

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL
9800 Savage Road, Suite 6247
Fort George G. Meade, MD 20755-6247



8 March 2016

To: Chief, D14

From: Investigator [redacted]

Subject: Computer Misuse

File No: IV-14-0057

Precedence: Routine

Purpose: To provide a summary report of investigation and to refer this matter to the Chief, Maryland Procurement Office (B3P); and the Associate Directorate for Security and Counterintelligence - Contractor Clearances (Q232) and Special Actions (Q242), for review and any action deemed appropriate.

Details:

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

I. (U) Background:

(U//~~FOUO~~) On 27 February 2014, the NSA/CSS Office of the Inspector General (OIG) received a referral containing a network activity report identifying possible misuse of the classified NSA/CSS Information System (IS) by contractor affiliate [redacted] is employed by [redacted] and is an NSA/CSS contractor affiliate working on the [redacted] contract [redacted] which provides [redacted] support to [redacted] Team. On 7 March 2014, the OIG initiated an investigation into [redacted] suspected misuse of the classified NSA/CSS IS.

II. (U) Allegation:

(U//~~FOUO~~) Did [redacted] a contractor affiliate supporting the [redacted] [redacted], misuse the classified NSA/CSS IS in violation of NSA/CSS Policy 6-4?

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

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

III. (U) Applicable Standard(s):

(U//~~FOUO~~) NSA/CSS Policy 6-4, *Contractor Use of NSA/CSS Information Systems and Resources*, dated 22 October 2013

IV. (U) Investigative Activity:

A. (U//~~FOUO~~) Analysis of Routine Monitoring of [redacted] Classified NSA/CSS IS Activity:

(U//~~FOUO~~) Initially, one network activity report was referred to the OIG which detailed [redacted] suspected misuse of the classified IS during the period 13 January 2014 – 6 February 2014 (Report A). A subsequent network activity report (Report B) was requested and obtained for the period 7 April 2015 – 6 May 2015 to determine whether the suspected misuse was ongoing.

(U//~~FOUO~~) Report A indicated that during routine monitoring of the classified NSA/CSS IS, the user account bearing [redacted] NSA/CSS Standard Identification (SID), [redacted] was detected developing a business plan for a personal business using the classified network. Upon further review, it was determined [redacted] was developing a business plan for a lifestyle media blog, called [redacted]. Specifically, [redacted] was detected drafting documents on an NSA/CSS classified workstation describing the blog's purpose, content, target audience, and business plan; as well as planning the subject matter for potential articles to be published to the blog.¹ For example, on 23 and 24 January 2014 respectively, [redacted] created documents containing a description of the

[redacted] Portions of these documents later appeared on the "About" page on the [redacted] under the heading [redacted] (See Appendix B). On 28

(b) (6)

January 2015, [redacted] drafted a document [redacted] (See Appendix C), which were each posted to his blog on 18 April 2015. Finally, [redacted] drafted another document on 28 January 2014 [redacted]

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

[redacted] (See Appendix D), which was posted to his blog on 27 June 2015.

(U//~~FOUO~~) Report B indicated that during routine monitoring of the classified NSA/CSS IS, the user account bearing [redacted] SID [redacted] was detected conducting non-work-related activity on the classified network. Specifically, [redacted] was detected spending a significant amount of time drafting what appeared to be articles for his blog [redacted]. Of note, certain articles that were drafted by [redacted] using an NSA/CSS classified workstation were later posted to his blog. For example, on 8 April 2015, [redacted] was detected drafting an

¹ The OIG obtained no evidence to suggest that [redacted] posted any content to his blog using U.S. Government resources.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

article entitled [redacted] (See Appendix E), which was later posted on his blog on 25 April 2015. On 9 April 2015, [redacted] was detected drafting an article entitled, [redacted] (See Appendix F). That article was posted to [redacted] blog on 3 July 2015. On 30 April 2015, [redacted] was detected drafting an article entitled [redacted] (See Appendix G), which was later posted to his blog on 28 August 2015. Finally, [redacted] was detected drafting an article entitled [redacted] (See Appendix H), on 6 May 2015, which was later posted on his blog on 25 July 2015. [redacted] was also detected conducting research related to his articles on the internal Wikipedia website.

B. (U) Interview(s):

(U//FOUO) On 8 December 2015, [redacted] was interviewed and provided the following sworn testimony:

(U//FOUO) [redacted] stated that he has not used the classified IS for personal use in the last two years. He typically uses the classified IS for work-related purposes. He stated that he uses the unclassified IS from time-to-time to check personal emails and that he rarely uses the unclassified IS to check the news.

