NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

12 April 2013

IV-12-0101

Alleged Inappropriate Access to a Security Database

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

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

(U//~~FOUO~~) On June 19, 2012, the Associate Directorate for Security and Counterintelligence (ADS&CI) Chief of Adjudications (Q23), requested that the Office of the Inspector General (OIG) look into an allegation that [redacted] had inappropriately accessed a security database.

(U//~~FOUO~~) After interviewing witnesses and reviewing available documentary evidence, we determined that the preponderance of the evidence supports the conclusion that [redacted] inappropriately accessed and shared personnel privileged and Privacy Act information, in violation of 5 USC §552a (b), 5 CFR §2635.704, Joint Ethics Regulation DoD 5500.7-R, Section 2-301, DoD Directive 5400.11, DoD Privacy Program, Section E3.1.2, DoD Privacy Program DoD 5400.11-R, C4.2.1, and the NSA/CSS Personnel Management Manual (PMM) 30-2, Chapter 366, Section 2-2 (A,E&G) and Section 2-4 (D&E).

(U//~~FOUO~~) Copies of the OIG report will be forwarded to MR, Employee Relations, for appropriate action and D23, the Office of General Counsel (Administrative Law) for information. A summary of the investigative findings will be forwarded to Q234 (Special Actions) for information.

II. (U) BACKGROUND

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

(U) Introduction

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

(U//~~FOUO~~) On June 14, 2012, [redacted] contacted [redacted] Office of Personnel Security Staff, Q209, to request the removal of [redacted] access to a security database that was not needed for his current position. It had come to [redacted] attention that [redacted] an employee she supervises who had [redacted] had accessed the database. On June 19, 2012, Chief Q23, referred the matter to the OIG for investigation.

(b) (6)

(U//~~FOUO~~) [redacted] has worked in [redacted] since [redacted] under [redacted] Prior, he worked in the [redacted] His tenure with [redacted]

(U//~~FOUO~~) [redacted] works [redacted]

(U) Applicable Authorities

(U) The investigation looked at possible violations of the following authorities. See Appendix A for the full citations.

- (U) 5 U.S.C. § 552a (b)
- (U) 5 C.F.R. § 2635.704
- (U) DoD Directive 5400.11, DoD Privacy Program, E3.1.2.
- (U) Joint Ethics Regulation DoD 5500.7-R, Section 2-301
- (U) DoD Privacy Program DoD 5400.11-R, C4.2.1

- (U) NSA/CSS PMM, Chapter 366, Section 2-2 (A,E&G) and Section 2-4 (D and E)

III. (U) FINDINGS

(U//~~FOUO~~) Did [redacted] inappropriately access personnel privileged or Privacy Act information contained in a security database? And if so, did he share that information in violation of government regulations?

(U//~~FOUO~~) CONCLUSION: Substantiated. *The preponderance of the evidence supports the conclusion that [redacted] inappropriately accessed and shared personnel privileged and Privacy Act information[1], in violation of 5 USC §552a (b), 5 CFR § 2635.704, Joint Ethics Regulation DoD 5500.7-R, Section 2-301, DoD Directive 5400.11, DoD Privacy Program, Section E3.1.2., DoD Privacy Program DoD 5400.11-R, C4.2.1. and the NSA/CSS Personnel Management Manual (PMM), Chapter 366, Section 2-2 (A, E&G) and Section 2-4 (D&E).*

(U) Documentary Evidence

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

(U) **Master Index of Security Records**[2]

(U//~~FOUO~~) The OIG requested copies of the files that [redacted] had the *capability* of viewing given his security accesses. Specifically, we reviewed [redacted] and [redacted] security records as depicted in the [redacted] database. The files are attached in Appendices B and C, respectively.

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

(U) Testimonial Evidence

(U//~~FOUO~~) [redacted] was interviewed on September 6, 2012 and provided the following sworn testimony.

[1] (U) Personnel Privileged is any information or records concerning an individual which are maintained and used in the personnel management or personnel policy setting process. Privacy Act information is records which contain personal information about an individual (e.g. home address, home telephone number, birth date, details about financial, medical, and educational history) and which identifies the individual.

