NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

27 September 2016

IV-16-0032

Alleged Misuse of Government Resources

(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.

I. (U) SUMMARY

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

(U//~~FOUO~~) On 14 July 2016, the NSA/CSS Office of Inspector General (OIG) received a referral from the Associate Directorate for Security and Counterintelligence (ADS&CI) detailing alleged misuse of the NSA/CSS Unclassified network by NSA/CSS Civilian employee, [redacted] The information regarding [redacted] alleged misuse was derived from routine monitoring of NSA/CSS Information Systems (IS).

(U//~~FOUO~~) The referral provided to the OIG indicated that [redacted] used the NSA/CSS Unclassified network for the purpose of running his personal businesses. The referral showed that between 07 June 2016 and 06 July 2016, [redacted] composed, sent, received, and responded to more than 100 business-related emails, as well as spent time researching matters associated with the running of his personal business.

(U//~~FOUO~~) The OIG obtained sworn testimony from [redacted] on 23 August 2016. [redacted] acknowledged that he owned two personal businesses, [redacted] and [redacted][2]. He testified to using the NSA/CSS Unclassified network to browse his business websites, to send emails from his personal email address to the business, and research items pertaining to his business. He testified that he drafted emails and sent them to his business partner to send out to clients and employees of the two businesses. During the interview, [redacted] admitted that he should not have conducted such activity on the NSA/CSS Unclassified network and stated, "in all honesty, I've been kind of doing it on and off for years and no one has questioned it… By the letter of the law, I was wrong." Additionally, [redacted] testified that he had used the NSA/CSS Unclassified network as recently as 22 August 2016 to send an email regarding his personal businesses.

(U//~~FOUO~~) A preponderance of the evidence shows that from 07 June 2016 to 22 August 2016, [redacted] used the NSA/CSS Unclassified network to engage in communications related to outside business activities in violation of DoD Joint Ethics Regulation 5500.07-R, Subpart 2-301, and NSA/CSS Policy 6-6.

(U//~~FOUO~~) A copy of the NSA/CSS OIG report will be forwarded to Employee Relations (MR) for information and any action deemed appropriate. Also, a summary of the findings will be

(b)(6)

[1] (U) [redacted] business owned by [redacted] and his business partner. It [redacted]

[2] (U) [redacted] is a company owned by [redacted] and a division of [redacted]

forwarded to the Associate Directorate for Security and Counterintelligence (ADS&CI), Special Actions (A5242) and [redacted] supervisor.

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

II. (U) BACKGROUND

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

(b) (6)

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

(U) Introduction

(U//~~FOUO~~) [redacted] is a [redacted] NSA/CSS Civilian assigned to [redacted] He has been an Agency employee since November 2002.

(U//~~FOUO~~) NSA/CSS Policy requires that all NSA/CSS Information Systems (ISs) and networks be monitored to "collect information in order to detect…internal misuse…" During routine monitoring of NSA/CSS ISs, the NSA/CSS ADS&CI detected possible misuse of the NSA/CSS Unclassified network associated with the NSA/CSS Standard Identification (SID) assigned to [redacted] ADS&CI analyzed [redacted] activity from 07 June 2016 and 06 July 2016, and forwarded their report to the OIG on 14 July 2016.

(U) Applicable Authorities

(U) See Appendix A for the full text of the applicable authorities.

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

III. (U) FINDINGS

*(U//~~FOUO~~) **ALLEGATION: Did** [redacted] **NSA/CSS Civilian, use the NSA/CSS Unclassified network from 07 June 2016 to 22 August 2016, to engage in communications related to outside business activities in violation of DoD JER 5500.07-R and NSA/CSS Policy 6-6?***

*(U//~~FOUO~~) **CONCLUSION:** Substantiated.*

(U) Documentary Evidence

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

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

(U//~~FOUO~~) ADS&CI provided a network activity report to the OIG containing an analysis of [redacted] personal email activity via the NSA/CSS Unclassified network from 07 June 2016 to 06 July 2016. The report estimated that between 07 June 2016 and 06 July 2016, [redacted] spent approximately 5.4 hours composing, sending, and responding to more than 100 emails, as well as researching items associated with the running of his personal businesses. Excerpts of these emails and searches can be found in Appendix B.

