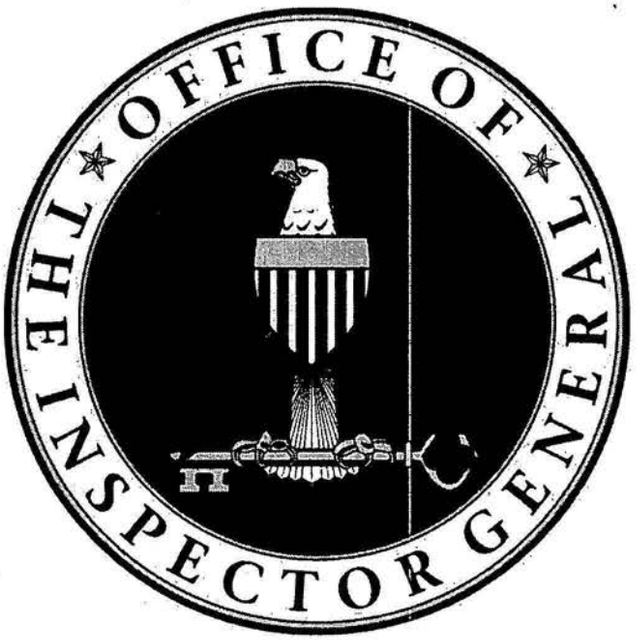
NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



INSPECTOR GENERAL

REPORT OF INVESTIGATION

12 July 2016

IV-16-0017

Misuse of Government Resources

WARNING: THIS REPORT MAY CONTAIN GRAPHIC IMAGES AND/OR LANGUAGE

(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.

(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.

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

I. (U) SUMMARY

(U//~~FOUO~~) On 24 March 2016, the NSA/CSS Office of the Inspector General (OIG) received a referral from the Associate Directorate for Security & Counterintelligence (ADS&CI) detailing U.S. Navy [redacted] alleged misuse of the NSA/CSS Unclassified network on multiple occasions from 22 January – 17 March 2016. The information regarding [redacted] alleged misuse was derived from routine monitoring of NSA/CSS Information Systems (IS). The network activity report revealed that [redacted] used his personal email account [redacted] on the NSA/CSS unclassified network to send sexually explicit emails to individuals who answered his Craigslist[1] advertisements for sexual partners.

(b)(6)

(U//~~FOUO~~) The OIG obtained sworn testimony from [redacted] on 15 April 2016. He admitted that some of the emails he sent contained sexually explicit language. The OIG reviewed a sample (Appendix B) of the sexually explicit communications with him. [redacted] acknowledged that the sample contained accurate statements he exchanged with individuals through Craigslist. [redacted] informed the OIG that he had used the NSA/CSS unclassified network to access his personal email account to send sexually explicit emails from about the middle of December 2015 until about the week prior to his interview with the OIG.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that from approximately the middle of December 2015 to approximately 8 April 2016, the week prior to his interview with the OIG, [redacted] used the NSA/CSS unclassified network to send sexually explicit email communications using his personal email account. [redacted] use of the NSA/CSS information systems to engage in such activity violated the DoD JER 5500.07-R; Subpart 2-301, and NSA/CSS Policy 6-6.

(U//~~FOUO~~) A copy of this report will be provided to the [redacted] for information and appropriate action. A summary of the findings will be provided to the [redacted] for appropriate action.

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

[1] (U) Craigslist is a webpage that hosts advertisements with sections devoted to jobs, housing, personals, for sale, items wanted, service, community, gigs, resumes and discussion forums.

II. (U) BACKGROUND

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

(U) Introduction

(b) (6)

(U//~~FOUO~~) [redacted] in the U.S. Navy. He is currently assigned to the [redacted] located at Fort Meade Maryland. Currently, [redacted] is the Division Senior Enlisted Leader in the [redacted] where he has been assigned since approximately November 2015.

(U//~~FOUO~~) During routine monitoring of NSA/CSS ISs, the user account associated with the NSA/CSS Standard Identification (SID) assigned to [redacted] was detected conducting activity on an unclassified NSA/CSS network in possible violation of NSA/CSS policy. Further analysis of [redacted] activity revealed that on multiple occasions from 22 January 2016 – 17 March 2016, [redacted] accessed his personal email account via an unclassified NSA/CSS network to exchange sexually explicit emails with individuals who answered his Craigslist advertisements seeking sexual partners.