[2] (U//~~FOUO~~) [redacted] is a relational database consisting of numerous smaller databases such as human resources, medical, training, and security. The security portion of [redacted] is called [redacted] and contains the [redacted]

(U//~~FOUO~~) On June 14, 2012, Office Administrator [redacted] came to [redacted] and reported in confidence that [redacted] had been accessing information about his co-workers in a security database. [redacted] reported that [redacted] was discussing this personal information in an open forum with other co-workers. [redacted] stated that several office members were concerned that [redacted] would access information about them. [redacted] reported that [redacted] had accessed information about [redacted] and an unnamed acquaintance of [redacted] According to [redacted] was discussing allegations involving [redacted] and alleged [redacted]

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

(b) (6)

(U//~~FOUO~~) [redacted] subsequently discussed the rumors with [redacted] reported as follows:

- [redacted] had accessed information about [redacted] at [redacted] request. [redacted] was [redacted] was concerned about how her security profile would be impacted.
- [redacted] accessed information about [redacted] also at [redacted] request. [redacted] wanted to review [redacted] record because [redacted] had been in a similar [redacted] and [redacted] thought it might be illustrative.
- [redacted] denied accessing any information about [redacted] alleged [redacted] He stated that he did not have access to that kind of information.

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

- [redacted] denied looking up any other individuals at [redacted] request. He specifically denied attempting to query information related to the [redacted] of [redacted]
- When [redacted] prompted [redacted] to disclose any other records he had accessed, he admitted viewing [redacted] profile at [redacted] request. [redacted] was a contractor who supports [redacted] and wanted to find out his clearance expiration date.
- [redacted] also admitted that he had periodically accessed contractor clearance information at the request of co-workers and also in the course of his duties as a Contracting Officer's Representative (COR). [redacted] thought [redacted] made him more efficient in his job as a COR and a helpful colleague to his co-workers who frequently asked for clearance information on contractors. [redacted] did not know how

often [redacted] had done this, but [redacted] stated that [redacted]

- [redacted] showed [redacted] the link he was able to access in [redacted] did not know if [redacted] retained any other accesses.

(U//~~FOUO~~) [redacted] also spoke with [redacted] reported as follows:

- [redacted] admitted asking [redacted] to access her own security record as well as [redacted] record.
- [redacted] denied knowing or discussing any [redacted] information concerning [redacted]
- [redacted] denied asking [redacted] to access information about her [redacted]

(U//~~FOUO~~) [redacted] immediately reported this information to security, [redacted] and [redacted] subsequently informed [redacted] that [redacted] accesses were removed effective [redacted]

(U//~~FOUO~~) [redacted] was interviewed on September 27, 2012, and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] learned about the incident involving [redacted] on Monday, June 18, 2012 from [redacted] supervisor, [redacted] had emailed [redacted] on the evening of Thursday, June 14, 2012, but [redacted] was out of the office until Monday. When he arrived in the office Monday morning, [redacted] contacted [redacted] to have [redacted] accesses removed. [redacted] informed [redacted] that he had removed [redacted] accesses on Friday, June 15, 2012, upon direction from [redacted] In [redacted] absence, [redacted] had emailed [redacted] who had requested the removal.

(U//~~FOUO~~) It was not intended for [redacted] it was an oversight on [redacted] part. However, [redacted] is trying to rectify this problem. [redacted] did not know what the procedure was for individuals departing the organization, but

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

(b) (6)

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

thought that they were supposed to be outbriefed, and have their database accesses removed. He thought that it was the administrative officer's responsibility to notify that an individual had left and that their accesses needed to be removed. However, was not certain whether there was an organizational SOP or checklist. When asked whether could remove a person's access per the administrative officer's request alone, he was not certain.

(U//~~FOUO~~) explained that removing accesses was a complicated prospect because of the numerous personnel who are deployed around the Agency. Those individuals may no longer work in directorate, but still require security accesses to do the job. When they arrive at their new assignments, they might complain if their access is restricted, but they generally do not hear from them if they have more accesses than they need. knew of no special accesses given to CORs to support their role.

