July 2014, [redacted] Project Manager, [redacted] alleged to the OIG that [redacted] Data Scientist, [redacted] had disclosed her personal salary information to [redacted] former husband and [redacted] fiancé. At the time of the alleged disclosure, [redacted] was employed as a Cognos administrator for [redacted] on the [redacted] contract [redacted]

(b) (6)

(U//FOUO) During an OIG interview, [redacted] explained that in July 2014, [redacted] had via text message, requested that she increase her monetary contribution toward extra-curricular activities for their three children. [redacted] replied that she had taken a pay cut when she transitioned from contractor to government employment and therefore could not afford to increase her contribution. [redacted] allegedly replied via text that he knew that she "didn't take too much of a pay cut" and it was "only a \$5,000 pay cut." When she asked him why he thought it was only \$5,000, he allegedly replied "your grade."

(U//FOUO) [redacted] reported to the OIG that she had never told [redacted] her new salary as a civilian or her grade and step. Yet, he was correct;

<sup>1</sup> (U//FOUO) [redacted] waived her confidentiality on 14 November 2014.

<sup>2</sup> (U) "Cognos" refers to Cognos ReportNet, a web-based software product for creating and managing ad hoc and custom-made reports.

~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

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

she had taken a pay cut of exactly \$5,000. [redacted] concluded that the only way [redacted] could have known her salary was if someone with access to payroll information had provided it to him. [redacted] hypothesized that [redacted] by virtue of her position, had access to her salary and shared it with [redacted]

(b) (6)

II. (U) Issue(s)

(U//FOUO) Did [redacted] use NSA/CSS ISs to perform tasks not authorized by the contract, approved by the Contracting Office, or permitted by NSA/CSS Policy 6-4?

(U//FOUO) Did [redacted] disclose personally identifiable information (PII) concerning [redacted] without authorization?

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

III. (U) Applicable Standard(s)

- (U//FOUO) NSA/CSS Policy 6-4: *Contractor use of NSA/CSS Information Systems and Resources.*

(U) Policy.

1. (U) Contractors shall only use NSA/CSS ISs to perform tasks that are authorized by contract, approved by the Contracting Officer (CO), and permitted by this policy.
2. (U) Contractor employees using NSA/CSS ISs are subject to the entire NSA/CSS IT Policy Series the same as Government employees...

(U) RESPONSIBILITIES

...  
25. (U) All users shall:

...

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

- (U//FOUO) Department of Defense Directive 5400.11: *DoD Privacy Program.* (October 29, 2014)

(U) Policy.

- a. An individual's privacy is a fundamental legal right that must be respected and protected.

~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

...

3. (U) DoD personnel and DoD contractors have an affirmative responsibility to protect an individual's privacy when maintaining his or her PII.

...

f. Disclosure of records pertaining to an individual from a system of records is prohibited except with his or her consent or as otherwise authorized....

**(U) RULES OF CONDUCT**

(U) DoD personnel and DoD contractor personnel will:

- a. (U) Take action to ensure that any PII contained in a system of records that they access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.
- b. (U) Not disclose any PII contained in any system of records, except as authorized by The Privacy Act, or other applicable statute, Executive order, regulation, or policy. Those willfully making any unlawful or unauthorized disclosure, knowing that disclosure is prohibited, may be subject to criminal penalties or administrative sanctions.

...

f. (U) Safeguard the privacy of all individuals and the confidentiality of all PII.

**(U) DEFINITIONS**

PII. Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information. For purposes of this issuance, the term PII also includes personal information and information in identifiable form.

**IV. (U) Investigative Activity**

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

**A. (U) Document Review**

(S//REL) [redacted] reviewed [redacted] Top Secret account to determine if she

~~SECRET//REL TO USA, FVEY~~

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

conducted searches using [redacted] name or SID. [redacted] was observed running Mandatory Training Reports, Travel Reports and Leave Availability Reports on the [redacted] Cognos system as part of her job duties.<sup>3</sup> Due to technology limitations, [redacted] was unable to determine if she “clicked on” (selected) any hyperlinks within these reports. Therefore [redacted] was unable to determine if [redacted] accessed any of [redacted] PII. [redacted] did observe that [redacted] looked up [redacted] and [redacted] in JSignout and Microsoft Lync numerous times a day.<sup>4</sup> However, [redacted] did not message either individual on Lync.