(U//FOUO) [redacted] stated that he is not entirely clear on [redacted] policy regarding use of the classified or unclassified IS. He is aware, however, that [redacted] has provided guidance on the proper use of both networks. He believes that he is permitted to check personal email from time-to-time and to print driving directions as needed. [redacted] is aware that NSA/CSS ISs are monitored. His understanding of the policy is to refrain from doing anything that would jeopardize the nation's security or anything that could put the U.S. at risk. He is aware that his use of NSA/CSS ISs constitutes consent to monitoring. He is familiar with the "Consent to Monitoring" banner that pops-up when logging on to either system though he does not know specifically what it says. He is also aware of the NSA/CSS Policy regarding contractor use of NSA/CSS ISs, his understanding of which is that moderate personal use is permitted as long as he is not on the system all day (a point that he specifically recalled hearing from government officials and managers). It surprised [redacted] to know that use of the NSA/CSS ISs constitutes consent to monitoring of their personal activity, such as email.

(U//FOUO) [redacted] stated that he is the owner/operator of the blog website, [redacted]. He described the blog as a lifestyle blog covering topics such as an individual's life experiences and being able to connect to and improve the quality of people's lives. While at work he has jotted down/drafted notes, via his personal email, for the articles which appear on that website. [redacted] stated that he would usually do this once a day for about 20 minutes. He is certain of the time because he claims the workstation contains a timer that switches the connection from the unclassified network back to the classified network every 15 minutes. He stated that he has never used the classified network to draft articles for his blog. The blog "went live" on or about late April or early May of 2015. Any articles that he writes or publishes are posted to the blog every Friday or Saturday at 1 a.m., and are time stamped. He stated that he posts 20 – 24 articles per month. Any preparation for the creation of his blog would have only

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

(b) (6)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

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

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

taken place either after work or on the weekends. All of his blog articles are written a week or two in advance of being posted. [redacted] drafted several articles in advance of his blog going live.

(U//~~FOUO~~) The creation of the blog's webpage was outsourced to independent graphic designers because [redacted] does not possess such skills. He stated that he did not conduct any research related to creating a blog or designing the website on the classified network, but he did research news on the unclassified IS as it related to creating a "startup" and lifestyle topics; but nothing that concerned the government, public sector, or intelligence. He stated that he never conducted any research on the classified network related to the content of his blog or planning the startup. He has however looked up information on the classified "Wikipedia" page regarding [redacted]

(U//~~FOUO~~) [redacted] stated that the website, "washingtondcscore.org", is the website for a mentoring organization that provides guidance for starting a business, as well as the process for doing so. [redacted] stated that he visited the website on two occasions to submit information in response to a survey, and he twice met with them on his personal time in Ballston, VA and Washington, D.C. He stated that he did not conduct any research on "washingtondcscore.org" to assist with starting his blog. Any work he has done in advance of creating his blog was solely via trial and error and conducted on the weekends. [redacted] stated that his blog went live three months after he heard of "washingtondcscore.org". [redacted] reiterated that any work related to his blog was done after work or on the weekends.

(U//~~FOUO~~) [redacted] stated that he did not draft his blog articles or a trademark application on the classified network. The article, [redacted] (which, evidence confirms, was drafted on the classified network), was published on his blog on April 25, 2015 at 3 a.m. [redacted] stated that the article was not posted to his blog while he was at work. [redacted] acknowledged that he did in fact draft articles while at work possibly in late 2014. He stopped drafting and printing them around April 2015. He stated that he has not drafted any articles while at work since that time, including those that were posted in the week preceding this interview. [redacted] explained that he was not completely forthcoming regarding his use of the classified network to draft blog articles because he was unsure as to what he might have done wrong and did not understand the questioning. [redacted] stated that he uses "Google Apps" on the way to work to draft his blog articles by dictating the articles to the app, which is then transferred to a MS Word document. He reiterated that he did not post the articles to his blog while he was at work and that he has not drafted any articles from work since April 2015.

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

(b) (6)

(U//~~FOUO~~) [redacted] stated that he did not get paid while drafting the articles. However, he acknowledged that he did not account for the time spent drafting the articles at work on his timesheet, i.e. he did not deduct that time from the total work hours he claimed on his timesheet. He understood that he was in fact being paid by the government during the time he was drafting his blog articles.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

V. (U) Analysis:

(b) (6)

(U//~~FOUO~~) The two network activity reports detailing [redacted] activity on the classified NSA/CSS IS confirmed that [redacted] used the classified IS to conduct personal, non-contract related-activities pertaining to his personal blog, [redacted]. Although he initially denied having used the Classified IS for personal use at any time since December 2013, [redacted] ultimately admitted during his interview with the OIG that he had in fact drafted articles for his personal blog using his classified NSA/CSS workstation in 2014 and 2015. Further, [redacted] acknowledged that the time spent conducting these non-contract-related activities was charged to the government. Despite his acknowledgement, this investigation was unable to ascertain the exact amount of time that was billed to the government.