(U) Testimonial Evidence

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

(U//~~FOUO~~) On 23 August 2016, [redacted] was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] does not have an NSA/CSS Unclassified network computer located on his desk. There are four shared NSA/CSS Unclassified computers throughout his office. [redacted] is authorized to use the NSA/CSS Unclassified network for work-related purposes, which includes [redacted] He also uses the NSA/CSS Unclassified network to conduct non-work related activity such as accessing his personal email, his personal google calendar, CNN, slickdeals.com, and Amazon.com. [redacted] also visits websites like MSNBC, and he recently researched the Rio Olympics and various HVAC companies. [redacted] testified that he tries to limit his time spent on the NSA/CSS Unclassified network to approximately 20 minutes to research work-related items and approximately five minutes on non-work-related items because he is cognizant that others may need to use the system.

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

(U//~~FOUO~~) is aware that he provides consent to monitoring every time he logs onto the NSA/CSS Information systems. He believes that consent to monitor means that "they're going to monitor and tell me if I did something bad and obviously I try not to do anything bad; I would expect nothing less, we are the government." is also familiar with the NSA/CSS Policies governing the use the NSA/CSS Classified and Unclassified networks. He believes that the rule is that the NSA/CSS Unclassified network is to be used for work-related purposes only. testified that viewing his personal email and calendar was a violation of NSA/CSS Policy.[3]

(b) (6)

(U//~~FOUO~~) has two businesses, and . He testified to browsing his personal business websites from the NSA/CSS Unclassified network. He sends emails from his personal email addresses via the NSA/CSS Unclassified network to his business partner to inform him that he cannot meet certain obligations due to conflicting schedules between his job at NSA and the business. He also corresponds with other employees of his businesses as well, composing emails he wants them to send to clients. also admitted to researching matters pertaining to his business but denied purchasing items via the NSA/CSS Unclassified network. Additionally, testified to accessing the NSA/CSS unclassified network to send an email pertaining to his business as recently as 22 August 2016.

(U//~~FOUO~~) believed that because he had supervisory authorization to use the NSA/CSS unclassified network and had never been told he was doing anything wrong, that he was okay. admitted that he should not have been sending the emails but that he continued to send them because "in all honesty, I've been kind of doing it on and off for a few years and no one has questioned it. By the letter of the law, I was wrong."

(U//~~FOUO~~) The OIG explained the NSA/CSS Policy 6-6 to specifically covering the prohibited activities. agreed that his use of the NSA/CSS Unclassified network to conduct business activities is considered a violation. He stated "obviously I knew it was monitored and I did it and unfortunately, to be very honest, it's [policy] not something I reread every month… Obviously, yes, I am admitting that I did send emails against policy."

(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 defines "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

[3] (U) In contrast to impression, NSA/CSS Policy 6-6 paragraph 15(j) allows users, with supervisory approval, to access their personal IbC accounts for limited personal use.

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 5500.07-R, Subpart 2-301(a)(2)(a) do not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization) and (JER 5500.07-R, Subpart 2-301 (a)(2)(b)) are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods. It further explains that authorized purposes 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 a spouse, minor children, scheduling doctor and auto or home repair appointments, and brief internet searches.

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

(U//~~FOUO~~) [redacted] actions of accessing his personal email account via the NSA/CSS Unclassified network for the express purpose of sending, composing, receiving and responding to business-related emails and conducting searches pertaining to his personal businesses does not meet the criteria as outlined in the JER. Therefore his actions violate the DoD JER 5500.07-R, Subpart 2-301.

(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 18(c) defines prohibited activities such as, soliciting or advertising for products or services that are not work-related… and (g) conducting a private business or commercial venture including, but not limited to, engaging in personal sales activities, operating a private business for profit, engaging in communications related to outside business activities.

