

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY
SERVICE**



**INSPECTOR GENERAL
REPORT OF INVESTIGATION**

19 December 2014

IV-15-0021

Alleged Mishandling of PII

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~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)

(U//~~FOUO~~) This investigation was conducted in response to a complaint alleging that an Agency employee received possible personal security information described as an image of a picture badge, or the image of an affiliate used on a picture badge, from an unidentified Associate Directorate for Security and Counterintelligence (ADS&CI) employee. The complainant believed that the recipient of the image may have a romantic interest in the person whose information was exchanged.

(U//~~FOUO~~) During the course of the investigation it was determined that [redacted] expressed interest to [redacted] a friend in [redacted] about an NSA Police Officer subsequently identified as [redacted]. Her interest was relayed by [redacted] to [redacted]. [redacted] was simply interested in learning the identity of the officer. [redacted] contacted [redacted] and described the officer's physical characteristics. [redacted] believed that the inquiry was for official purposes and, based upon the description, believed that the officer was [redacted]. In order to be certain, she scanned a picture of [redacted] with his name beneath it, which was maintained in the NSAP office. [redacted] emailed the image to the [redacted] [redacted] who forwarded the image via email to [redacted] then emailed the image of [redacted] to [redacted].

(U//~~FOUO~~) The OIG concluded that the image of [redacted] coupled with his name, constituted personally identifiable information (PII). By sharing PII without an authorized purpose and without the required disclaimer, [redacted] and [redacted] were in violation of NSA/CSS Policy 1-22, *Protecting Privacy on NSA/CSS Electronic Information Systems*, Paragraphs 13 (a) & (b).

(U//~~FOUO~~) A copy of this report will be forwarded to MR/Employee Relations for any action deemed appropriate, and a summary will be provided to the Chief, Q2 Personnel Security, for information.

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

II. (U) BACKGROUND

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

(b) (6)

(U) Introduction

(U//FOUO) [redacted] She has been an NSA employee since [redacted] and has worked in [redacted] since [redacted].

(U//FOUO) [redacted] She has been an NSA employee since [redacted] and has served as the [redacted] since October 2003.

(U//FOUO) [redacted] She has been an NSA employee since [redacted] and has spent her entire career in positions supporting [redacted].

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

(U) Applicable Authorities

(U) The investigation looked at possible violation of the following authority.

(U) NSA/CSS Policy 1-22, *Protecting Privacy on NSA/CSS Electronic Information Systems*

13. (U) Authorized users of NSA/CSS internal electronic information systems shall:

a. (U) When sending PII over email, certify: that there is an official need; that addressee(s) (including "cc" addressees) are authorized to receive it under the Privacy Act; and that it is protected from unauthorized disclosure, loss, or alteration; and,

b. (U) When transmitting personal information over email, apply the following statement at the beginning of the email: "Privacy Sensitive – any misuse or unauthorized access may result in disciplinary action."

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

III. (U) FINDINGS

(U//~~FOUO~~) **ALLEGATION:** [redacted] and [redacted] transmit PII over NSA/CSS information systems without an official purpose?

(U//~~FOUO~~) **CONCLUSION:** Substantiated. The preponderance of the evidence supports the conclusion that [redacted] and [redacted] emailed PII for unauthorized purposes and without the required disclaimer in violation of NSA/CSS Policy 1-22, Paragraphs 13 (a) & (b).

(U) Evidence

(U) Documentary Evidence

(U//~~FOUO~~) On 4 September 2014 at 1411 hours, [redacted] sent [redacted] an email, Subject line [redacted] with a scanned picture of [redacted] named [redacted].jpg," attached. [redacted] is written on the bottom of the picture. In the body of the email, [redacted] wrote: [redacted] Here is a picture of [redacted] I blocked out his information since I'm emailing this.

(U//~~FOUO~~) On 4 September 2014 at 1415 hours, [redacted] forwarded the same email with the picture attached to [redacted]. Nothing was written in the body of the email. A copy of that email chain is attached at Appendix A.

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

(U//~~FOUO~~) On 4 September 2014 at 1421 hours, [redacted] forwarded the same email to [redacted] however, she deleted the information identifying [redacted] and [redacted] and simply emailed the picture with nothing written in the body of the email. A copy of that email is attached at Appendix B.

(U//~~FOUO~~) On 9 December 2014, [redacted] emailed the OIG the following information, in part, in response to questions about whether or not her office considered the mishandling of PII as described in this case to be a PII Breach.

(U//~~FOUO~~) In this particular instance, DJ4 made the determination that this was not a reportable PII breach. Make no mistake that the image should not have been pulled for this purpose, nor should it have been shared with the individual who expressed interest in the officer. However, DJ4 determined that because of the actions and discussions that occurred when this came to light, combined with the fact that the photo, to the best of our knowledge, never left positive government control, there was a negligible chance that harm would come to the individual. Since the IG was working this clear cut case of misconduct, DJ4 deferred to the actions of the OIG. Had the IG not been handling the case, DJ4 would

Personnel Privileged Information

have run an investigation and conferred with all individuals involved and the leadership of the principles. If we determined legal action should have been taken we would have coordinated with OGC. Any disciplinary action would have been coordinated with leadership and HR. In this case, those involved acknowledged their actions were inappropriate and seem to have learned their lesson about only using PII for the purposes it is collected. Again, while DJ4 did not determine this to be a reportable PII breach, it is a clear case of misconduct.