(U//~~FOUO~~) ADS&CI referred the activity report to the OIG on 24 March 2016.

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

(U) Applicable Authorities

(U//~~FOUO~~) The investigation looked at possible violations of the following authorities:

- (U//~~FOUO~~) NSA/CSS Policy 6-6, Use of Unclassified Information Systems (IS) and Internet Based Capabilities dated 1 August 2014, revised 27 May 2015 and 2 March 2016.
- (U//~~FOUO~~) Department of Defense Joint Ethics Regulation (JER) 5500.07-R; Subpart 2-301: Use of Federal Government Resources

(U//~~FOUO~~) Full citations are contained in Appendix A.

III. (U) FINDINGS

(U//~~FOUO~~) ***ALLEGATION:*** *Did [redacted] misuse the unclassified NSA/CSS IS in violation of the DoD JER 5500.07-R; Subpart 2-301, and NSA/CSS Policy 6-6?*

(U//~~FOUO~~) ***CONCLUSION: Substantiated.*** The preponderance of the evidence supports the conclusion that from approximately the middle of December 2015 until approximately 8 April 2016, [redacted] used the NSA/CSS unclassified network to send sexually explicit email communications using his personal email account in violation of DoD JER 5500.07; Subpart 2-301, and NSA/CSS Policy 6-6.

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

(U) Documentary Evidence

(U//~~FOUO~~) Network Activity Report Communication

(U//~~FOUO~~) On 24 March 2016, a network activity report was referred to the OIG indicating that during routine monitoring of the unclassified NSA/CSS network, the user account bearing [redacted] SID, [redacted] was detected sending emails containing sexually explicit language. The report contained 95 email responses sent from [redacted] unclassified network from 22 January 2016 – 17 March 2016. The emails were sent from [redacted] personal email account that was accessed via the NSA/CSS unclassified information system. [redacted] exchanged emails with several unknown individuals who were answering his Craigslist advertisements seeking partners to engage in sexual activity. A sample of the activity is contained in Appendix B.

(U//~~FOUO~~) Email Correspondence from [redacted]

(U//~~FOUO~~) On 18 April 2016, following his interview with the OIG, [redacted] sent an email to the OIG. [redacted] had reviewed the policies concerning computer misuse and did not believe that he violated them. [redacted] stated that his emails "were explicit but it was between adults not a web site nor was there any pornography." He also indicated that there were no pictures or videos. Although he admitted that he should not have sent the messages on his email account at work and called his actions "immoral", he wrote that he did not violate policy. A full version of the email and the OIG's response can be seen in **Appendix C**.

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

(U) Testimonial Evidence

(U//~~FOUO~~)

(U//~~FOUO~~) On 15 April 2016, Division Senior Enlisted Leader, was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) conducts about 50% of his job functions as well as service related training and email on the unclassified NSA/CSS Information Systems (IS). He has received NSA/CSS related training on NSA IS systems, however he does not recall when he last received the training; he also said he does not receive annual ethics training.[2]

(U//~~FOUO~~) is aware that use of the NSA/CSS IS system constitutes consent to monitoring. His understanding of the consent to monitoring is that, "no matter what I do it's being watched." He is not familiar with Joint Ethics Regulation (JER) 5500.07-R or NSA/CSS Policy 6-6, Use of Unclassified Information Systems. However, after the OIG briefed him on the two policy documents, he opined that he did not violate the JER or NSA/CSS Policy 6-6 through his use of the NSA unclassified system.

(U//~~FOUO~~) uses the NSA/CSS unclassified IS to check personal email as a part of non-work related activity. He also uses the NSA/CSS Unclassified computer to complete training, search for flights, and hotel and rental cars for training at different NSA sites. He has not looked at websites such as Craigslist while at work. When checking his personal email account via the NSA/CSS unclassified network, he responds to posts or emails through his personal email account. He estimated that he responds once to twice per day to emails through his personal account. Some of the emails he receives and replies to pertain to advertisements he has posted on Craigslist.

