~~SECRET//SI//REL TO USA, FVEY~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

8 July 2015

IV-15-0026

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~~) During routine network monitoring, [redacted], an Agency civilian employee, was detected potentially misusing his NSA/CSS Information System (IS). The NSA/CSS Office of the Inspector General (OIG) subsequently opened an investigation into his activity.

(U//~~FOUO~~) An analysis of [redacted] usage of his unclassified IS revealed extensive searching for and viewing of adult-oriented material and pornography.

(U//~~FOUO~~) During his interview with the OIG, [redacted] admitted to intentionally searching for and viewing pornographic material using his NSA/CSS IS unclassified account. When asked to quantify the amount of time he spent searching for pornography, [redacted] estimated that he did it at least one to two times per month for at least the last year. [redacted] stated that he is a [redacted]

(b)(6)

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that from March 2014 through March 2015, [redacted]

- (U//~~FOUO~~) Engaged in an unauthorized use of government resources by searching for and viewing adult-oriented material and pornography on an NSA/CSS IS in violation of DoD 5500.7-R, "Joint Ethics Regulation," Paragraph 2-301, Use of Federal Government Resources, and NSA/CSS Policy 6-6, dated 30 September 2004, revised 15 October 2013; and

- (U//~~FOUO~~) Engaged in prohibited activity on an NSA/CSS IS by searching for and viewing adult-oriented material and pornography in violation of NSA/CSS Policy 6-6, dated 1 August 2014, and all subsequent revisions.[1]

---

[1] (U//~~FOUO~~) There are numerous versions of NSA/CSS Policy 6-6 applicable to this investigation:
(1) "*Use of Unclassified Information Systems Such as the Internet,*" dated 30 September 2004, revised 15 October 2013 [covers alleged misuse from March 2014 – July 2014];
(2) "*Use of Unclassified Information Systems and Internet-Based Capabilities,*" dated 1 August 2014, which superseded NSA/CSS Policy 6-6, dated 30 September 2004, revised 15 October 2013 [covers alleged misuse from August 2014 – 14 December 2014];
(3) "*Use of Unclassified Information Systems and Internet-Based Capabilities,*" dated 1 August 2014, revised 15 December 2014 [covers alleged misuse from 15 December 2014 – 03 March 2015];

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~*20400501*~~

(U//~~FOUO~~) A copy of this report will be forwarded to Employee Relations (MR) for any action deemed appropriate. A summary of the investigative findings will be forwarded to the Associate Directorate for Security and Counterintelligence (ADS&CI), Special Actions (Q242), and [redacted] supervisor.

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

(4) *"Use of Unclassified Information Systems and Internet-Based Capabilities,"* dated 01 August 2014, revised 04 March 2015 [covers alleged misuse from 04 March 2015 - current].

(U//~~FOUO~~) The OIG examined [redacted] conduct against all applicable versions of NSA/CSS Policy 6-6. However, within the scope of this investigation, the relevant language remains the same in all three of the most recent versions of Policy 6-6. Accordingly, the OIG's analysis of any alleged misuse by [redacted] occurring after 01 August 2014 is combined.

II. (U) BACKGROUND

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

(U) Introduction

~~(S//SI//REL)~~ GG-12, is the Deputy Branch Chief of the a position he has held since July 2014. Prior to working in he worked in the from June 2009 to June 2014. entered on duty at NSA/CSS on

(b)(6)

(U) Prior Incident

(U//~~FOUO~~) In November 2009, the NSA/CSS Information Systems Incident Response Team (NISIRT), through routine monitoring, detected that the IP address associated with unclassified NSA IS was used to perform searches for adult-oriented images and to view adult-oriented images.

(U//~~FOUO~~) On 19 November 2009, the OIG informed that he violated DoD Joint Ethics Regulation (JER) and NSA/CSS Policy 6-6 by accessing adult-oriented material using his NSA/CSS unclassified account. In November 2009, the OIG asked him to review the relevant policies and acknowledge that he would adhere to them in the future. On 30 November 2009, confirmed that he read the policies and would adhere to them in the future.[2] The OIG notified MR and Q234 of this incident on 28 December 2009.

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

(U) Current Allegations

~~(S//REL)~~ On 14 August 2014, ADS&CI personnel informed the OIG that the [3] detected using his NSA/CSS unclassified IS to

---

[2] (U//~~FOUO~~) During his interview with the OIG on 07 May 2015, denied that he misused his NSA/CSS unclassified IS in regard to the November 2009 incident and emails. claimed that he was authorized to share his access to his unclassified NSA/CSS IS with his colleagues (in order to enable them to conduct investigative research for their mission), and that the misuse detected in 2009 was attributable to these individuals. The OIG does not find denial to be credible, based in part upon subsequently acknowledging that he was the one who authorized the sharing and the lack of any such explanation or information in his 30 November 2009 response to the OIG.

[3] ~~(C//REL)~~ supports the ADS&CI mission of safeguarding NSA/CSS information from exploitation, compromise, and unauthorized disclosure by deterring, detecting, and mitigating insider threats. To accomplish its mission, works in partnership with the Technology Directorate's NISIRT to audit and monitor NSA's internal TOP SECRET, SECRET, and UNCLASSIFIED networks.

search for adult-oriented material/pornography. The date range of the alleged misuse detected was 19 March 2014 to 03 August 2014.

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

~~(S//REL)~~ On 02 September 2014, [redacted] informed the OIG that they had detected [redacted] searching for and viewing pornographic images on his NSA/CSS unclassified IS. The date range of the alleged misuse detected by [redacted] was 20 August 2014 to 25 August 2014.

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

~~(S//REL)~~ On 05 December 2014, [redacted] personnel informed the OIG that they had again detected [redacted] searching for and viewing pornographic images on his NSA/CSS unclassified IS. The date range of the alleged misuse detected by [redacted] which included over 30 instances of misuse, was 05 November 2014 to 02 December 2014.

~~(S//REL)~~ On 03 April 2015, at the request of the OIG, [redacted] provided the OIG additional information concerning [redacted] searching for and viewing of pornographic images on his NSA/CSS unclassified IS. [redacted] provided additional information to the OIG concerning the previously reported misuse, and also conducted a new analysis of [redacted] recent usage of his NSA/CSS unclassified system. The date range of the review component was 16 April 2014 to 04 December 2014, while the new analysis covered 23 December 2014 to 22 March 2015. Both [redacted] analyses revealed dozens of examples of text and imagery related to [redacted] searching for and viewing pornographic images on his NSA/CSS unclassified IS.

(U) Applicable Authorities

(U) This investigation looked at possible violations of the following authorities:

(U//~~FOUO~~) NSA/CSS Policy 6-6, "*Use of Unclassified Information Systems Such as the Internet*," dated 30 September 2004, revised 15 October 2013 [covers alleged misuse from March 2014 – July 2014];

(U//~~FOUO~~) NSA/CSS Policy 6-6, "*Use of Unclassified Information Systems and Internet-Based Capabilities*," dated 1 August 2014, which superseded NSA/CSS Policy 6-6, dated 30 September 2004, revised 15 October 2013 [covers alleged misuse from August 2014 – 14 December 2014];

(U//~~FOUO~~) NSA/CSS Policy 6-6, "*Use of Unclassified Information Systems and Internet-Based Capabilities*," dated 1 August 2014, revised 15 December 2014 [covers alleged misuse from 15 December 2014 – 03 March 2015];

(U//~~FOUO~~) NSA/CSS Policy 6-6, "*Use of Unclassified Information Systems and Internet-Based Capabilities*," dated 01 August 2014, revised 04 March 2015 [covers alleged misuse from 04 March 2015 - current]; and

(U) DoD 5500.7-R, "Joint Ethics Regulation," Paragraph 2-301, Use of Federal Government Resources.