(U//~~FOUO~~) Although NSA Policy permits limited personal use of IS accounts, it specifically prohibits conducting a private business. The ADS&CI report of [redacted] activity on the NSA/CSS Unclassified network confirmed that [redacted] accessed his personal email account via the NSA/CSS Unclassified network for the express purpose of sending, composing, receiving, and responding to business-related emails and conducting searches pertaining to his personal businesses. Furthermore, during his interview with the OIG, [redacted] admitted to accessing his personal email from the NSA/CSS Unclassified network to conduct activities related to his personal businesses.

(U//~~FOUO~~) A preponderance of the evidence shows that from 07 June 2016 to 22 August 2016, [redacted] used the NSA/CSS Unclassified network to engage in communications related to outside business activities in violation of DoD Joint Ethics Regulation 5500.07-R, Subpart 2-301 and NSA/CSS Policy 6-6.

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

(U//~~FOUO~~) On 02 September 2016, [redacted] responded to the OIG's tentative conclusions. His response included the following, "Now that I have read the policies I am accused of violating I am in agreement that I did violate them. With the previous being stated and the fact that being able to accomplish some of the items I am accused of while on the NSA/CSS Unclassified network allowed me [to] attend meetings and be a more productive employee without having the additional worry of outside things needing to be accomplished immediately when I left work. I feel that I limited my use of the unclassified system and logged out if I was no longer performing an NSA/CSS job related function. I would normally check my personal and personal business email while searches were being conducted for my job so that my time was not wasted. This is still no excuse for my violation of the policies and as such I have discontinued my unclassified network use at this time and shall only be using it for approved NSA/CSS and DoD defined purposes moving forward."

(U//~~FOUO~~) [redacted] emailed response can be found in Appendix C.

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

V. (U) CONCLUSION

(U//~~FOUO~~) A preponderance of the evidence shows that from 07 June 2016 to 22 August 2016, [redacted] used the NSA/CSS Unclassified network to engage in communications related to outside business activities in violation of DoD Joint Ethics Regulation 5500.07-R, Subpart 2-301 and NSA/CSS Policy 6-6.

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

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report of investigation will be provided to Employee Relations (MR). A summary of the investigative findings will be provided to A5242, and [redacted] supervisor.

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

[redacted]
Investigator

Concurred by:

[redacted]
Assistant Inspector General
for
Investigations

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

APPENDIX A

(U) Applicable Authorities

(U//~~FOUO~~) **Department of Defense Joint Ethics Regulation (JER) 5500.07-R; Subpart 2-301** ***Use of Federal 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.

(1) Official use includes emergency communications and communications that the DoD component determines are necessary in the interest of the Federal Government. Official use may include, when approved by theater commanders in the interest of morale and welfare, communications by military members and other DoD employees who are deployed for extended periods away from home on official DoD business.

(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; emailing directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:

(a) Do not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization.

(b) Are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods…

(U//~~FOUO~~) **NSA/CSS Policy 6-6: Use of Unclassified Information Systems and Internet-Based Capabilities dated 1 August 2014, revised 2 March 2016.**

(U) POLICY

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 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…

g. (U) Conducting a private business or commercial venture including, but not limited to, engaging in personal sales activities, operating a private business for profit, engaging in communications related to outside business activities, or participating in online gaming or gambling activity.