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

(U//~~FOUO~~) After it was discovered that had been accessing the security database, did a scrub of their databases. They reviewed of them. In the future, they hope to do a better job managing who leaves the organization, with the help of an HR representative to

(U//~~FOUO~~) had access to the which is the primary clearance database for all agency affiliates. Some people refer to it as but that is a misnomer, because contains more than Security, like Human Resources. The is one of the database files within Within the had several "views" available to him. Among the views available was , which was a structured display of the data. contained clearance information, badge information, and adjudicative criteria.

(U//~~FOUO~~) had only "query" capability for all of the views except one – – for which he had "update"

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

permissions. Case Cost showed the monetary cost of a clearance investigation for statistical purposes.[3]

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

(U//~~FOUO~~) did not believe that

(U//~~FOUO~~) confirmed that would have been able to view all the pages of and security profiles, including the adjudicative criteria pages.

(U//~~FOUO~~) Chief, responded to a question posed by the OIG on July 17, 2012. In her response, she provided the following information.

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

(U//~~FOUO~~) spoke with developers to determine

(U//~~FOUO~~) Office Manager, was interviewed on November 2, 2012, and provided the following sworn testimony.

(U//~~FOUO~~) did not personally observe or access the security database. Instead, heard about the incident on two separate occasions from two co-workers who were concerned that their personal information might be accessed as well: and Witness #1[4]. According to her sources, had asked to access information pertaining to the They also accessed the information of co-worker did not know what, if anything, they had seen in the record (she knew neither of their names). heard that records contained

(b)(6)

[3] (U//~~FOUO~~) In an email dated 9/27/12, amended his earlier statement and reported that also had "update" capability for the data view. it was unrelated to personnel security.

[4] (U//~~FOUO~~) Witness #1 requested that his/her name be kept confidential.

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

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

(b)(6)

something from her [redacted] did not see it herself, but heard that [redacted] and possibly others discussed [redacted] record in the aisle prior to [redacted] arrival in the morning. [redacted] did not know whether [redacted] had accessed [redacted] information. [redacted] did not know if [redacted] had accessed any other files.

(U//~~FOUO~~) [redacted] reported these events to [redacted] supervisor. Although she was not a first-hand witness, [redacted] knew that [redacted] and Witness #1 were not comfortable reporting it themselves. [redacted] thought maybe two days elapsed between the time she first heard the rumors and when she reported it to [redacted]

(U//~~FOUO~~) [redacted] Business Manager, [redacted] was interviewed on November 7, 2012, and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] heard from a co-worker, Witness #1, that [redacted] had given [redacted] the names of [redacted] and [redacted] to look up in whatever security database [redacted] could access: [redacted] When they determined what they could see, [redacted] and [redacted] then looked up co-worker [redacted] did not hear any other individuals mentioned, but speculated that [redacted] and [redacted] had attempted to query information related to other people as well.

(U//~~FOUO~~) [redacted] did not hear anything about what was contained in [redacted] file or her [redacted] file. However, she did hear that [redacted] record contained something related to [redacted]

(U//~~FOUO~~) [redacted] source of information, Witness #1, heard about the events directly from [redacted] in turn, discussed these events with [redacted]

(U//~~FOUO~~) **Witness #1,** [redacted] was interviewed on November 9, 2012, and provided the following sworn testimony.

(U//~~FOUO~~) told Witness #1 that she and had accessed security record. Witness #1 believed that this occurred in the January/February 2012 timeframe. told Witness #1 that She also told Witness #1 that had When asked whether obtained this information from the database accessed by Witness #1 was not certain. Witness #1 did not know access level and believed he could only see a certain amount. However, Witness #1 assumed the information must have come from the database because, "where else would she have got it?" 'stays to herself' and would not have shared that type of personal information with

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

(U//~~FOUO~~) In the March/April timeframe, Witness #1 was visiting co-workers Witness #1 saw (also from the visiting in his cubicle. Witness #1 believed that and were pulling up information on the database, as evidenced by checking in and out of the cubicle to see if anyone was coming. Twenty minutes later, returned and began whispering with a co-worker, Witness #1 overheard bits and pieces of the conversation and concluded that and had accessed Witness #1's security file and was now discussing it with Witness #1 heard no details about the contents of file.