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

(S//REL) [redacted] Audit of Cognos. [redacted] audited Cognos logs from 1 May 2014 through 31 July 2014. They reviewed all reports run by [redacted] during the timeframe. The audit log reflected no reports related to [redacted]. However, due to technology limitations, the audit records only included queries made on “saved” reports in the Cognos environment. Therefore, if a user ran a query one time, and did not save the search (i.e. if [redacted] searched Cognos for [redacted] on an ad hoc basis), there would be no audit record.

(U//FOUO) Email Evidence. The OIG reviewed [redacted] Top Secret and Unclassified email files (\*.pst) between September 2013 and September 2014. The OIG found two references to [redacted] only one of which was by name. The first was an August 2010 email between [redacted] and [redacted] in which they corresponded about job opportunities and their personal lives. The second was an email dated 17 September 2013, in which [redacted] wrote that her boyfriend’s [assumed to be [redacted] ex-wife [assumed to be [redacted] “works down the hall from me and I run in to her in the hall sometimes.” The vast majority of the email was work-related and concerned Cognos settings, issues, questions, tests, upgrade, errors, and migration. The OIG found no evidence that [redacted] emailed PII to anyone.

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

(b) (6)

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

B. (U) Interviews

(U//FOUO) [redacted] was interviewed on 5 February 2015 and provided the following sworn testimony.

(U//FOUO) As a Cognos administrator on the [redacted] contract, [redacted] could access the databases that Cognos drew from. Cognos pulls information from large databases (such as the [redacted] and the Human Resources Management System) and displays the desired information. The [redacted] contained all of the

<sup>3</sup> (U//FOUO) The [redacted] brings the data, tools, and a robust warehouse architecture together to enable the data exploration and visualization necessary to identify trends, support strategic planning and timely decision-making.

<sup>4</sup> (U//FOUO) [redacted] is [redacted] boyfriend (see interviews). JSignout is a web-based tool that indicates who is in and out of the office. Microsoft Lync is an instant messaging and synchronized collaboration tool.

<sup>5</sup> (U//FOUO) [redacted] organization.

~~SECRET//REL TO USA, FVEY~~

Defense Civilian Intelligence Personnel System (DCIPS) data and human resources data. Leave and Earnings statements, for example, are contained in the [redacted]

(U//FOUO) Part of [redacted] job was to build Cognos reports, test reports, and run reports requested by managers and other authorized users. Typically, [redacted] ran reports requested by the OIG, Human Resources (M), and Installations and Logistics (L), though any manager could request that she run one.

(U//FOUO) [redacted] never used Cognos for her own personal use. She only built reports requested by the customer. She knew that divulging the information that she acquired by means of her special access to someone not authorized to receive it would be a "no-no." She took the NSA-required Privacy Act training and denied ever divulging personally identifiable information to anyone.

(U//FOUO) [redacted] explained that [redacted] is her fiancé [redacted] [redacted] is his ex-wife. When asked if she had ever given [redacted] information she obtained about [redacted] through her work at the NSA, she stated that she had checked "J-Signout" for him when he wanted to know whether [redacted] was at work. However, that was all. In fact, [redacted] once asked her for his ex-wife's new phone number when she moved desks but she did not give it to him.

(U//FOUO) [redacted] has access to the [redacted] table that resides in the [redacted]. The table contains all of the information about civilian employees together in one place. [redacted] draws from this table to generate reports requested by several organizations. She recalled scrolling through the table to examine [redacted] information and did take note of the fact that [redacted] was a "14 step something." However, she denied disclosing [redacted] salary information to anyone. She did not recall which report that she was running, or for whom she was running the report, when she looked at [redacted] salary. [redacted] denied ever building a query to look for information about [redacted]

(U//FOUO) When asked how [redacted] knows how much [redacted] earns, [redacted] stated that she does not believe that [redacted] does know [redacted] salary. [redacted] has told [redacted] that she cannot pay for child care expenses because she took a pay cut when she became a civilian employee. [redacted] does not know whether [redacted] took a pay cut or not. [redacted] had suggested to [redacted] that he subpoena [redacted] payroll records to find out.