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

(U//~~FOUO~~) [redacted] is employed by [redacted] and is an NSA/CSS contractor affiliate working on a contract that provides [redacted] support to [redacted]. In this capacity, [redacted] is an authorized user of the NSA/CSS classified IS. As such, NSA/CSS Policy 6-4, *Contractor Use of NSA/CSS Information Systems and Resources* applies to his use of the classified NSA/CSS IS. NSA/CSS Policy 6-4 specifically limits contractor use of NSA/CSS ISs to the performance of tasks authorized by contract, approved by the Contracting Officer, and permitted by the policy itself.² Per Paragraph 9 of the policy,³ contractor affiliates are prohibited from using NSA/CSS ISs for personal use "except for brief, infrequent communications to deal with urgent matters." This limited exception to the personal use prohibition applies only when:

- a. (U) Unavoidable personal matters arise such as, but not limited to, contacting a spouse, dependent family member, or other individuals responsible for a dependent's care; scheduling a physician's appointment; or vehicle maintenance;
- b. (U) The communication does not adversely affect the NSA/CSS mission or reflect poorly on NSA/CSS;
- c. (U) The communication does not result in other than minimal expense to the Government (e.g., the call is local, toll-free);
- d. (U) Time spent using the NSA/CSS IS or resource is not billed to the contract; and
- e. (U) The use is not associated with personal business activities outside the scope and purpose of the contract.

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

(U//~~FOUO~~) During the periods 13 January 2014 – 6 February 2014, and 7 April 2015 – 6 May 2015, [redacted] utilized the classified NSA/CSS IS and workstation to 1) draft a business plan for the development of his personal blog, [redacted] and 2) to draft articles for the purpose of posting them on his personal blog. These activities were personal in nature,

² See NSA/CSS Policy 6-4, Paragraph 1, dated 22 October 2013;³ See NSA/CSS Policy 6-4, dated 22 October 2013;UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

conducting them using a classified NSA/CSS workstation is inconsistent with NSA/CSS Policy 6-4's limited exception to the personal use prohibition. Specifically, [redacted] activities cannot be characterized as unavoidable personal matters requiring his immediate attention; rather, they were activities that were directly associated with the furtherance of his personal business which was outside the scope and purpose of his contract. Further, and as [redacted] himself acknowledged, the time spent conducting such non-contract, non-work-related activities was billed to the contract.

(U//~~FOUO~~) The OIG finds that a preponderance of the evidence exists to support the conclusion that, during the periods 13 January 2014 – 6 February 2014, and 7 April 2015 – 6 May 2015, [redacted] used the classified NSA/CSS IS for non-contract-related personal use to draft a business plan for a personal blog, and to draft articles for the purpose of posting them to the blog, in violation of NSA/CSS Policy 6-4.

VI. (U) Response to Tentative Conclusion:

(U//~~FOUO~~) The tentative conclusion was provided to [redacted] on 3 February 2016. On 17 February 2016, [redacted] responded to the tentative conclusion by stating that he had no further information or comments to provide on the matter.

(U//~~FOUO~~) Because [redacted] provided no new information or mitigation that would impact our analysis, our preliminary conclusion became final.

VII. (U) Conclusion(s):

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

(U//~~FOUO~~) **Substantiated.** The preponderance of the evidence supports the conclusion that, during the periods 13 January 2014 – 6 February 2014, and 7 April 2015 – 6 May 2015, [redacted] used the classified NSA/CSS IS for non-contract-related personal use to draft a business plan for a personal blog, and to draft articles for the purpose of posting them to the blog, in violation of NSA/CSS Policy 6-4.

* (U//~~FOUO~~) This report is property of NSA and may not be disseminated further without specific approval of the NSA OIG and the Office of the General Counsel (OGC). Furthermore, the information in this report cannot be used in affidavits, court proceedings, subpoenas, or for other legal or judicial purposes without prior OIG and OGC approval.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) APPENDIX A

(U) Network Activity Reports

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Excerpts from Network Activity Reports

Edits were made by the OIG for readability purposes.