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

(b) (6)

(U//~~FOUO~~) Witness #1 did not know whether and had attempted to access anyone else's record, aside from Witness #1s and However, Witness #1 believed that tried to find information about Witness #1 did not know whether was trying to access information concerning but confirmed that told her that

(U//~~FOUO~~) Witness #1 never spoke with about these events. Witness #1 commented that attempts to access security related information on affiliates anytime someone asks. When co-workers had an inquiry, the common refrain was, "go ask he can look up anyone's information." Witness #1 believes it goes on all the time.

(U//~~FOUO~~) Business Manager, was interviewed on September 28, 2012, and provided the following sworn testimony:

(U//~~FOUO~~) knew that and was able to access people's security information for the She assumed he had this access because his program was high profile and also because

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

(U//~~FOUO~~) Although she reported the ongoing issues to her SSO, she was very concerned about how the would affect her record. In June, she went to the and asked to check her record for any indications that the were affecting her clearance. Although she was standing next to him in his cubicle, could not see the screen and did not know exactly what accessed. pulled up her record and told her that "it didn't show anything." thought that meant that did successfully retrieve her record and may have seen other information related to her, but did not see anything

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

(U//~~FOUO~~) thought perhaps the reason her record showed nothing was because of Consequently, asked to look up co-worker record, as knew had gone through something similar. thought was and went through the same kind of accessed record and said he did not see anything in hers either. did not tell about anything derogatory in record.

(b)(6)

(U//~~FOUO~~) did not ask to look up anyone else. She did not ask to look up her record. She does not even know does not know where the rumors came from regarding her but speculated that it may have come from previous joking when said that it would be nice if they could look up people's records, like

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

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

(b)(6)

(U//~~FOUO~~) Following these events, [redacted] returned to her desk [redacted]. When she returned, she told her co-worker, [redacted] about what had happened. She told him that [redacted] had looked at her file and [redacted] file and did not see anything. [redacted] stated that the only person she told about database access was [redacted] though others may have overheard them talking. [redacted] said nothing about the contents of [redacted] record. She does not know where the rumors about the contents of [redacted] record came from.

(U//~~FOUO~~) [redacted] was not concerned about the propriety of asking [redacted] to access her security records, as they were her own. She was concerned about how [redacted] would affect her job and that is the only reason she asked. As for asking [redacted] to obtain information concerning [redacted] contends that she did not see the contents, so she did nothing wrong. However, she did acknowledge that it may have been inappropriate to ask for [redacted] information. [redacted] objected to the characterization that she had inappropriately accessed a security database, because she does not have an account and cannot access anything.

(U//~~FOUO~~) [redacted] was interviewed on September 13, 2012, and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] has had limited security access to personnel information since he started at [redacted]. His access consisted of a limited view of the security application in [redacted] He did not have "full" access, which he believes consists of [redacted] He could only view the information contained in the database, he could not modify it. Never in his career had he modified any of the information.

(U//~~FOUO~~) Shortly after [redacted]

[redacted] As he was doing this, he checked the security database and noticed that he still had access. He kept expecting it to disappear, but it never did.

(U//~~FOUO~~) [redacted] assumed that he had the access because of what he was continuing to do. He was still fulfilling the role he had in [redacted] He remained a COR and was still processing clearance certification requests, badge requests, visitor requests, and anything related to processing contractors and new employees. Access to the database continued to be of use to him over the years as he processed contractors and new civilians coming on board. When he processed a visit request, for instance, he did not have to request the individual's SSN and he could check to see what accesses they had before filling out the request. He could see if a contractor's clearance was active and if their polygraph or background investigation was out of scope (older than 5 years). All of [redacted] managers knew that he could get this kind of information and would come to him often to ask him to process the requests because he could so do much more quickly than through the normal channels. Everyone knew he [redacted] He was considered the [redacted]

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

(b)(6)

(U//~~FOUO~~) It never really occurred to [redacted] to notify [redacted] that he retained access to the [redacted] database, because he thought they let him keep it on purpose. He would have assumed had they not meant for him to have it that [redacted] would have taken access away from him [redacted] guessed that [redacted] thought he should have it [redacted] and the fact that he was still a COR. [redacted] admitted that other CORs, as a rule, do not have access, and have to request the information they need. In hindsight, [redacted] stated that he probably should have notified [redacted]