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

(U//~~FOUO~~) While utilizing the NSA/CSS unclassified network, does not write anything he believes is inappropriate. The OIG informed that the OIG obtained copies of email exchanges he sent containing sexually explicit content. His understanding of sexually explicit content is, "going into detail of things that are going on within relationships." He told the OIG that "once or twice" he may have written emails that contained sexually explicit language. At first, said he had been writing sexually explicit emails to non-Agency affiliated individuals on the NSA/CSS unclassified network for approximately two weeks.

(U//~~FOUO~~) viewed a sample of the sexually explicit emails that were sent from his NSA/CSS unclassified network. After reading the material, he admitted that the sexually explicit email messages were his. When asked whether he thought that any of the information he had just read was inappropriate, he responded, "Some of them, yes… some of them are inappropriate and it should not go on systems, yes." He has not paid anyone for sexual services and denied

[2] (U//~~FOUO~~) The indicated that although not listed on training record, took an Ethics course called, "Chart the Course" on 1 April 2016. No further information was available.

(b)(6)

accessing any other online services outside of Craigslist. [redacted] denies meeting anyone to engage in sexual activity and described the emails as "just talk." He acknowledged he understood using NSA/CSS computers to have sexually explicit conversations was inappropriate.

(U//~~FOUO~~) After being confronted with samples of his emails, [redacted] revised his estimate of how long it had been going on. He estimated that he had been engaging in the exchange of sexually explicit emails on NSA/CSS unclassified network since approximately the middle of December 2015 until approximately 8 April 2016, the week prior to his interview. During the interview he stated, "This is definitely not anything I need to do anymore." He does not write sexually explicit language in emails to any Agency affiliates nor does he engage in this conduct on the NSA/CSS classified network. He has not accessed videos or pornography on the NSA/CSS unclassified network nor has he engaged in any sexual conduct while on NSA/CSS property.

(U//~~FOUO~~) [redacted] said, "Should I have been doing this at work, no and I'm definitely sorry that I actually did it on the computers here, not because I got caught but because it's misuse."

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

(U) Analysis and Conclusions

(U//~~FOUO~~) The DoD JER 5500.07-R, Subpart 2-301(a) limits the use of Federal Government communication systems and equipment to "official use and authorized purposes only." The DoD JER 5500.07-R, Subpart 2-301(a)(1) and 2-301(a)(2), respectively define "official use" and "authorized purposes" as: emergency communications and communications that the DoD component determines are necessary in the interest of the Federal Government;" and, "brief communications made by DoD employees… include[ing] personal communications from the DoD employee's usual work place that are most reasonably made while at the work place…when… such communications serve a legitimate public interest (JER 5500.7-R, Subpart 2-301(a)(2)(c)), and do not put Federal government communication systems to uses would reflect adversely on DoD or the DoD component (JER 5500.07-R, Subpart 2-301(a)(2)(d)).

(U//~~FOUO~~) NSA/CSS Policy 6-6, states that IS accounts shall be used to conduct "official NSA/CSS business." Personal use is limited and must be consistent with DoD JER 5500.07-R. NSA/CSS Policy 6-6, paragraph 16(h) defines prohibited activities as those that "violate[ing] laws or regulations or participation in other uses of any NSA/CSS IS that are incompatible with public service…"

(U//~~FOUO~~) The OIG received documented evidence of [redacted] non-mission related email exchanges from 22 January 2016 through 17 March 2016 that included the use of sexually explicit language seeking individuals to engage in sexual activity. Through [redacted] testimony, the OIG was able to determine that the sexually explicit communications took place from approximately the middle of December 2015 until approximately 8 April 2016, the week prior to his interview with the OIG. The evidence, as well as [redacted] admission to engaging in such activity on the NSA/CSS unclassified network substantiates a violation of the JER and

NSA/CSS Policy 6-6. Such activity does not constitute "official use" of Federal Government communications under the JER; sexually explicit emails seeking partners to engage in sexual activity cannot be considered emergency communications and/or communications that have been determined to be necessary in the interest of the Federal Government. Further, utilizing a Federal Government communications systems to engage in sexually explicit email communications cannot be reasonably considered as an "authorized purpose" as defined by the JER. Although the JER allows for personal communications from the employee's usual workplace to be made most reasonably while at work, sexually explicit emails seeking individuals to engage in sexual activity cannot be considered reasonable. Additionally, sending sexually explicit emails on the NSA/CSS unclassified network served no legitimate public interest and reflected adversely on the NSA/CSS and the DoD. Finally, [redacted] admitted to the OIG that he should not have engaged in such communication while at work and considered his email communications as "misuse."