(U//~~FOUO~~) Applicable excerpts from the above authorities are contained in Appendix A.

III. (U) FINDINGS

(U//~~FOUO~~) ***ALLEGATION****: Did* [redacted] *engage in an unauthorized use of government resources and misuse an NSA/CSS IS by searching for and viewing adult-oriented material and pornography in violation of DoD 5500.7-R, "Joint Ethics Regulation," and NSA/CSS Policy 6-6?*

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

(U) Documentary Evidence

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

~~(S//REL)~~ At various times throughout 2014 and 2015 [redacted] detected [redacted] using his NSA/CSS unclassified IS to search for and view adult-oriented material and pornography. [redacted] documented [redacted] misuse in numerous [redacted] reports, which they also provided to the OIG. Samples of [redacted] usage of his NSA/CSS unclassified IS detected by [redacted] are attached at Appendix B.[4]

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

(U//~~FOUO~~) During his interview on 07 May 2015, [redacted] denied that he misused his NSA/CSS unclassified IS in November 2009. Email correspondence between [redacted] and the OIG concerning [redacted] denial of his previous misuse of NSA/CSS unclassified IS is attached as Appendix C.

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

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

(U) Testimonial Evidence

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

(U//~~FOUO~~) On 07 May 2015, [redacted] was interviewed and provided the following sworn testimony:

[4] ~~(S//REL)~~ One of the [redacted] reports contains concerns that [redacted] may have been searching for and/or viewing child pornography on his NSA unclassified IS. Accordingly, on 29 April 2015 (email) and 06 May 2015 (discussion – phone call), the OIG shared these concerns with the appropriate personnel at the Federal Bureau of Investigation.

(U//~~FOUO~~) He acknowledged that he intentionally used his NSA/CSS unclassified IS to search for and view pornography. He estimated that, while at work, he has searched for pornography at least a couple of times a month for about a year or more.

(b) (6)

(U//~~FOUO~~) He is a [redacted]
He has shared his background with NSA Security personnel. [redacted] is unpredictable – for example, some months are better than others.

(U//~~FOUO~~) He denies searching for, or viewing of, child pornography, and has no interest in anything related to pedophilia. He has no mission use for his unclassified account, and intends to ask his management to remove it from his workspace. With respect to his searches for escort and/or massage services, he never actually used the services.

(U//~~FOUO~~) He denied any misuse in regard to the November 2009 incident and emails. He claimed that he was authorized to share his access to his unclassified NSA/CSS IS with his colleagues (in order to enable them to conduct investigative research for their mission), and that the misuse detected in 2009 was attributable to these individuals.[5]

(U//~~FOUO~~) He is aware that using his unclassified account to search for pornography was inappropriate and against NSA policy.

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

(U) Analysis and Conclusions

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

(~~S//REL~~) A review of the [redacted] reports detailing [redacted] use of his unclassified NSA/CSS IS reveals that he repeatedly searched for and viewed adult-oriented material and pornography on his unclassified IS. During his testimony, [redacted] admitted he searched for and viewed pornography at least a couple of times a month for about a year or more.

(U//~~FOUO~~) DoD 5500.7-R, "Joint Ethics Regulation," (JER) requires that Government communication systems and equipment, which includes NSA/CSS unclassified ISs, must be operated for official use and authorized purposes only, that the use of the systems and equipment serve a legitimate public interest, and that they are not to be used for activities that would reflect adversely on the DoD or the DoD Component. The JER states, "Official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the Federal Government." The JER also states that brief personal communications are permitted as long as they do not reflect adversely on the DoD and NSA, specifically citing to pornography as example of use that is not permitted.

[5] However, in response to a subsequent request from the OIG for additional detail as to his statement that he was authorized to share his access to his unclassified NSA/CSS IS, he stated, via an email response (Appendix C), that he was the one that authorized the sharing of his unclassified NSA/CSS IS with his colleagues.

(U//~~FOUO~~) [redacted] admitted to using his NSA/CSS unclassified ISs to search for and view pornography. Searching for or viewing adult-oriented material or pornography does not constitute an official use or authorized purpose of the government resource, nor does it serve a legitimate public interest. Further, [redacted] activities undoubtedly reflect adversely on both the DoD and NSA. Therefore, by using his computer to search for and view adult-oriented material and pornography, [redacted] violated the JER.

(U//~~FOUO~~) NSA/CSS Policy 6-6 governs the use of NSA/CSS unclassified ISs by NSA/CSS civilian personnel such as [redacted]. There were several revisions to NSA/CSS Policy 6-6 during the period of misuse by [redacted] applicable to this investigation, with the earliest applicable version dated 30 September 2004 (revised 15 October 2013). This version permitted the use of NSA/CSS ISs for purposes "that are directly related to official unclassified U.S. Government business," and for individuals to "conduct limited personal communications" so long as they did so in a manner consistent with the provisions of the JER. [redacted] use of his NSA/CSS IS to search for adult-oriented material and pornography was not related to official U.S. Government business. Further, as discussed in the analysis of the JER above, searching for or viewing adult-oriented material or pornography does not constitute an official use or authorized purpose of the government resource. Accordingly, [redacted] use of his NSA/CSS IS to search for adult-oriented material in April 2014 (see Appendix B for a sample of the activity) violates NSA/CSS Policy 6-6, dated 30 September 2004 and revised 15 October 2013.

(U//~~FOUO~~) In the context of analyzing the propriety of [redacted] alleged misconduct under subsequent versions of NSA/CSS Policy 6-6, specifically those dated on or after 01 August 2014, the relevant language in the Policies that is applicable to this investigation, and therefore any associated analysis, remains the same: users of NSA/CSS unclassified ISs must avoid engaging in prohibited activities, of which accessing pornography is explicitly noted as such, while using ISs. [redacted] use of his unclassified IS to search for and view pornography, as evidenced by the material in Appendix B, is specifically prohibited under NSA/CSS Policy 6-6.

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

(U//~~FOUO~~) Ultimately, no version of NSA/CSS Policy 6-6 condones using NSA/CSS ISs to search for or view adult-oriented material and pornography.

(U//~~FOUO~~) Thus, the OIG concluded by a preponderance of the evidence that, from April 2014 through March 2015, [redacted]

- (U//~~FOUO~~) Engaged in an unauthorized use of government resources by searching for and viewing adult-oriented material and pornography on an NSA/CSS IS in violation of DoD 5500.7-R, "Joint Ethics Regulation," Paragraph 2-301, Use of Federal Government Resources, and NSA/CSS Policy 6-6, dated 30 September 2004, revised 15 October 2013; and

- (U//~~FOUO~~) Engaged in prohibited activity on an NSA/CSS IS by searching for and viewing adult-oriented material and pornography in violation of NSA/CSS Policy 6-6, dated 1 August 2014, and all subsequent revisions.

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

(U//~~FOUO~~) [redacted] was provided the tentative conclusions on 19 June 2015. On 23 June 2015, [redacted] acknowledged receipt of the tentative conclusions, but did not provide any additional information.