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

(U//~~FOUO~~) On Monday, June 11, 2012, [redacted] co-worker and friend, [redacted] (who worked [redacted], came to visit [redacted] had been [redacted] She asked [redacted] to look at her security record to see if her account had been noted to reflect [redacted] In a lapse of judgment he did access her record. As in the past, he could see the standard information, like place of birth and date of birth. He

did not see anything related to [redacted] however, and said, [redacted] I can't see anything." When asked what he expected to see in [redacted] file given his past experience with the database, [redacted] replied that he was not sure since he had never tried to find personal information before and thought there might be some kind of "notation" with regards to [redacted]

(U//~~FOUO~~) When her own record failed to reflect anything related to [redacted] said that co-worker [redacted] had gone through something similar and asked [redacted] to look at her record as well. In his second lapse of judgment, he pulled up [redacted] record. As in [redacted] case, he saw the boilerplate information, but nothing related to [redacted] He saw nothing related to [redacted] and no derogatory information. He told [redacted] that he did not see anything. When asked why he thought there would be a different outcome in [redacted] case, [redacted] replied that [redacted] record might contain more information because [redacted] whereas [redacted]

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

(U//~~FOUO~~) A few days later, on June 15, 2012, [redacted] supervisor, [redacted] asked [redacted] about the incident. [redacted] surmised that sometime between June 11 and June 15, [redacted] had told some individuals that he had attempted to access [redacted] security records. Someone in earshot must have overheard and become concerned that he would access their information. [redacted] does not know who [redacted] told, but is certain she had to have told someone on the [redacted] because he did not. [redacted] told [redacted] what had happened and she contacted [redacted] ADS&CI, to have his access removed. [redacted] believes [redacted] subsequently removed his access to the security data applications in [redacted] He does not know for certain, however, since he has not touched the database since June 14, 2012.

(b) (6)

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

(U//~~FOUO~~) [redacted] was asked about rumors circulating concerning [redacted] record and [redacted] On four separate occasions, [redacted] stated that he did not see anything in [redacted] record related to [redacted] and did not share the contents of [redacted] record with anyone. He had no idea where the rumors came from.

(b) (6)

(U//~~FOUO~~) stated that also asked him to look up but he refused. He told her that was enough.

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

(U//~~FOUO~~) When first started in a contractor named asked him to check when his background reinvestigation was due and provided the information. Outside of these three occasions and does not recall querying anyone else's record at their request. However, he makes a distinction in case. He accessed records for security processing reasons, not for personal issues. The incident with was the first and only time he looked up personal information. He could not fix a number on how many contractor records he had accessed over the years, but thought it was "tons." was emphatic that he only did this to facilitate the clearance process.

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

(U//~~FOUO~~) admitted he should not have accessed the database for personal information, but he thought it was just between him and In the back of his mind, he knew it was wrong, but he was attempting to help a friend. He asked not to tell anyone that he accessed the records, but she did. He is completely remorseful, and should have known better. He cannot believe he did it and feels horrible about it. He wants to move forward and rebuild his career.

(U) Analysis and Conclusions

(U//~~FOUO~~) Due to those pages he had the *capability* of viewing in concert with his testimony.

(U//~~FOUO~~) Furthermore, direct eye-witness testimony outside of and was lacking. What the OIG did learn from other witnesses was based upon 2nd and 3rd hand information, combined with rumors, innuendo, and supposition.

(U//~~FOUO~~) Nevertheless, the preponderance of the evidence demonstrated the following:

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

1.(U//~~FOUO~~) [redacted] accessed the security database for other than authorized purposes and official use. By his own admission [redacted] accessed [redacted] and [redacted] records "to help a friend." Furthermore, [redacted] argument that he had official need for the database is not credible. He testified that he believed he retained access because of his status as a COR. However, he admitted that CORs, as rule, do not have access to the same database.

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

2. (U//~~FOUO~~) [redacted] disclosed information contained in the database to [redacted] knowing that [redacted] did not have a need for it in the performance of her assigned duties. He stated that she wanted the information for personal reasons. Furthermore, he asked [redacted] not to tell anyone that he had accessed the records, knowing full well that neither of them had an official reason for accessing it.