(U) Testimonial Evidence¹

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

(U//FOUO) [redacted] was interviewed on 31 October 2014, and provided the following information.

(U//FOUO) [redacted] acknowledged that she received an image of an NSA Police Officer, name unrecalled, from [redacted], whom she described as a "friend in security." Although [redacted] did not ask that [redacted] send her the picture, it was received after she had expressed an interest in the officer, later identified as [redacted] to [redacted]

(U//FOUO) [redacted] was interviewed telephonically on 12 November 2014, and provided the following pertinent information.

(U//FOUO) After hearing that [redacted] had an interest in finding out the name of a NSA Police Officer, [redacted] called [redacted] to see if she could determine his name. [redacted] did not request a picture of the officer, but she did eventually receive a scanned image from who she initially believed was [redacted]. On 13 November 2014, [redacted] contacted the OIG via email to advise that it was actually [redacted] who sent her the picture of [redacted]. [redacted] subsequently emailed the scanned photo to [redacted].

(U//FOUO) [redacted] was interviewed telephonically on 25 November 2014, and provided the following information.

(U//FOUO) [redacted] acknowledged accessing a hardcopy image of [redacted] from the local NSA police files, scanning the picture, and emailing it to [redacted].

(U//FOUO) [redacted] was interviewed under oath on 18 December 2014, and provided the following sworn testimony.

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

(U//FOUO) She was contacted by [redacted] in an effort to determine the identity of a specific NSAP officer. A physical description was given and, based upon that, she believed the officer to be [redacted]. [redacted] believed that the query was official in nature, potentially resulting from a complaint about the officer. At no time was she informed that the request was for personal reasons. [redacted] decided to scan a copy of [redacted] picture and send it to [redacted] so that they could make sure he was the one that they were trying to identify. She heard nothing more about the matter until being contacted by an OIG Hotline manager.

¹ (U//FOUO) All of the individuals interviewed denied having user access to retention badge images.

(U//FOUO) [redacted] was telephonically interviewed on 25 November 2014, and provided the following pertinent information.

(U//FOUO) [redacted] acknowledged sending the image of [redacted] to [redacted] after having received it via email from [redacted]. [redacted] confirmed that when she forwarded the picture she knew it was not for an official purpose.

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

(U) Analysis and Conclusions

(U//FOUO) NSA/CSS Policy 1-22 states that when sending PII via email there must be an official need, the recipients must be authorized to receive the PII under the Privacy Act, and it must be protected from disclosure, loss or alterations. Further, there is a requirement to apply a "Privacy Sensitive" statement at the beginning of an email containing PII. When [redacted] and [redacted] emailed the picture of [redacted] it was done without an official need, and they failed to include a "Privacy Sensitive" statement in the email. As a result, the preponderance of the evidence supports the conclusion that [redacted] and [redacted] were in violation of NSA/CSS Policy 1-22, Protecting Privacy on NSA/CSS Electronic Information Systems, Paragraphs 13 (a) & (b). [redacted] believed that the query was for official purposes; therefore, we did not find that she was in violation of applicable policy.

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

V. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//~~FOUO~~) On 17 December 2014, [redacted] provided the following response to the OIG tentative conclusions.

(U//~~FOUO~~) I would like to respond to the tentative conclusions below.

(U//~~FOUO~~) Even though I did not request the picture that I received via email, I did forward it. I honestly have to say though that I was not aware that the picture and the name together was a violation of PII Policy. I would never intentionally violate any NSA Policy and I sincerely apologize for doing so. I had no idea that the information that I forwarded was PII and truly regret my actions.

(U//~~FOUO~~) I have been with NSA for [redacted] years and have been committed to upholding all policies and procedures. I have strived to be a good employee and now understand that my actions were in violation of the Policy stated below. I respectfully request that this not be a part of my permanent record.

(U) Thank you for the opportunity to respond.

(U//~~FOUO~~) On 18 December 2014, [redacted] provided the following response to the OIG tentative conclusions.

(U//~~FOUO~~) I did not knowingly distribute PII information, as I did not open the email attachment that was forwarded to me by [redacted]. I did, however, forward the information via email to [redacted]. The signature block of all my emails lists the following statement, "This email may contain information subject to the Privacy Act." I was unaware that a person's name and picture together deemed the information PII. I apologize for any involvement that I had in this matter and know that in the future I will not forward any personal information via email.

(U//~~FOUO~~) On 18 December 2014, [redacted] provided the following response to the OIG tentative conclusions.