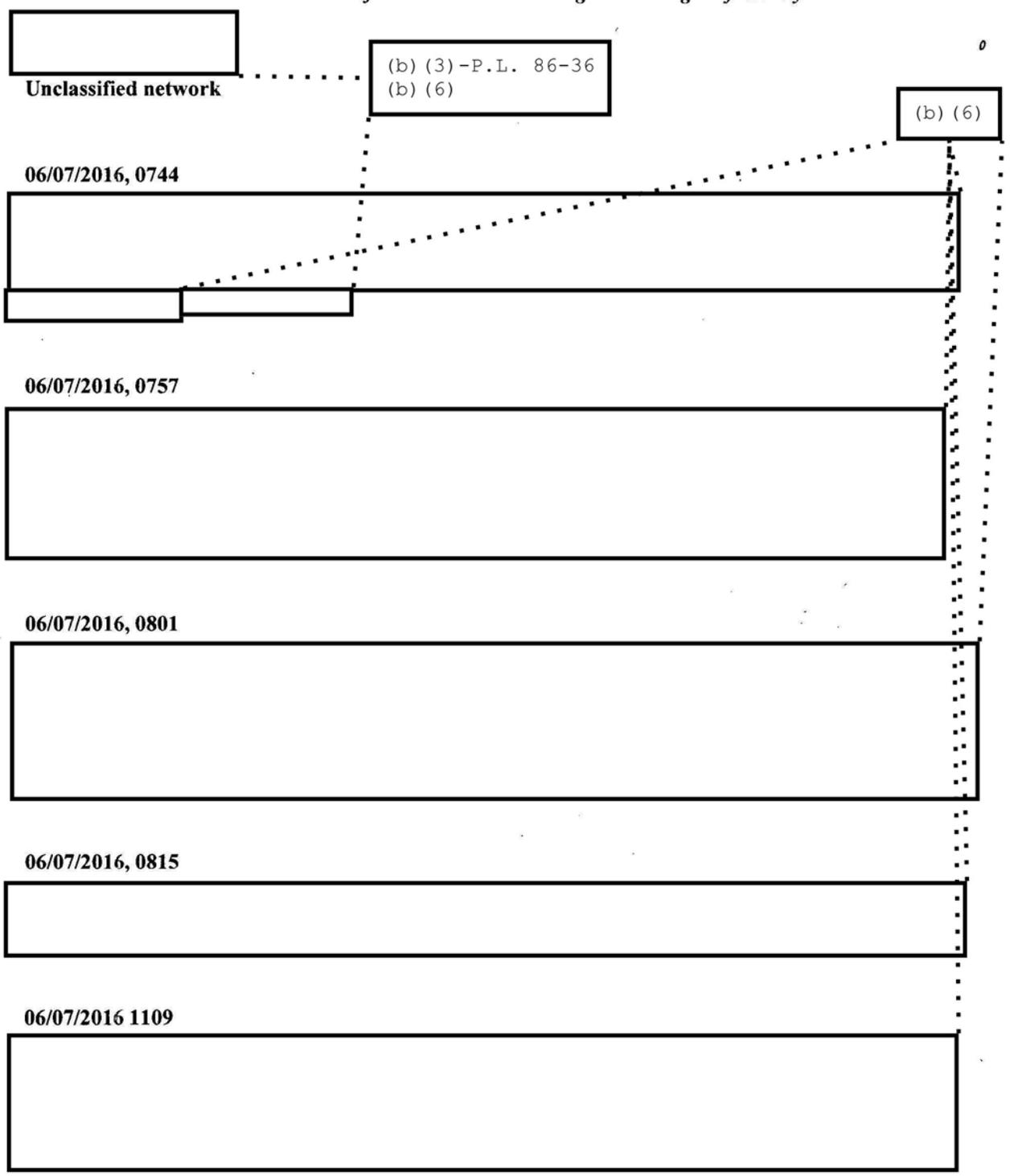
APPENDIX B

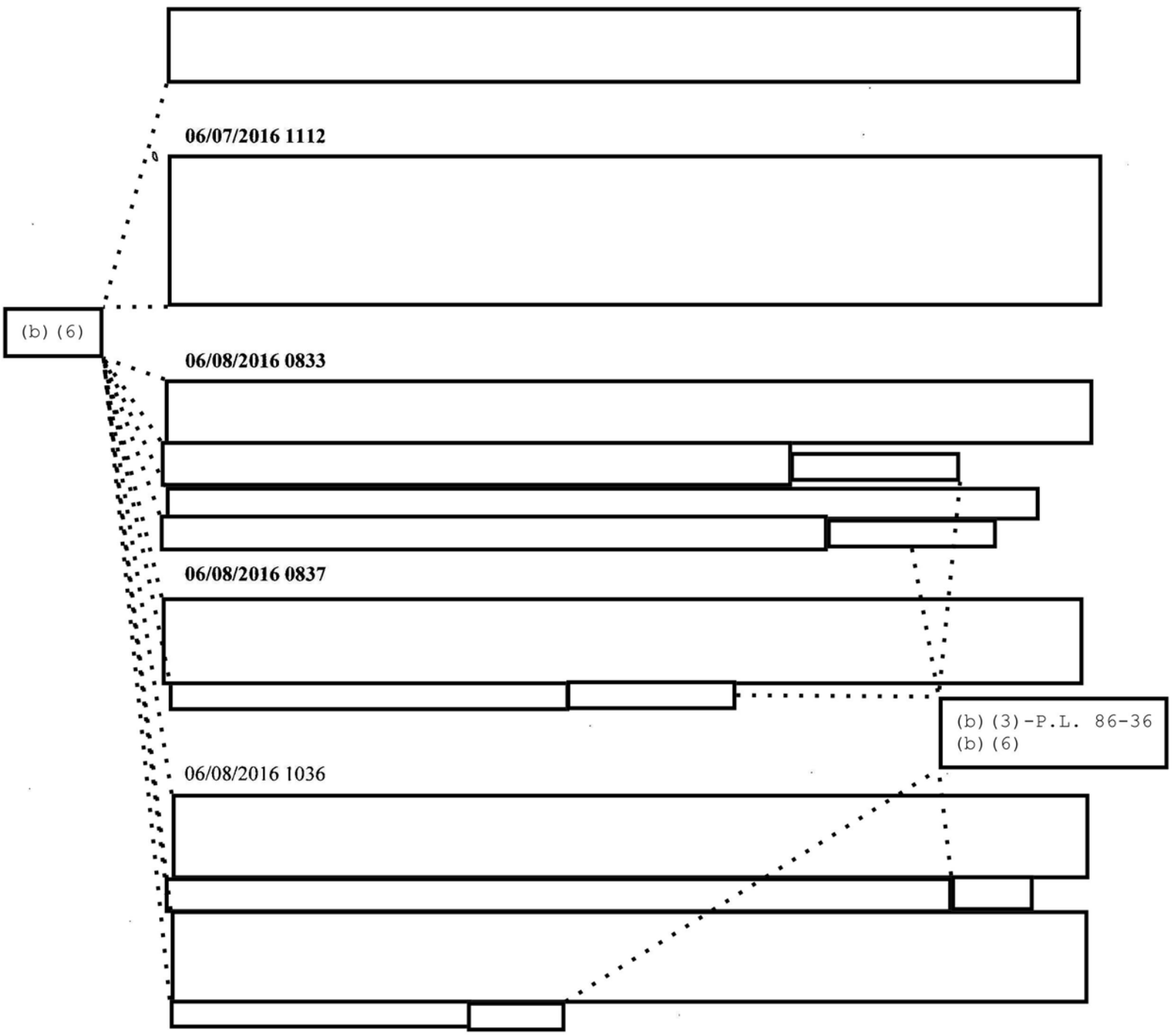
(U) Excerpts of Emails

Unclassified Network Activity SAMPLE

***OIG edited for readability purposes**

****Does not include ALL data derived from routine monitoring due to length of activity**



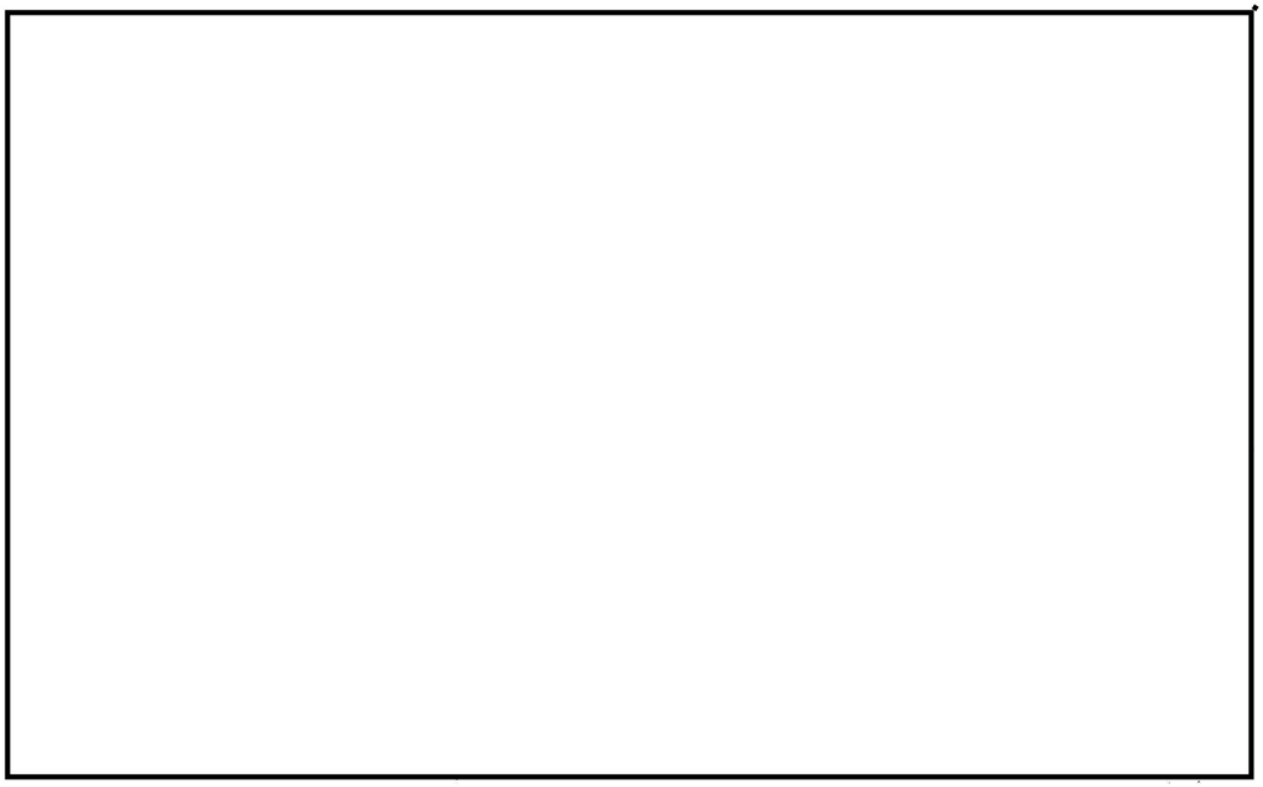


Internet searches

06/10/2016

(b) (6)

(b) (6)



APPENDIX C

(U//~~FOUO~~) [redacted] Response to the Tentative Conclusion

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

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

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: (U) OIG Notification Of Tentative Conclusion
Date: Friday, September 02, 2016 8:59:57 AM

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

(U//~~FOUO~~) I wanted to provide this initial information for the record but also confirm that I can provide additional details/questions over the next few days if something else comes up where I am able to locate additional information. (b)(3)-P.L. 86-36