(U//FOUO) Later, [redacted] theorized about how [redacted] may have guessed [redacted] salary. In the summer of 2014, she and

~~SECRET//REL TO USA, FVEY~~

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

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

(b) (6)

~~SECRET//REL TO USA, FVEY~~

[redacted] discussed the possibility of [redacted] becoming a government employee. [redacted] speculated that she could be hired as a high GG-13 or a low GG-14. [redacted] may have based his guess about [redacted] salary on this discussion and his assumptions regarding her qualifications [redacted].

(U//FOUO) When asked why she checked J-Signout frequently for [redacted] [redacted] explained that [redacted] had an office right down the hall from her. There was a lot of conflict between them and she did not want to inadvertently run into [redacted] in the hall or bathroom.

(U//FOUO) When asked who [redacted] was, [redacted] explained that he is [redacted] current boyfriend. She admitted to checking J-Signout for his whereabouts because she was "being nosy."

(U//FOUO) [redacted] ex-husband of [redacted] and current fiancé of [redacted] was interviewed telephonically on 9 February 2015 and provided the following information.

(U//FOUO) [redacted] stated that he had "no clue" how much [redacted] actually earns. When he was married to [redacted] they discussed the possibility of her switching from contractor to government and talked about the grade at which she would likely be hired. The GS pay scale is publicly available online.

(U//FOUO) Once divorced, they argued over the bills for the children. They had an agreement that she was supposed to pay half. However, she complained about paying when she obtained a job with the government. She claimed she took a huge pay cut. However, [redacted] doubted her and "threw out numbers," guessing at her new salary. When he reached a number, she stopped denying it, so he speculated that he had guessed accurately. He has no hard evidence about what she earns, only guesses.

(U//FOUO) [redacted] said that he obtained [redacted] new phone number from the person who answered at her former work phone number. He did not recollect that individual's name.

(U//FOUO) [redacted] vehemently denied obtaining [redacted] salary information from [redacted].

## V. (U) Analysis

(S//REL) NSA/CSS Policy 6-4 states that contractors shall only use NSA/CSS ISS to perform tasks authorized by the contract, approved by the Contracting Officer, and permitted by the Policy. Although [redacted] admitted that she viewed [redacted] salary information in the routine course of her duties, there is

~~SECRET//REL TO USA, FVEY~~

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

no evidence to suggest that she misused an NSA IS. Neither [redacted] nor [redacted] uncovered any evidence that [redacted] built any unauthorized queries to uncover PII about [redacted]. [redacted] also denied using Cognos to look for information about [redacted].

(U//FOUO) [redacted] admitted that she checked [redacted] and [redacted] presence on JSignout and Lync; but there is no policy prohibiting such incidental use.

(U//FOUO) DoD Directive 5400.11 states that contractor personnel will not disclose any PII contained in any system of records, except as authorized. Although [redacted] viewed [redacted] salary information, she denied disclosing that information to anyone. [redacted] also denied learning [redacted] salary information from [redacted].

(b) (6)

(U//FOUO) The OIG uses a preponderance of the evidence standard in administrative and civil investigations. This standard is considered to be satisfied if, after weighing the evidence, there is a greater than 50% chance that the proposition is true. In this case, there is no physical evidence to show that [redacted] related the salary information she obtained to [redacted] (i.e. an email). Furthermore, when considering testimony, one witness claimed that [redacted] disclosed PII, while two witnesses claimed that she did not. Finally, the OIG found the subject, [redacted] to be a credible witness. Therefore, there was insufficient evidence to support the claim and the allegation was unsubstantiated.

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

**VI. (U) Conclusion(s)**

(U//FOUO) Unsubstantiated. The OIG did not find by a preponderance of evidence that [redacted]

1. Used NSA/CSS ISs to perform tasks not authorized by the contract, approved by the Contracting Office, or permitted by NSA/CSS Policy 6-4;
2. Disclosed personally identifiable information (PII) concerning [redacted] without authorization.

**VII. (U) Recommendation(s)**

(U//FOUO) In accordance with the information contained herein, this case should be closed. [redacted] will be notified of the investigative conclusion.

**VIII. (U) OGC Concurrence (as appropriate)**

(U//FOUO) N/A