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that from approximately the middle of December 2015 until the week of 8 April 2016, [redacted] used the NSA/CSS unclassified network to send sexually explicit email communications using his personal email account. [redacted] use of NSA/CSS information systems to engage in such activity violated DoD JER 5500.07-R; Subpart 2-301, and NSA/CSS Policy 6-6.

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

IV. (U) RESPONSE TO TENTATIVE CONCLUSION(S)

(U//~~FOUO~~) On 20 June 2016, the OIG sent [redacted] the tentative conclusion reached in the investigation. In his 21 June 2016 response, [redacted] wrote that he conducted research of his own by reading DoD 5240.1-R and E.O. 12333. He also read the references provided to him in the tentative conclusion which included DoD JER 5500.7-R; Subpart 2-301, and NSA/CSS Policy 6-6. [redacted] believes that his personal email communication had nothing to do with DoD nor did he say anything about working with DoD therefore his emails cannot possibly be negative towards the DoD. He acknowledged consenting to monitoring by logging onto the DoD system but did not believe his personal email account had any affiliation with DoD. Therefore, the OIG violated his privacy by reading his emails. Furthermore, DoD JER 5500.07-R(d) did not state he could not email someone from his personal email account while on break or lunch. He further opined that while his emails were explicit, they did not constitute pornography and if he should not be able to send emails from work then all internet emails should be blocked.

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

(U//~~FOUO~~) [redacted] response to the tentative conclusion did not modify the conclusion reached by the OIG. Regarding his concerns about the private and personal nature of his emails, as required by DoD Instruction 8500.01, Cyber Security (as implemented by various NSA/CSS policies including, but not limited to Policy 6-6 and NSA/CSS Policy 6-26), all NSA/CSS Information systems display the standard mandatory notice and consent banner at logon. Every time [redacted] logged on to an NSA/CSS information system, this statement was displayed:

> *Notice and Consent to Monitor*
> *You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only.*
> *By using this IS (which includes any device attached to this IS), you consent to the following conditions:*
> *--- The USG routinely intercepts and monitors communication on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.*
> *--- At any time, the USG may inspect and seize data stored on this IS.*
> *--- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose (emphasis added).*

(U//~~FOUO~~) Therefore, by using the NSA/CSS information system, [redacted] consented to the type of monitoring and the use of the results of that monitoring that are the subject of this investigation.

(U//~~FOUO~~) [redacted] response to the tentative conclusions can be found in **Appendix D**.

V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that from approximately the middle of December 2015 until approximately 8 April 2016, [redacted] used the NSA/CSS unclassified network to send sexually explicit email communications using his personal email account in violation of DoD JER 5500.07-R; Subpart 2-301, and NSA/CSS Policy 6-6.

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

V. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy or summary of this report of investigation will be provided to:

1. [redacted]
2. [redacted] (b) (6)
3. [redacted] Current Supervisor

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

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

Investigator

Concurred by: [redacted]

Inspector General
For Investigations

APPENDIX A

(U) Applicable Authorities

(U) NSA/CSS Policy 6-6: *Use of Unclassified Information Systems and Internet-based Capabilities dated 1 August 2014, revised 27 May 2015 and 2 March 2016*

1. (U) NSA/CSS shall provide unclassified, associated access IS accounts to authorized users to conduct official NSA/CSS business. Associated access via IbC for official purposes is further described, in terms of procedural permissions and constraints in paragraphs 15 and 18.

(U) **Approved Activities**

15. (U) Via an associated access account, users may:

    j. (U) Access, with supervisory approval, their personal IbC accounts and conduct limited personal use that is consistent with Reference b1[3] and is not a prohibited activity.