(U//~~FOUO~~) In response to the statement "express purpose of sending, composing, receiving and respond to business-related emails and conducting searches...." I did login to the NSA/CSS Unclassified network for things related to my job at NSA. During my time on the NSA/CSS Unclassified network I spent time researching issues [redacted] requested by users and my management, [redacted] During the specific time that the evidence covered I was in the process of planning a TDY and was getting information related to my upcoming trip. On my trip I had [redacted] and the search that I was presented with during our interview/discussion was for personal and was not related specifically [redacted] business. (b)(6)

(U//~~FOUO~~) In regards to NSA/CSS Policy 6-6 I do not feel that I was in violation of (c) soliciting or advertising for products or services. I was responding to emails from clients/customers that were already requesting information related to my personal business or communicating with my business partner [redacted] or employees. I do agree that paragraph (g) is what I was in violation of and not (c) in this case.

(U//~~FOUO~~) Now that I have read the policies I am accused of violating I am in agreement that I did violate them. With the previous being stated and the fact that being able to accomplish some of the items I am accused of

while on the NSA/CSS Unclassified network allowed me attend meetings and be a more productive employee without having
the additional worry of outside things needing to be accomplished immediately when I left work. I feel that I limited my use
of the unclassified system and logged out if I was no longer preforming an NSA/CSS job related function. I would normally check
my personal and personal business email while searches were being conducted for my job so that my time was not wasted.
This is still no excuse for my violation of the policies and as such I have discontinued my unclassified network use
at this time and shall only be using it for approved NSA/CSS and DoD defined purposes moving forward.