01/13/2014 13:12:07

[Redacted]

01/13/2014 13:33:10

[Redacted]

(b) (6)

01/14/2014 10:48:29

[Redacted]

01/14/2014 12:33:20

[Redacted]

01/14/2014 13:24:26

[Redacted]

01/16/2014 13:41:26

[Redacted]

01/16/2014 14:12:11

[Redacted]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

[Redacted]

01/16/2014 16:24:38

[Redacted]

01/17/2014 11:39:07

[Redacted]

01/17/2014 12:55:47

[Redacted]

01/17/2014 13:20:04

[Redacted]

01/20/2014 13:33:59

[Redacted]

01/22/2014 14:26:41

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

[Redacted]

01/22/2014 14:27:28

[Redacted]

01/23/2014 10:14:14

[Redacted]

01/23/2014 12:23:46

[Redacted]

(b) (6)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

01/24/2014 09:42:22

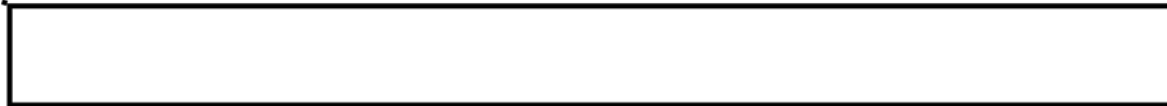


01/24/2014 12:12:38



(b) (6)

01/27/2014 13:48:40



01/28/2014 12:53:33



01/28/2014 14:44:10



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



01/29/2014 09:47:36



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

01/29/2014 10:25:48



01/29/2014 11:27:09

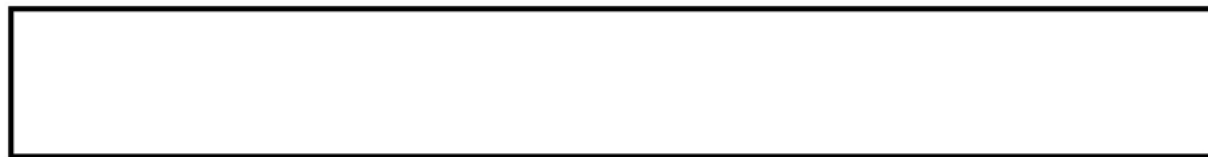


(b) (6)

01/29/2014 13:13:12



01/30/2014 09:05:12



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

01/30/2014 13:23:04

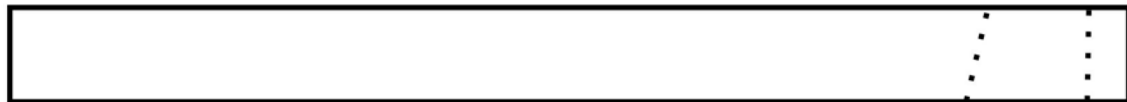


(b) (6)

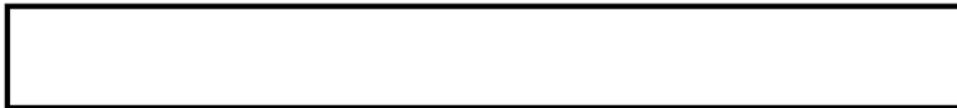
01/31/2014 12:24:48



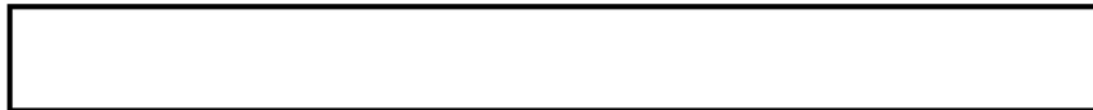
02/03/2014 13:53:36



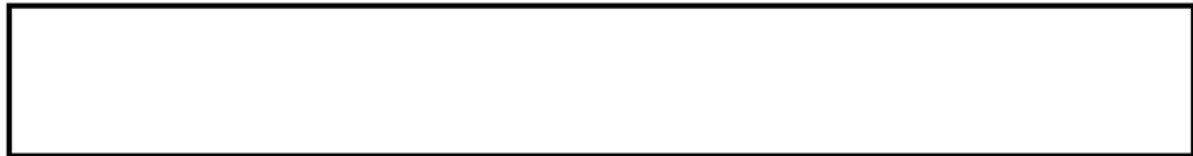
02/05/2014 08:13:40



02/06/2014 08:48:00



04/08/2015 12:08:39



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

[Redacted]

04/08/2015 12:17:29

[Redacted]

(b) (6)

04/08/2015 13:00:29

[Redacted]

04/09/2015 10:40:07

[Redacted]

04/09/2015 12:23:32

[Redacted]

04/10/2015 12:19:21

[Redacted]

04/14/2015 15:24:41

[Redacted]

04/30/2015 16:20:31

[Redacted]

05/06/2015 09:50:40

[Redacted]

05/06/2015 12:10:19

[Redacted]

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) APPENDIX B

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

(b) (6)