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

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

V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that, from April 2014 through March 2015,

- (U//~~FOUO~~) Engaged in an unauthorized use of government resources by searching for and viewing adult-oriented material and pornography on an NSA/CSS IS in violation of DoD 5500.7-R, "Joint Ethics Regulation," Paragraph 2-301, Use of Federal Government Resources, and NSA/CSS Policy 6-6, dated 30 September 2004, revised 15 October 2013; and

- (U//~~FOUO~~) Engaged in prohibited activity on an NSA/CSS IS by searching for and viewing adult-oriented material and pornography in violation of NSA/CSS Policy 6-6, dated 1 August 2014, and all subsequent revisions.

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report will be forwarded to Employee Relations (MR) for any action deemed appropriate. A summary of the investigative findings will be forwarded to the Associate Directorate for Security and Counterintelligence (ADS&CI), Special Actions (Q242), and [redacted] supervisor.

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

[redacted]
Senior Investigator

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

Concurred by:

[redacted]
Assistant Inspector General
For Investigations

APPENDIX A

(U) Applicable Authorities

(U//~~FOUO~~) NSA/CSS Policy 6-6: "*Use of Unclassified Information Systems Such as the Internet,*" dated 30 September 2004, revised 15 October 2013[6]

(U) Policy

1. (U) NSA/CSS provides *authorized users* with access to unclassified information systems (ISs) for the purpose of research, training, and/or communications that are directly related to official unclassified U.S. Government business.

. . .

3. (U) Supervisors may authorize NSA/CSS affiliates to conduct limited personal communications while using an NSA/CSS-sponsored account for official business, or while using U.S. Government resources such as ISs consistent with the provisions contained in the Joint Ethics Regulation (JER) . . .

25. (U) All users shall

...

(n) (U) Use good judgment and common sense when accessing and/or communicating on unclassified ISs;

(U) Definitions

. . .

41. (U) Authorized User – An individual who has received approval to utilize an unclassified IS for the purpose of conducting research, training, and/or communications that are directly related to official U.S. Government business.

(U//~~FOUO~~) NSA/CSS Policy 6-6: "*Use of Unclassified Information Systems and Internet-Based Capabilities*," dated 01 August 2014, Revised 04 March 2015[7]

(U) Policy

1. (U) NSA/CSS shall provide unclassified, associated access IS accounts to authorized users to conduct official NSA/CSS business.

(U) Approved Activities

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

j. Access, with supervisory approval, their personal IbC accounts and conduct limited *personal use* that is consistent with Reference b and is not a *prohibited activity*.

---

[6](U//~~FOUO~~) For all IS activity prior to 01 August 2014.

[7](U//~~FOUO~~) For all IS activity on or after 01 August 2014. NSA/CSS Policy 6-6, "Use of Unclassified Information Systems and Internet-Based Capabilities," dated 1 August 2014, superseded NSA/CSS Policy 6-6, dated 30 September 2004, revised 15 October 2013. Given the date range of the allegations, other versions of Policy 6-6 are also applicable to this investigation: the original 01 August 2014 version and the 15 December 2014 version. However, the relevant language for this investigation remains the same in all three versions of Policy 6-6.

(U) Prohibited Activities

18. (U) Users shall avoid all prohibited activity and must not take any action (e.g., email, web-site registrations, web-site access) 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:

h. (U) Violating laws or regulations or participating in other uses of any NSA/CSS IS that are incompatible with public service.

(U) Responsibilities

39. (U) Users of associated access shall:

d. (U) Use an unclassified NSA/CSS IS or other IS permitted under paragraph 20 to conduct authorized, official business;

(U) Definitions

63. (U) Official Use – Described in JER (Reference b), Paragraph 2-301.a(1) and, for the purposes of this policy, includes authorized communication or activities conducted as an assigned NSA/CSS affiliate function.

69. (U) Prohibited Activity – Download, installation, or use of unauthorized software (e.g. applications, games, peer-to-peer software, movies, music videos, files); accessing pornography; unofficial advertising, selling, or soliciting; improperly handling classified information; using an NSA/CSS or DoD IS to gain unauthorized access to other systems or networks; endorsing non-[U.S. Government] products or services; participating in any lobbying activity or engaging in any prohibited partisan activity; posting NSA/CSS or DoD information to external newsgroups, bulletin boards, or other public forums without authorization; other uses incompatible with public service.

(U) DoD 5500.7-R, "Joint Ethics Regulation," Chapter 2, Standards of Ethical Conduct, Section 3, DoD Guidance, Paragraph 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.*

(1) Official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the Federal Government …

(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:

(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;

(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 the communications system; improving the morale of DoD employees stationed for extended periods 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 incompatible with public service); …

APPENDIX B

(U) Sampling of the Searches Conducted by [redacted] on His Unclassified NSA/CSS IS and/or the Images Viewed by [redacted] on His Unclassified NSA/CSS IS

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

WARNING:
THIS APPENDIX CONTAINS GRAPHIC IMAGES AND/OR LANGUAGE

~~SECRET//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
ASSOCIATE DIRECTORATE FOR SECURITY AND COUNTERINTELLIGENCE
[redacted] DIVISION

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

UNITED STATES GOVERNMENT

MEMORANDUM

MEMORANDUM FOR THE RECORD

DATE: 30 March 2015

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

SUBJECT/USER: [redacted]
FILE NUMBER: [redacted]
Case control number: [redacted]

~~(S//REL)~~ At the request of [redacted] management, focused analysis of [redacted] was conducted in support of an inquiry by the Office of the Inspector General (IG). The IG is concerned with previously reported incidents regarding [redacted] viewing inappropriate sexual content on HIS government computer. Please reference previous case numbers [redacted]

~~(S//NF)~~ [redacted] is a Civilian affiliate assigned to [redacted] Between 23 December 2014 and 22 March 2015, [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

~~(S//NF)~~ **Analyst comments:** Based on the search terms alone, it is evident [redacted] was attempting to view pornographic material. [redacted]

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20400601~~

~~SECRET//NOFORN~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

~~SECRET//NOFORN~~

[redacted]

~~(S//REL)~~ The UNCLASSIFIED network was reviewed for [redacted] activity from 5 December 2014 to 23 March 2015. Below, [redacted] network/user name activity is detailed:

Network	User account
UNCLASSIFIED	[redacted]

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

(U//~~FOUO~~) This information is provided for lead purposes only. Should you have any questions, please contact the undersigned at 969-8163, secure.

[redacted]
Office of Counterintelligence
Associate Directorate for Security and Counterintelligence
National Security Agency