(U//~~FOUO~~) These are just a few of the questions that I have, but in no way change the fact that I agree that I violated the
listed policies (DoD JER 5500.07-R and NSA/CSS Policy 6-6).

(U//~~FOUO~~) Questions:
(U//~~FOUO~~) When/Where were "we" told to read each policy and DoD standard (example DoD JER 5500 and NSA 6-6)?
- I agree that I should have read these probably every year, but I do not recall being asked to acknowledge
that I read them or being told to read them. We are told to read and take so many classes why isn't this a
annual requirement or why aren't we required to acknowledge reading it prior to logging in every time?
We do read a "motd" is known as the "consent to monitor agreement" and does list personnel misconduct.
I did not believe that I was performing "misconduct" since I was actively working my job and my peers
and supervisor had full sight of what I was doing as our NSA/CSS Unclassified systems are shared in the
office and in plain sight to anyone walking in and out of the area. There are times that I notice an announcement
of a change to a policy and will browse the document however unfortunately many of these notices go
unnoticed because of the large amount of email that I do receive for my daily duties.

(U//~~FOUO~~) Where is the user agreement that I signed for my Unclassified account?
- When I contacted [redacted] about the [redacted] barcoded hardware and my unclassified account they stated they do not require
a user agreement for an unclassified account, policy 6-6 paragraph 7 states that I should have signed one.
I do not recall signing one when I first received my account however that was when I EODed in

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

2012. I believe the account
was provided to me by my management at that time. I did email "go security" as directed by [redacted] requesting
further assistance in locating a possible user agreement that I would have signed or received.

(U//~~FOUO~~) Thank you for your time and the opportunity to provide additional information and questions regarding this investigation.

(U//~~FOUO~~)

[redacted]

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

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

From: [redacted]
Sent: Thursday, September 01, 2016 12:20 PM
To [redacted]
Subject: (U) OIG Notification Of Tentative Conclusion
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]

(U//~~FOUO~~) The OIG has completed the field work associated with your our investigation into allegations that you misused the NSA/CSS Unclassified network for the purpose of engaging in communications related to outside business activities.

(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 defines "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 5500.07-R, Subpart 2-301(a)(2)(a) do not adversely affect the performance of official duties by the DoD employee or the DoD employee's organization) and (JER 5500.07-R, Subpart 2-301 (a)(2)(b)) are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods. It further explains that authorized purposes 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 a spouse, minor children, scheduling doctor and auto or home repair appointments, and brief internet searches.

(U//~~FOUO~~) [redacted] actions of accessing his personal email account via the NSA/CSS Unclassified network for the express purpose of sending, composing, receiving and responding to business-related emails and conducting searches pertaining to his personal businesses does not meet the criteria as outlined in the JER. Therefore his actions violate the DoD JER 5500.07-R, Subpart 2-301.

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

(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 18(c) defines prohibited activities such as, soliciting or advertising for products or services that are not work-related… and (g) conducting a private business or commercial venture including, but not limited to, engaging in personal sales activities, operating a private business for profit, engaging in communications related to outside business activities.

(U//~~FOUO~~) Although NSA Policy permits limited personal use of IS accounts, it specifically prohibits conducting a private business. The ADS&CI report of [redacted] activity on the NSA/CSS Unclassified network confirmed that [redacted] accessed his personal email account via the NSA/CSS Unclassified network for the express purpose of sending, composing, receiving, and responding to business-related emails and conducting searches pertaining to his personal businesses. Furthermore, during his interview with the OIG, [redacted] admitted to accessing his personal email from the NSA/CSS Unclassified network to conduct activities related to his personal businesses.

(U//~~FOUO~~) A preponderance of the evidence shows that from 07 June 2016 to 22 August 2016, [redacted] used the NSA/CSS Unclassified network to engage in communications related to outside business activities in violation of DoD Joint Ethics Regulation 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 **Wednesday 14 September 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 as soon as practical, but no later than **Wednesday 14 September 2016.**

(U//~~FOUO~~) If you have any questions, please feel free to contact me.

V/r,

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

Investigator
NSA Office of the Inspector General

[redacted]

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

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

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