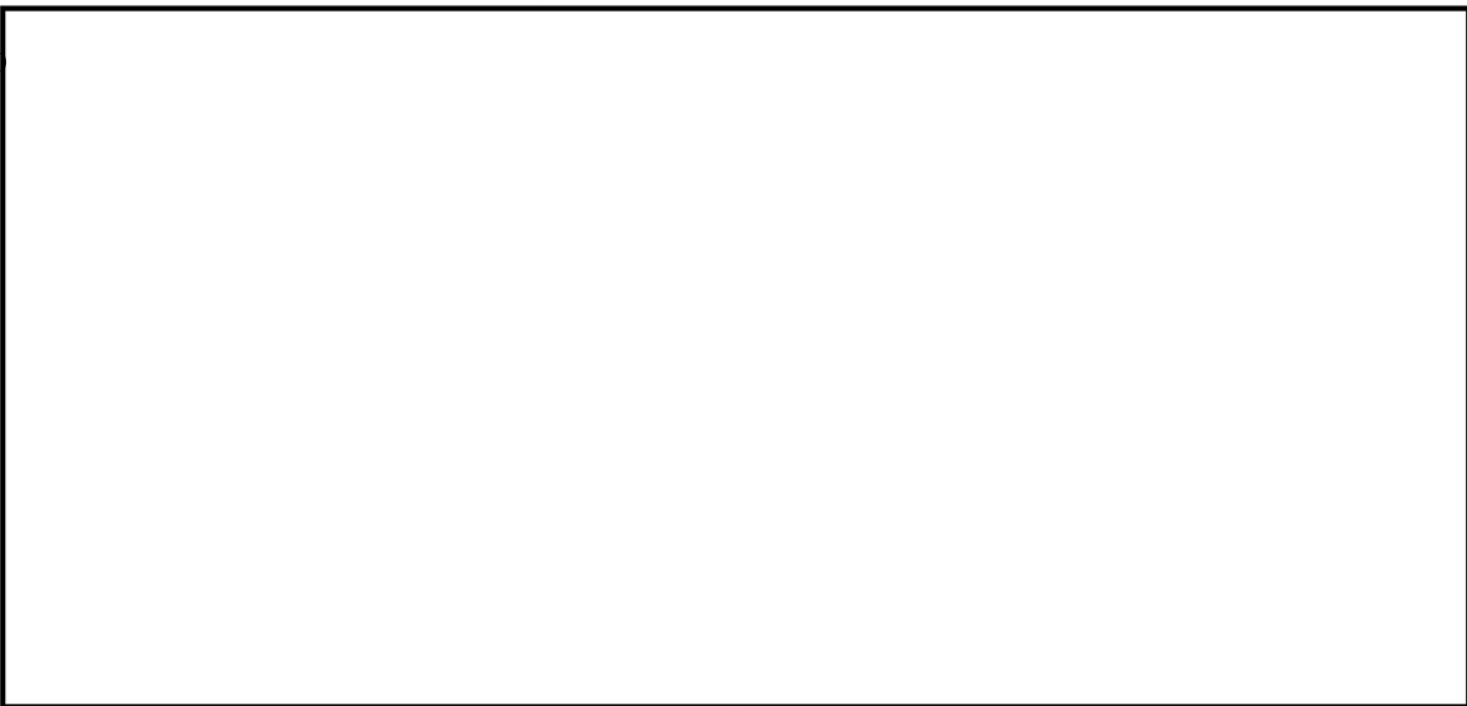
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) APPENDIX C

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

(b) (6)