Enclosures:
1. Supporting Data - Text
2. Supporting Data - Examples

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

Distribution:
1. D14
2. Q242

~~SECRET//NOFORN~~

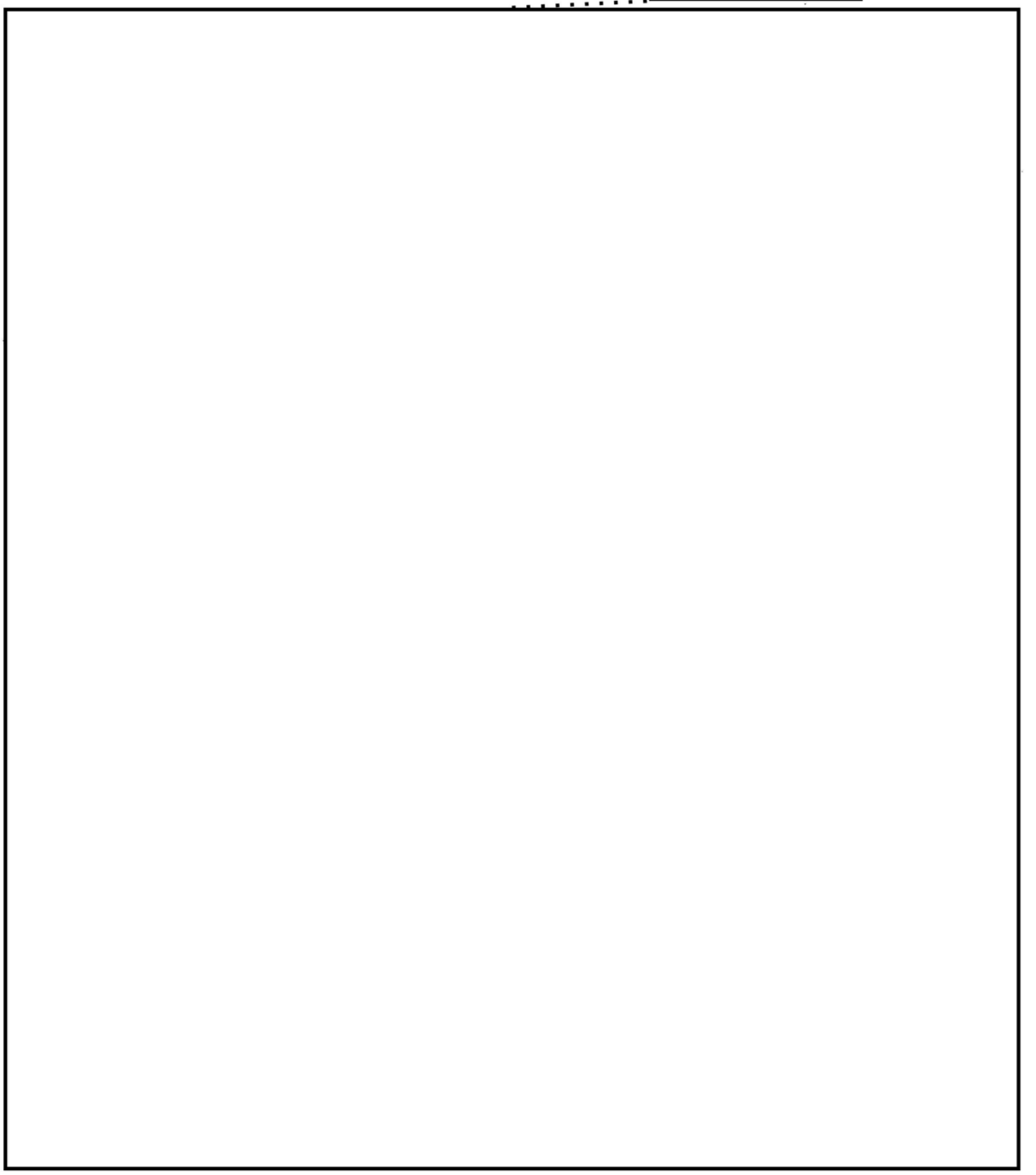
Enclosure 1

Supporting Data - Text

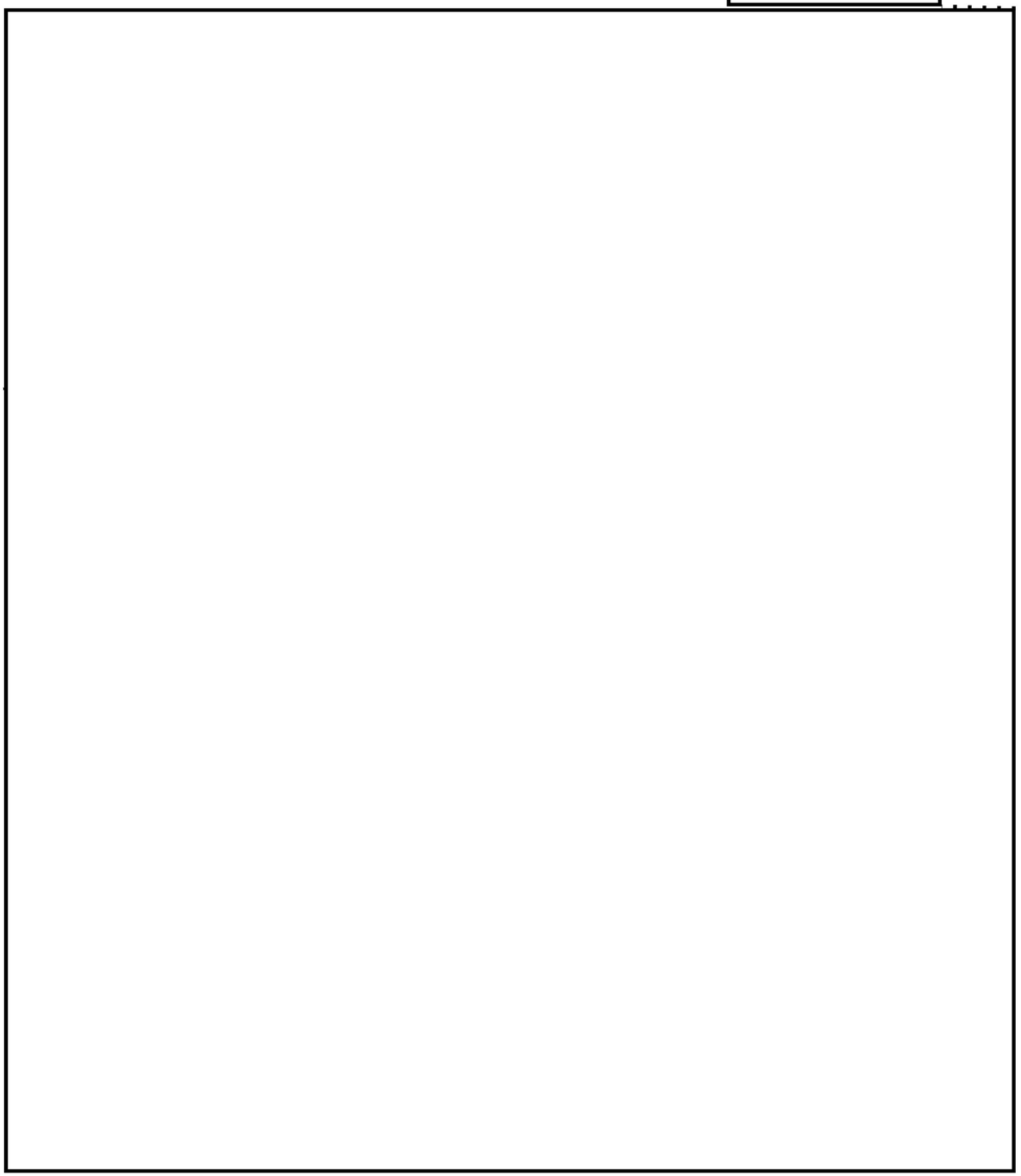
The supporting data contained in this enclosure is for limited distribution and should not be disseminated outside of ADS&CI without prior approval

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

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)



(b)(1)
(b)(3)-P.L. 86-36
(b)(6)