3. (U//~~FOUO~~) [redacted] failed in his duty to protect the sensitive information to which he was granted access, demonstrating a lack of discretion and trustworthiness. He admitted that accessing [redacted] and [redacted] records reflected a "lapse of judgment" on his part.

4. (U//~~FOUO~~) [redacted] failed in his duty to protect personnel privileged and Privacy Act information.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] inappropriately accessed and shared personnel privileged and Privacy Act information, in violation of 5 USC §552a (b), 5 CFR §2635.704, Joint Ethics Regulation DoD 5500.7-R, Section 2-301, DoD Directive 5400.11, DoD Privacy Program Section E3.1.2., DoD Privacy Program DoD 5400.11-R, C4.2.1, and the NSA/CSS Personnel Management Manual (PMM), Chapter 366, Section 2-2 (A,E&G) and Section 2-4 (D&E).

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

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

(U//~~FOUO~~) On 11 April 2012, [redacted] responded via email to the OIG tentative conclusions with the following:

> (U//~~FOUO~~) I have read over the conclusion to the incident report that has been prepared by the Office of Inspector General (OIG) and I unfortunately, agree with my wrong doing. For the past 10 months, this situation has been on my mind and I cannot say enough that I am truly sorry for what I did. I temporarily had a lapse of good judgment and as long as I am allowed to be a [sic] remain a valuable asset to NSA, I will strive to rebuild my once, stellar reputation that I have had for the past [redacted] years.
>
> (U//~~FOUO~~) I have also attached the self-report that I submitted to [redacted] after the incident occurred in June 2011 to this e-mail.
>
> (U//~~FOUO~~) If there are any questions, please do not hesitate to contact me.

(U//~~FOUO~~) The "self report" to [redacted] noted by [redacted] and dated 15 June 2012, states the following:

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

> (U//~~FOUO~~) I completely remorsefully need to share with you a violation of a security information related database (i.e. Personal Privileged Information) that I committed on Monday, 11 June 2012.
>
> (U//~~FOUO~~) Before I begin, I need to tell you that [redacted] and for some reason, I have retained my access to the Security Data Applications tab in [redacted] I thought that I retained this access because of [redacted] and also my continued role as a Contracting Officer's Representative (COR) for several NSA contracts. [redacted] and also outside of the directorate in the various other directorates that I have worked in, I have served and continue to serve as a COR and I used the information stored in this tab to gather information on the contractors that I sponsor for badging and Clearance Certification Requests (CCRs).

(b) (6)

> (U//~~FOUO~~) On the date noted above, a former co-worker of mine, [redacted] knowing that I have/had limited [redacted] access to personal information, approached me and asked me if I could look at her online security record and see how [redacted] would be documented and if any action had been taken to note her record. I work on the [redacted] assured me that she would not tell anyone of my action which I fully realize was completely wrong. Regretfully and at a moment of lapsed poor judgment while [redacted]

[redacted] was at my desk, I attempted to access her security record. When I was not able to see anything in her file, she then asked me to access someone else's security record in her group, [redacted] who in the past, experienced a similar situation of her own. I did as she requested and again like in [redacted] situation, I was not able to access any information. [redacted] then left my desk.

(U//~~FOUO~~) On Thursday, 14 June 2012, I was asked by my new manager, [redacted] to meet with her to discuss an issue that she became aware of. When I met with her, she questioned me about my attempt to access [redacted] information on a former co-worker. During our discussion, [redacted] name was mentioned and apparently at some point, [redacted] [redacted] returned back to her office on the [redacted] and discussed my failed attempt to review her security record and that of [redacted] -At least one person in the listening area heard what was about what was attempted and either he or she became concerned that I would look up their security related information.

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

(U//~~FOUO~~) The subsequent action that was taken by [redacted] from our meeting was that she asked me how I had access to the security related information and after I told her, then I volunteered [redacted] sent an e-mail to [redacted] requesting that my access be removed on Thursday, 14 June 2012. To date, I do not know if this action has been completed and I have not attempted to access the Security Data Application again.