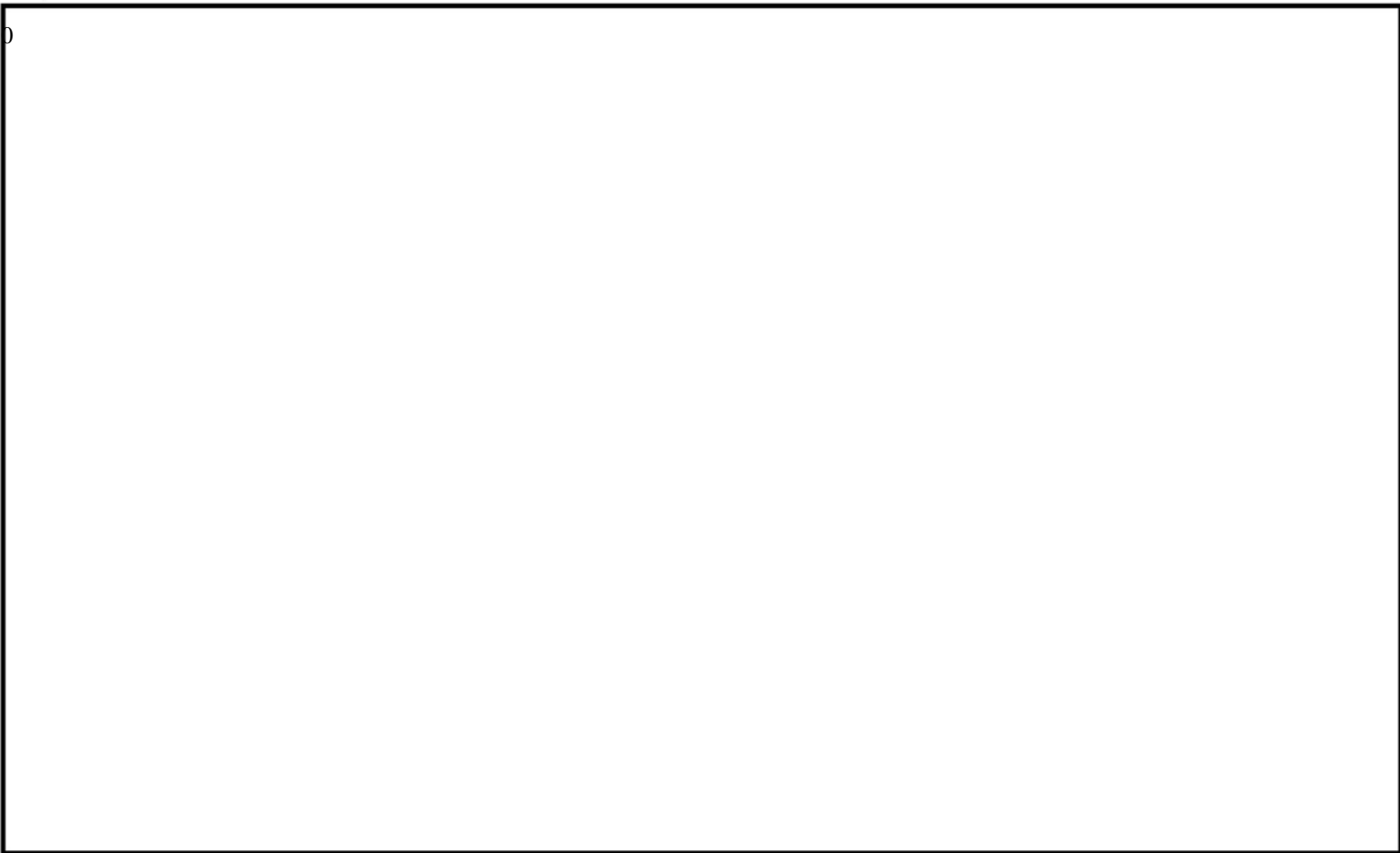


(b) (6)



(b) (6)

(b) (6)



(b) (6)