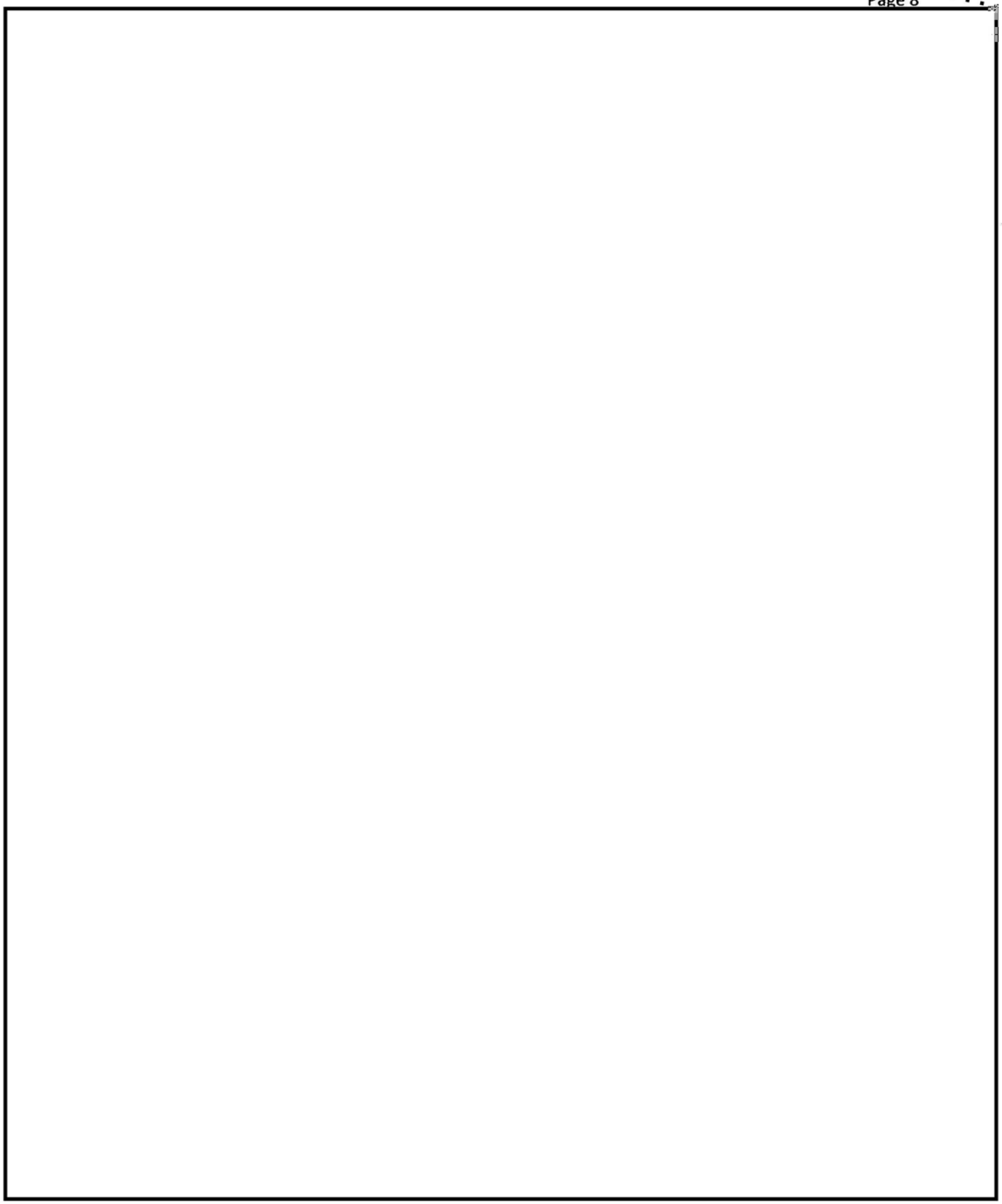
(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