(U) **Prohibited Activities**

18. (U) Users shall avoid all prohibited activity and must not take any action (e.g., opening an IbC application) that potentially circumvents security protections and/or presents a security risk to the NSA/CSS information technology infrastructure. When using an associated access account, the following actions are prohibited:

    c. (U) Soliciting or advertising for products or services that are not work-related…

    h. (U) Violating laws or regulations or participating in other uses of any NSA/CSS IS that are incompatible with public service ("go ethics" for additional guidance).[4]

(U) DoD Joint Ethics Regulation (JER) 5500.07-R; Subpart 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.

[3] Reference b1 refers to the DoD 5500.07-R, "Joint Ethics Regulation," Paragraph 2-301, dated 1 August 1993, incorporating change 7, dated 17 November 2011.
[4] "Go Ethics" is a hyperlink to the NSA Office of General Counsel (OGC) Administrative Law and Ethics webpage. On the OGC Administrative Law and Ethics webpage are links to NSA/CSS Ethics Regulations which directs the user to the DoD 5500.07-R, "Joint Ethics Regulation."

(2.) Authorized purposes include brief communications made by DoD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief internet searches; e-mailing directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:

(c) Serve a legitimate public interest (such as keeping DoD employees at their desks rather than requiring the use of commercial systems; educating the DoD employee on the use of communications systems; improving the morale of DoD employees stationed for extended periods of time away from home; enhancing the professional skills of the DoD employee; job-searching in response to Federal Government downsizing);

(d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are not incompatible with public service).

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

APPENDIX B

(U) Sampling of Emails Sent by [redacted] Containing Sexually Explicit Emails Seeking Sexual Activity with Craigslist Recipients

22 January 2016 – 17 March 2016

(b) (6)

Edits were made by the OIG for readability purposes.

01/26/2016 11:21am – 1:07pm

[redacted]

02/01/2016 07:57am – 11:38am

[redacted]

02/02/2016 01:17pm

[redacted]

02/03/2016 07:58am – 12:39pm

[redacted]

02/12/2016 09:40am – 11:03am

02/16/2016 09:40 – 09:41am

(b) (6)

03/02/2016 12:46 – 12:55pm

3/10/2016 08:07:32am – 11:09am

[redacted]

(b) (6)

3/17/2016 07:22am – 07:23am

[redacted]

Craigslist Ads include subject lines:

[redacted]

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

Appendix C

[redacted] 18 April 2016 Email to the OIG &
The OIG's 25 April 2016 response to [redacted] Email

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

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: (U) Request for Interview
Date: Monday, April 25, 2016 1:58:52 PM
Attachments: image001.png
image002.png

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

INSPECTOR GENERAL SENSITIVE INFORMATION: This email, including any attachments, is intended only for authorized recipients. This email message may contain information that is confidential, sensitive, and/or protected by Federal Law, including the Privacy Act of 1974, as amended.

Good Afternoon [redacted]

I am just getting back into the swing of things upon returning from TDY. I appreciate your clarification. To answer your questions:

1. No, you have not broken any state or federal laws with regards to the misuse of the NSA information systems. The allegations against you involves the violation of policies and regulations as it pertains to the use of the NSA information systems.

2. No classified material was discussed during our meeting.

I will take your email below into consideration as part of my tentative conclusions. As mentioned during our meeting, you will be provided the opportunity to respond to my tentative conclusions and any response you have will be taken into consideration of my final report.

I will notify you of my tentative conclusion as soon as I have completed it. I appreciate your cooperation and patience.

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

V/r,

[redacted]
Investigator
NSA Office of the Inspector General
[redacted]

PRIVACY SENSITIVE – any misuse or unauthorized disclosure may lead to disciplinary action.

From: [redacted]
Sent: Monday, April 18, 2016 6:53 AM
To: [redacted]

Cc: [redacted]
Subject: RE: (U) Request for Interview

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

Good Morning [redacted]

I reviewed the policies that I was told to review. I also have a few questions. Did I break any laws? Was any classified material discussed? Also as I reviewed the policies as any DoD policy I do understand that we are to not look at pornography. However I did not violate this policy. My emails that were on a personal email were explicit but it was between adults not a web site nor was there any pornography. There were no pictures nor was there videos nor did I go to any of those sites. Also I was not using my NSA.GOV email. What I did was immoral yes should I have sent them on my gmail at work no. However as per policy I have not violated them. The wife and I have gone through a bad patch and over the last week or so we have talked and are working things out. So I deleted that gmail account and I am moving forward with my wife. Please advise.