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

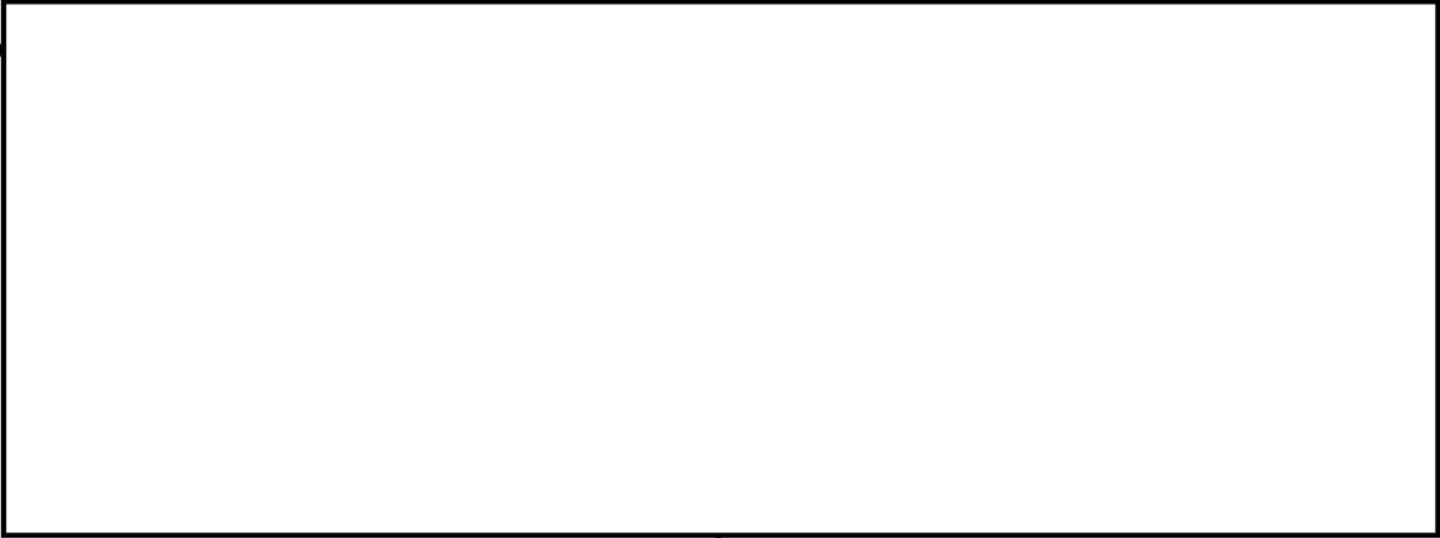
(U) APPENDIX D

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

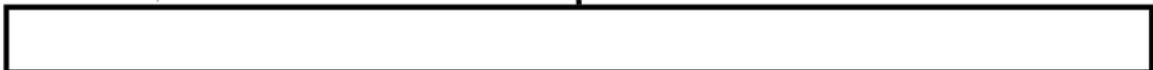
(b) (6)

(b) (6)

(b) (6)



(b) (6)



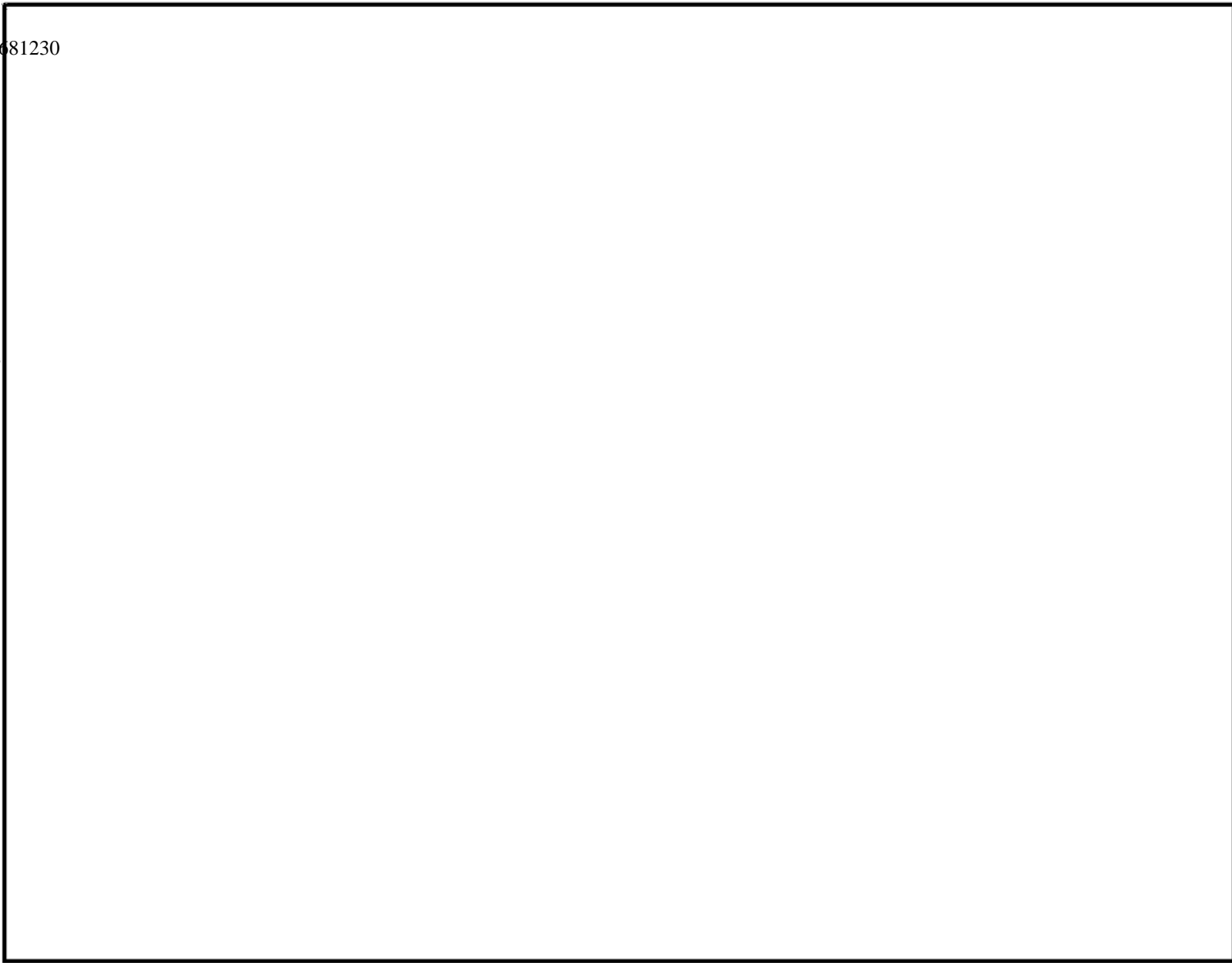
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) APPENDIX E