Enclosure 2

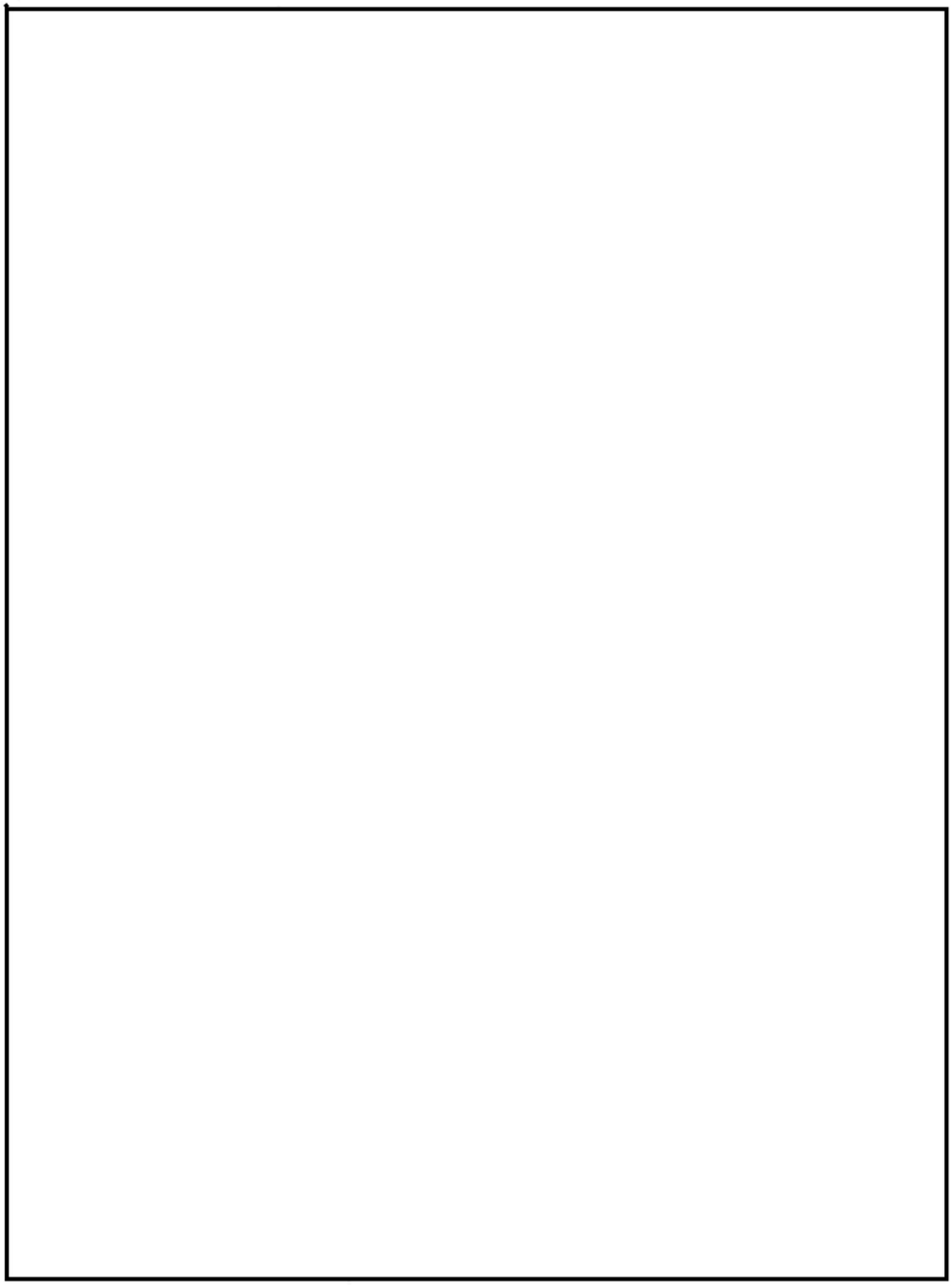
Supporting Data – Examples

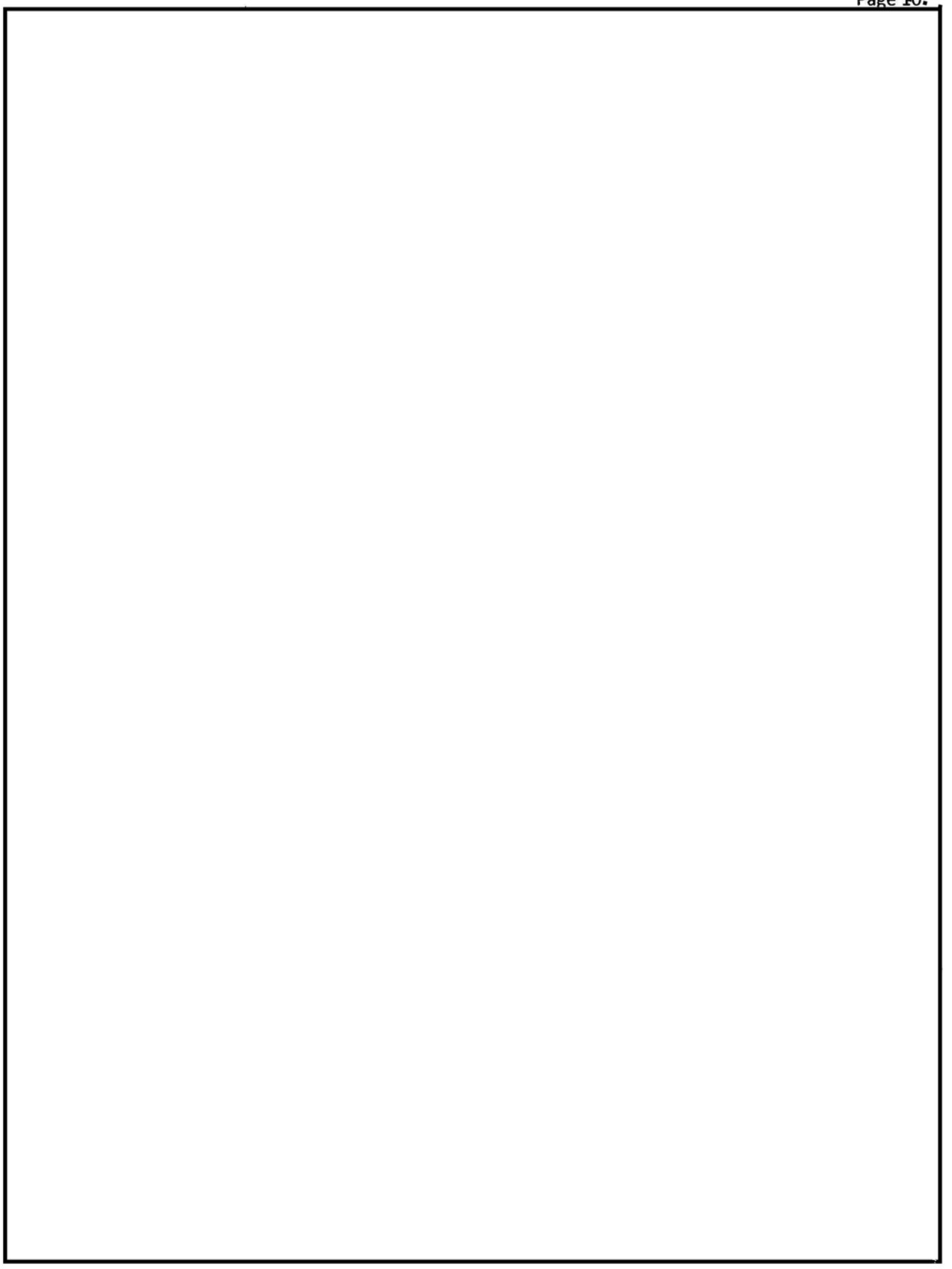
The supporting data contained in this enclosure is for limited distribution and should not be disseminated outside of ADS&CI without prior approval