(U//~~FOUO~~) After much anguish over my poor judgment call and after speaking to you today, I decided to self-report this incident in advance of any correspondence being sent to you from my [redacted] management chain. I cannot tell you how badly I feel about this situation because in my almost [redacted] years at the agency, I have had a pristine record, free of *any* blemishes. I truly hope that this action does not result any disciplinary action against me but if it does, then it is truly my fault because I knew better than to honor the inappropriate requests of another affiliate who does not have a need to know. I look forward to and hope to rebuild my reputation at NSA that unfortunately, now I believe is tarnished.

(b) (6)

(U//~~FOUO~~) If you have any questions, please do not hesitate to contact me.

(U//~~FOUO~~) [redacted] response was considered; however, it did not change the conclusions in this case.

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

VI. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] inappropriately accessed and shared personnel privileged and Privacy Act information, in violation of 5 USC §552a (b), 5 CFR §2635.704, Joint Ethics Regulation DoD 5500.7-R, Section 2-301, DoD Directive 5400.11, DoD Privacy Program Section E3.1.2., DoD Privacy Program DoD 5400.11-R, C4.2.1, and the NSA/CSS Personnel Management Manual (PMM), Chapter 366, Section 2-2 (A,E&G) and Section 2-4 (D&E).

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

VII. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report of investigation will be forwarded to MR, Employee Relations, for appropriate action and D23, the Office of General Counsel (Administrative Law) for information. A summary of the investigative findings will be forwarded to Q234 (Special Actions) for information.

[redacted]
Investigator

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

Concurred by:

[redacted]
Assistant Inspector General
for
Investigations

(U) APPENDIX A

(U) Applicable Authorities

(U) 5 USC §552a – Records maintained on individuals

(b) Conditions of Disclosure – No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be - …

(U) 5 CFR §2635.704, Code of Ethics for Government Service, - *Use of Government Property*

(a) Standard. An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes.

(U) Joint Ethics Regulation, DoD 5500.7-R, Section 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.

(U) DoD Privacy Program, DoD 5400.11-R, May 14, 2007. *Non-Consensual Conditions of Disclosures.*

C4.2.1.1. Records pertaining to an individual may be disclosed to a DoD official or employee provided:

C4.2.1.1.1. The requester has a need for the record in the performance of his or her assigned duties.

(U) DoD Directive 5400.11, DoD Privacy Program, Enclosure 3, *Rules of Conduct.*

Section E3.1 DoD personnel shall:

E3.1.2. Not disclose any personal information contained in any system of records, except as authorized by Reference (d), or other applicable laws or

regulations. Personnel willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

(U) NSA/CSS PMM 30-2, Chapter 366 – *Personal Conduct*

Section 2-2 – Personnel Security Requirements:

Employees granted access to classified information and Sensitive Compartmented Information must be stable; trustworthy; reliable; of excellent character, judgement, and discretion; and of unquestioned loyalty to the United States. Any conduct, including off-duty conduct, that brings into question these character traits may be cause for appropriate security action and in some cases administrative action. The following illustrations are provided as examples and are not inclusive:

A. Behavior, activities, or associations that raise doubts about an individual's reliability, trustworthiness, or loyalty to the U.S. Government;

E. Criminal, dishonest, or other conduct that would reflect adversely on the individual's reliability or trustworthiness;

G. Behavior which reflects a lack of judgement and discretion or which offers the potential for undue influence, duress, or exploitation.

Section 2-4 – Safeguarding Information:

Employees will protect all classified, Sensitive Compartmented Information (SCI), unclassified sensitive, personnel privileged, Privacy Act, and non-public information and/or material in accordance with all applicable laws, regulations, and procedures. All classified material must be appropriately secured and protected regardless of the manner acquired. NSA employees must ensure that the intended recipients of classified information possess the appropriate clearance and have a valid need-to-know. The following definitions apply:

D. Personnel Privileged-Any information or records concerning an individual which are maintained and used in the personnel management or personnel policy setting process.

E. Privacy Act Information-"Records" that are maintained in a "system of records", regardless of physical form or characteristics, which contain personal information about an individual (e.g. home address, home

telephone number, birth date, details about financial, medical, and educational history) and which identifies the individual. This information may only be accessed, used, or disseminated for official purposes described in Agency regulations.

(U) APPENDIX B

(U) [redacted] Record

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

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

(U) APPENDIX C

(U//~~FOUO~~) [redacted] **Record**

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

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

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

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

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

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

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

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

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

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