(U//~~FOUO~~) I was unaware that sending a picture along with a name violated via the agency policy concerning personally identifiable information (PII). The email was disseminated within the [redacted] channels and I believed that it would remain within the [redacted] channels. I never thought it would be disseminated any further and thus would be protected accordingly. Obviously, that was not the case. [redacted] regularly sends PII information, within [redacted] channels, without using the "PII caveat." An example of this is timecards. I regularly receive timecards via email for entry into DCPS system and the PII caveat is not on a lot of the emails I receive. The request was at the direction of my parent organization and I had no foreknowledge of the real reason behind the request. I would not knowingly violate any agency policy or regulation. If I had known beforehand what the real motive behind the request was for, I would have refused the request. I will make sure all emails that I send in the future has the "PII caveat" on them to protect myself from any other policy violations.

(U//~~FOUO~~) The responses noted do not change the findings with regard to [redacted] and [redacted] however, we determined that [redacted] did not violate policy.

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

(b) (6)

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

VI. (U) CONCLUSION

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

(U//~~FOUO~~) The OIG concluded that the image of [redacted] coupled with his name, constituted Personnel Privileged Information (PII). By sharing PII in the manner described, where there was no authorized purpose, the preponderance of the evidence supports the conclusion that [redacted] and [redacted] were in violation of NSA/CSS Policy 1-22, Protecting Privacy on NSA/CSS Electronic Information Systems, Paragraphs 13 (a) & (b).

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

Personnel Privileged Information

VII. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report of investigation will be provided to MR, Employee Relations for any action deemed appropriate.

(U//~~FOUO~~) A summary of this report of investigation will be provided to the Chief, Q2, Personnel Security, for information.

[Redacted Signature]

Deputy Assistant Inspector General
for Investigations

Concurred by:

[Redacted Signature]

Assistant Inspector General
for Investigations

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

APPENDIX A

(U) Email Chain

Personnel Privileged Information
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

APPENDIX B

(U) Email from [redacted] to [redacted]

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

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

From: [redacted]
To: [redacted]
Subject: (U) Email Request
Date: Tuesday, November 25, 2014 11:27:28 AM
Attachments: [redacted].jpg

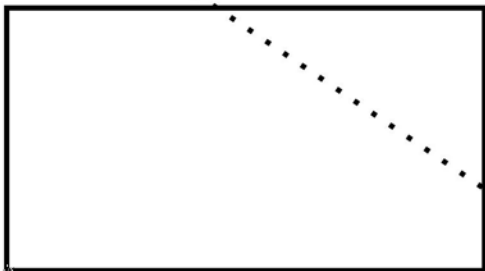
Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

[redacted]

Per our conversation and your request for me to forward this email to you, please see the below.

Thanks,

[redacted]



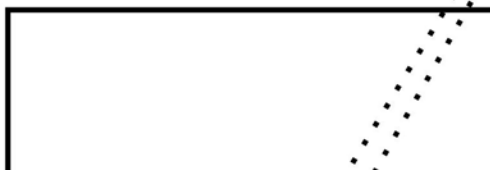
(b) (3) - P.L. 86-36

"This email may contain information subject to the Privacy Act."

From: [redacted]
Sent: Thursday, September 04, 2014 2:15 PM
To: [redacted]
Subject: FW: (U) [redacted] Picture

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

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~




"This email may contain information subject to the Privacy Act."

From: [redacted]
Sent: Thursday, September 04, 2014 2:11 PM
To: [redacted]
Subject: (U) [redacted] Picture

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

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



Here is a picture of . I blocked out his information since I'm emailing this.



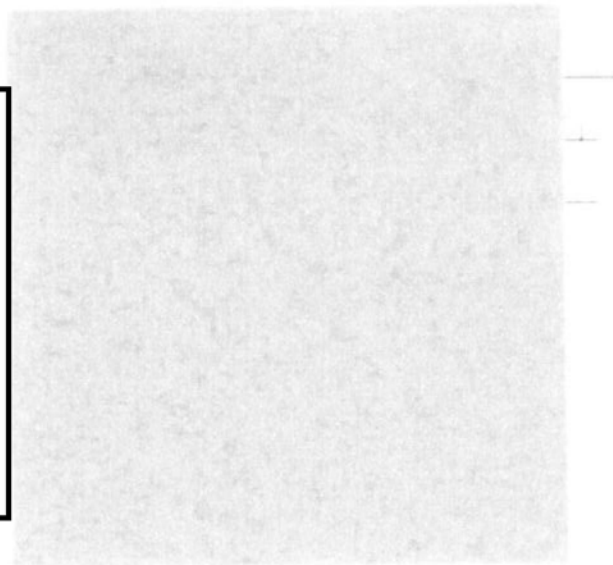
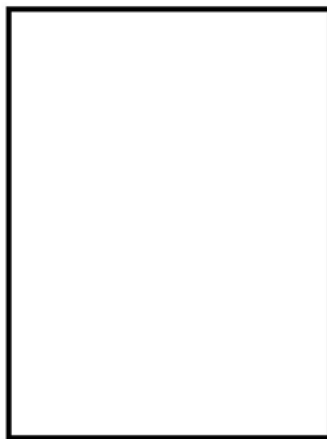
(b) (6)



Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



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

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

[Redacted]

From:

[Redacted]

Sent:

Thursday, September 04, 2014 2:21 PM

To:

[Redacted]

Subject:

FW: (U) [Redacted] Picture

Attachments:

[Redacted]

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

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