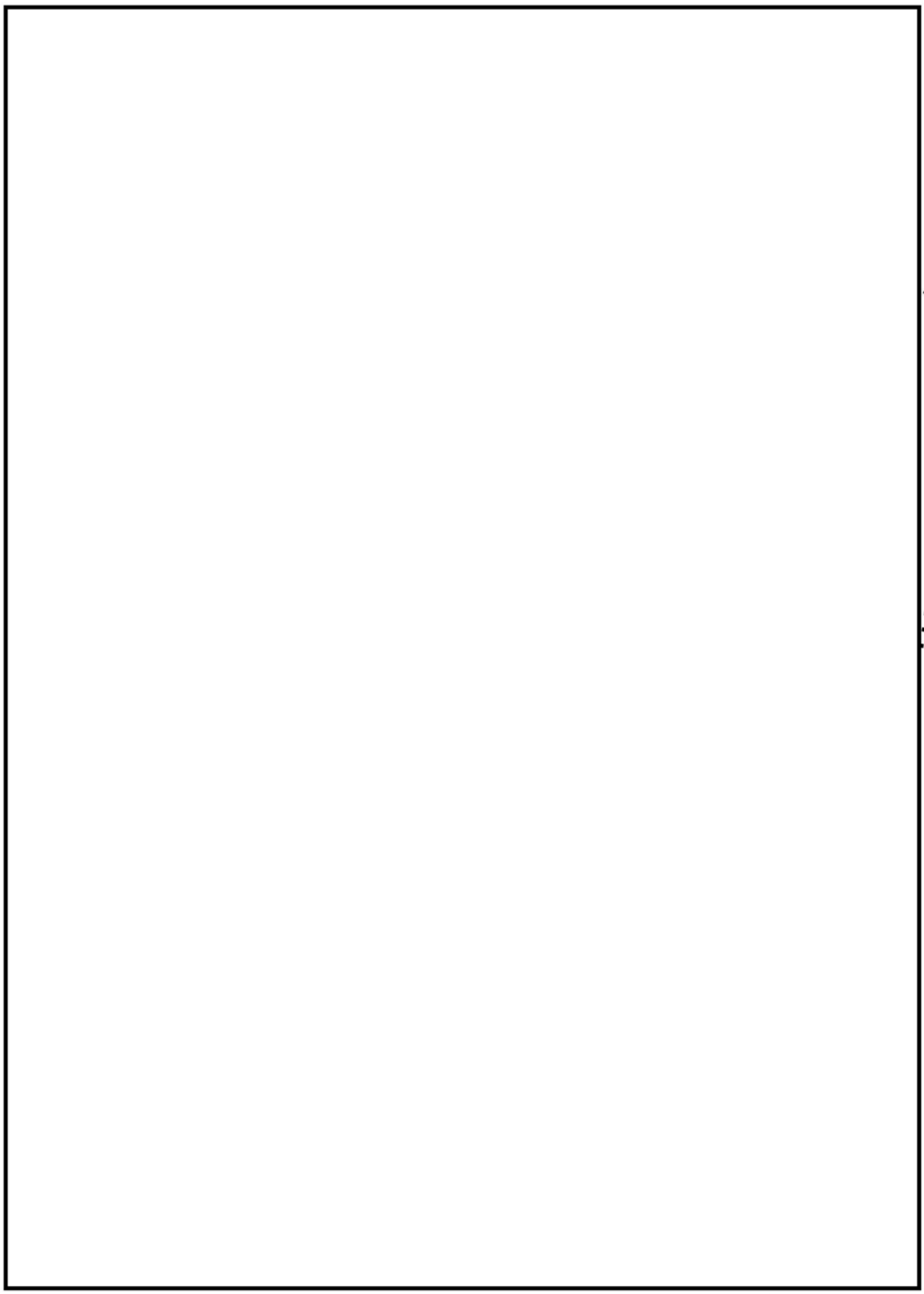
(b)(3)-P.L. 86-36



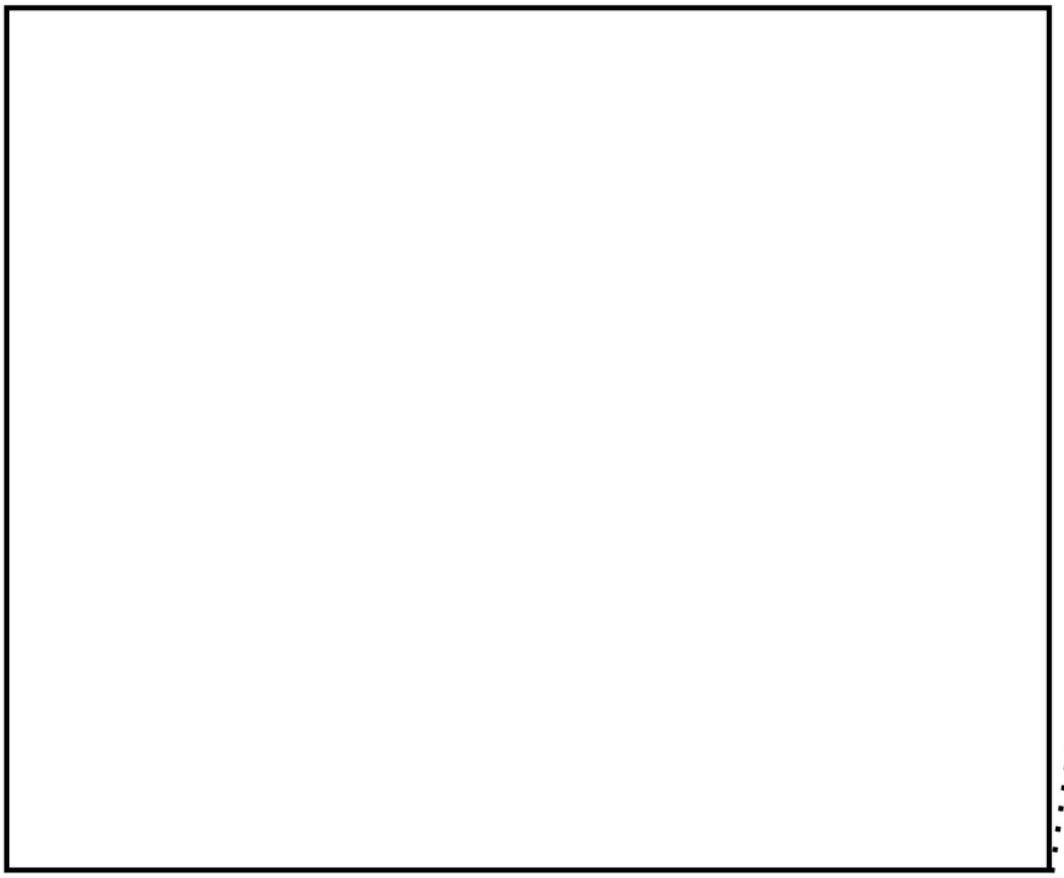
(b)(1)
(b)(3)-P.L. 86-36
(b)(6)







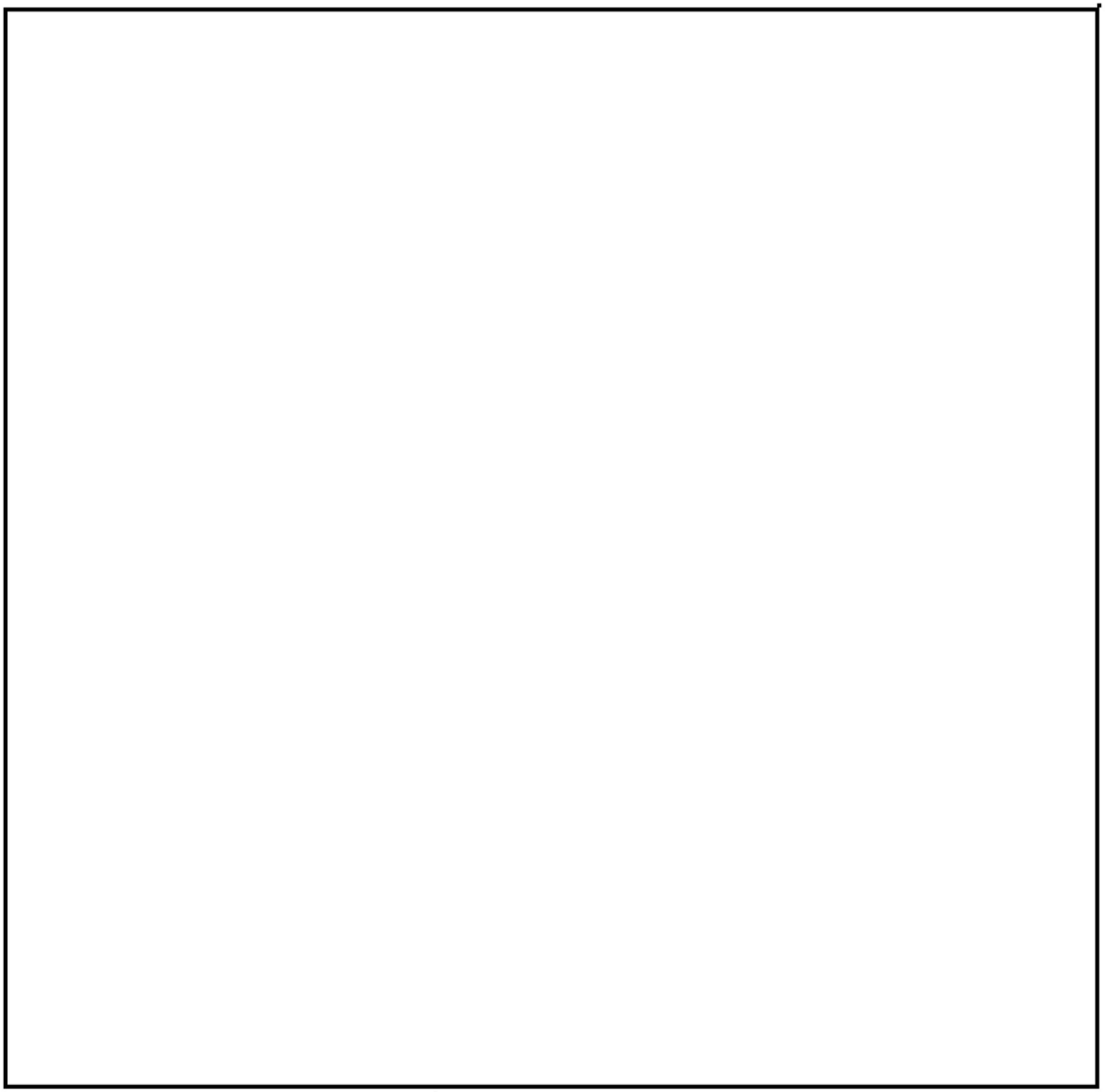
(b)(1)
(b)(3)-P.L. 86-36
(b)(6)



(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

~~SECRET//REL TO USA, FVEY~~

The information contained in this report is for limited distribution and should not be disseminated outside of ADS&CI without prior approval



Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20390401~~

~~SECRET//REL TO USA, FVEY~~

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

~~SECRET//REL TO USA, FVEY~~

The information contained in this report is for limited distribution and should not be disseminated outside of ADS&CI without prior approval

(~~S//REL~~) **Analyst Recommendation:** The reporting analyst recommends the following case be sent to the IG office.