Very respectfully,

[redacted]

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

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

From: [redacted]
Sent: Thursday, April 07, 2016 9:03 AM
To: [redacted]
Cc: [redacted]
Subject: (U) Request for Interview
Importance: High

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

INSPECTOR GENERAL SENSITIVE INFORMATION: This email, including any attachments, is intended only for authorized recipients. This email message may contain information that is confidential, sensitive, and/or protected by Federal Law, including the Privacy Act of 1974, as amended

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

I am an Investigator with the NSA/CSS Office of the Inspector General. I am investigating concerns about your use of NSA/CSS Information Systems and would like to discuss these matters with you at your earliest convenience. I would like to schedule an interview to be conducted in my office located at [redacted] Could you please provide me with a few dates within the next week (day and time) that you would be able to do so?

V/r,

[redacted]
Investigator
NSA Office of the Inspector General
(b)(3)-P.L. 86-36
[redacted]

PRIVACY SENSITIVE: This memorandum contains information protected by the Privacy Act of 1974, as amended, and should not be shared or distributed without the approval of the NSA/CSS OIG. The information being shared is relevant to the official responsibilities of your office and disclosed for a routine use as described in the NSA/CSS System of Records Notice GNSA 29.

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)(6)

Appendix D
[redacted] Reply to the Tentative Conclusions

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

From: [redacted]
To: [redacted]
Subject: (U) RE: OIG Tentative Conclusions
Date: Tuesday, June 21, 2016 11:32:43 AM
Attachments: image001.png
image003.png

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

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

[redacted]

Originator stated that the contents of his response are entirely U//FOUO and the document was misclassified as CONFIDENTIAL.

I have read your findings as well as I have done research myself into the matter. I have also read the DoD 5240.1-R and E.O. 12333. I have read all the references that you have provided as well. The first clip is from the Ethics and as I was on personal email having a personal conversation that had nothing to do with DoD or said anything about working with DoD it cant possible be negative towards the DoD. Second I consent to monitoring by logging on to DoD systems but nowhere does it say that you can copy and print unclassified personal emails that were written on a personal email account that has no affiliations with the DoD. Also to that affect as I have read 5500.7-R myself at no point did I violate any laws or am I involved with any foreign power. The section that you referred to in 5500.7-R (d) which is pasted below as I read it does not state that I cannot email someone on my break time or lunch on my personal email. It was explicit but it was not pornography (which is clearly stated in 5500.7-R p(d) and at no point does it state that it was left up to the persons interpretation. Yes it does state that we can email short emails to wife, kids, family and any service for home repairs things like that. If it is not something that should be done at work then all internet emails should be blocked. As my emails were short and to a person it was not wasting government time. Like YOUTUBE or Pandora or sports pages which is not waste fraud and abuse. Policies are vague and not pointing to this specific case. However in everything that has happened in this investigation you have violated my privacy and now you have documented all of it. Which is in violation of DoD 5240.1-R and E.O. 12333. Had I known that all of my private emails would be searched are read I would not have opened them at work. As some of those emails weren't even written on a government computer they were written on my phone and I read them here. I would understand if my NSA.GOV email was in question but it is not as that is an official email that points to the fact that I work for NSA and DoD. Please advise on who and whom has seen what you have printed out and where you will be forwarding that information to? As I need to let my Chain of Command know what is coming.

(d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service);

C2.2.3. Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization, or person.

C6.2.3. Whether concealed monitoring is to occur where the subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office responsible for advising the DoD intelligence component concerned. Reasonable expectation of privacy is the extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to monitoring by electronic, optical, or mechanical devices. For example, there are ordinarily reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal working conditions. Conversely, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed; however, such a person ordinarily would have an expectation of privacy within his or her residence.

C14.2.1. Employee Responsibilities. Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by law; Executive order, including E.O. 12333 (reference (a)), and applicable DoD Directives.

Very respectfully,

[redacted]

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

From: [redacted]
Sent: Monday, June 20, 2016 12:10 PM
To: [redacted]
Subject: OIG Tentative Conclusions
Importance: High

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

INSPECTOR GENERAL SENSITIVE INFORMATION: This email, including any attachments, is intended only for authorized recipients. This email message may contain information that is confidential, sensitive, and/or protected by Federal Law, including the Privacy Act of 1974, as amended.