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

(b) (6)



(b) (6)

[Redacted]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) APPENDIX F

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

(b) (6)

(b) (6)

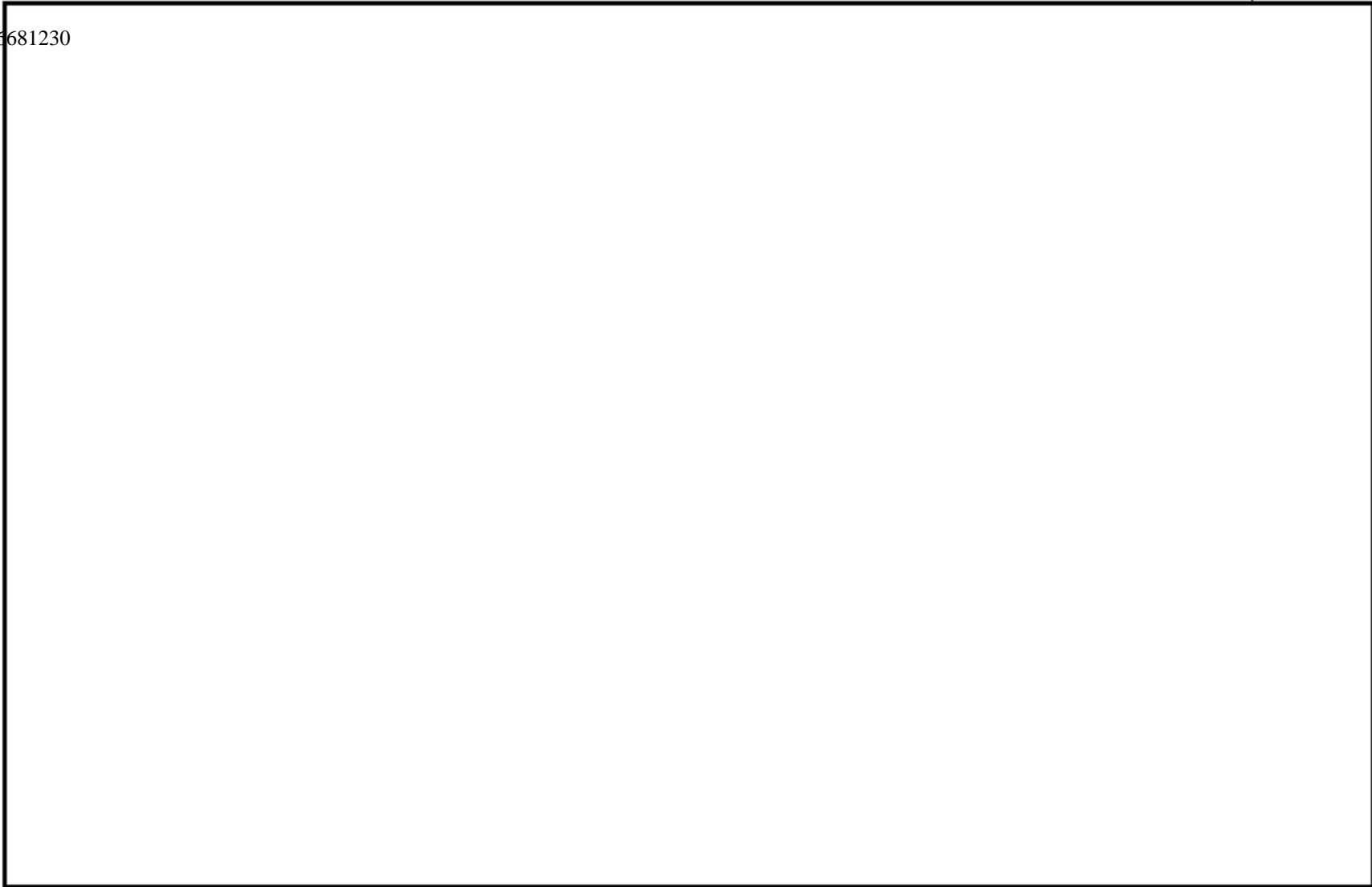
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

APPENDIX G

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b) (6)

(b) (6)



(b) (6)