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

(U//~~FOUO~~) We have completed the field work associated with our investigation into allegations that you misused the NSA/CSS unclassified network to send sexually explicit emails to individuals who answered your Craigslist advertisements for sexual partners.

(U//~~FOUO~~) Prior to finalizing the Report of Investigation, we are notifying you of our tentative conclusions and extending an opportunity for you to provide a response. We include this step in our investigative process to ensure that subjects are afforded the opportunity to review our findings and reply with any mitigation, facts, information, or evidence that might not have been considered in reaching our conclusion.

(U//~~FOUO~~) The DoD JER 5500.07-R, Subpart 2-301(a) limits the use of Federal Government communication systems and equipment to "official use and authorized purposes only." The DoD JER 5500.07-R, Subpart 2-301(a)(1) and 2-301(a)(2), respectively define "official use" and "authorized purposes" as: emergency communications and communications that the DoD component determines are necessary in the interest of the Federal Government;" and, "brief communications made by DoD employees… include[ing] personal communications from the DoD employee's usual work place that are most reasonably made while at the work place… when… such communications serve a legitimate public interest (JER 5500.7-R, Subpart 2-301(a)(2)(c)), and do not put Federal government communication systems to uses that would reflect adversely on DoD or the DoD component (JER 5500.07-R, Subpart 2-301(a)(2)(d)).

(U//~~FOUO~~) NSA/CSS Policy 6-6, states that IS accounts shall be used to conduct "official NSA/CSS business." Personal use is limited and must be consistent with DoD JER 5500.07-R. NSA/CSS Policy 6-6, paragraph 16(h) defines prohibited activities as those that "violate[ing] laws or regulations or participation in other uses of any NSA/CSS IS that are incompatible with public service…"

(U//~~FOUO~~) The OIG received documented evidence of your non-mission related email exchanges from 22 January 2016 through 17 March 2016 that included the use of sexually explicit language. You testified that your sexually explicit communications took place from approximately the middle of December 2015 until approximately 8 April 2016, the week prior to your interview with the OIG. The physical evidence, as well as your admission to engaging in such activity on the NSA/CSS unclassified network substantiates a violation of the JER and NSA/CSS Policy 6-6. Such activity does not constitute "official use" of Federal Government communications under the JER; sexually explicit emails seeking partners to engage in sexual activity cannot be considered emergency communications and/or communications that have been determined to be necessary in the interest of the Federal Government. Further, utilizing a Federal Government communications system to engage in sexually explicit email communications cannot be reasonably considered as an "authorized purpose" as defined by the JER. Although the JER allows for personal communications from the employee's usual workplace to be made most reasonably while at work, sexually explicit emails seeking individuals to engage in sexual activity cannot be considered reasonable. Additionally, sending sexually explicit emails on the NSA/CSS unclassified network served no legitimate public interest and reflected adversely on the NSA/CSS and the DoD.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that from approximately the middle of December 2015 until the week of 8 April 2016, you used the

NSA/CSS unclassified network to send sexually explicit email communications using your personal email account. Your use of NSA/CSS information systems to engage in such activity violated DoD JER 5500.07-R; Subpart 2-301, and NSA/CSS Policy 6-6.

(U//~~FOUO~~) Please take the following actions:

1. (U//~~FOUO~~) Immediately confirm receipt of this email.
2. (U//~~FOUO~~) Although you are not required to provide any input, if you choose to do so, please provide your input by **Monday 06/27/2016**. Your reply can be in the form of an email, memo, or any format you choose. Please provide as much detail as possible, including dates, facts, names, and supporting documentation.
3. (U//~~FOUO~~) If you choose not to provide any input, please let us know that as soon as practicable, but no later than **Monday 27 June 2016.**

(U//~~FOUO~~) Feel free to contact me if you have any questions.

V/r,

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

[redacted]
Investigator
NSA Office of the Inspector General

[redacted]

PRIVACY SENSITIVE – any misuse or unauthorized disclosure may lead to disciplinary action.

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20410601

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