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

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

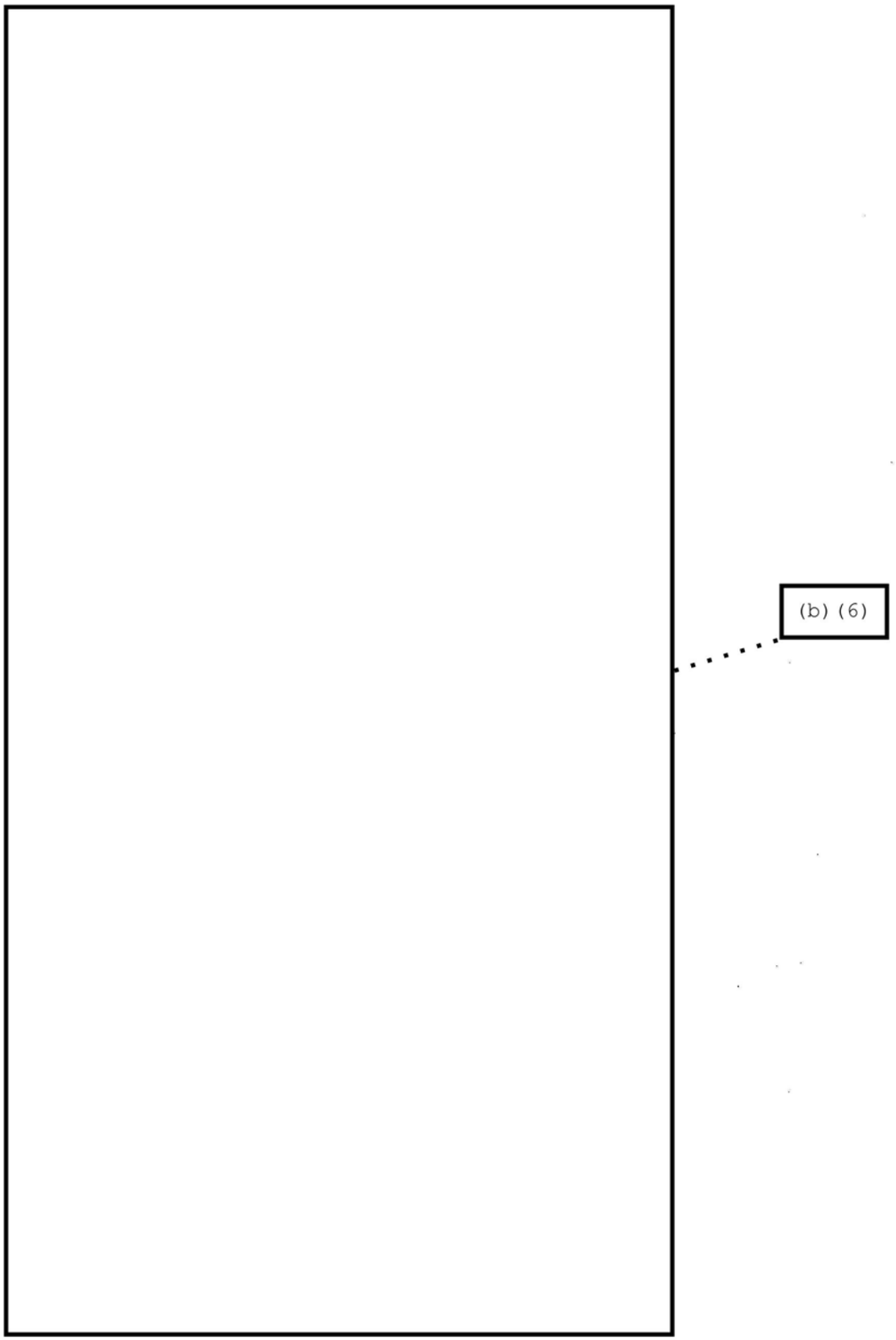
Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20390401~~

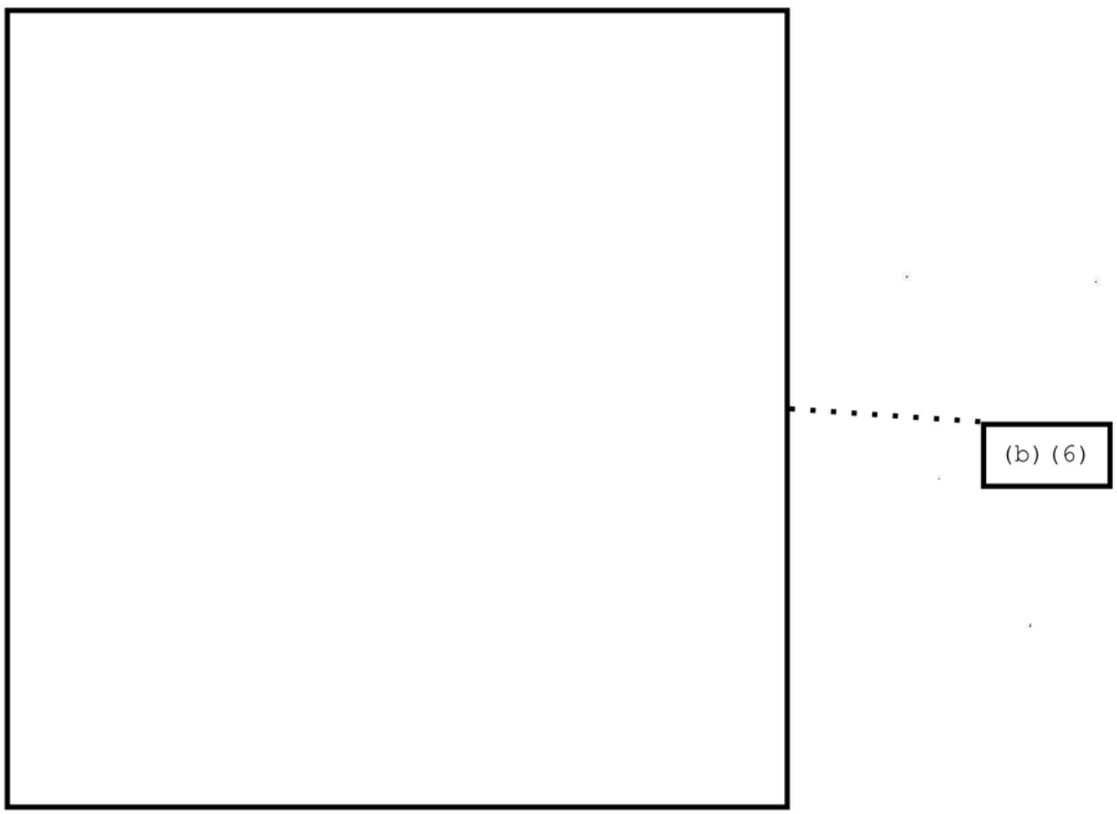
~~SECRET//REL TO USA, FVEY~~

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

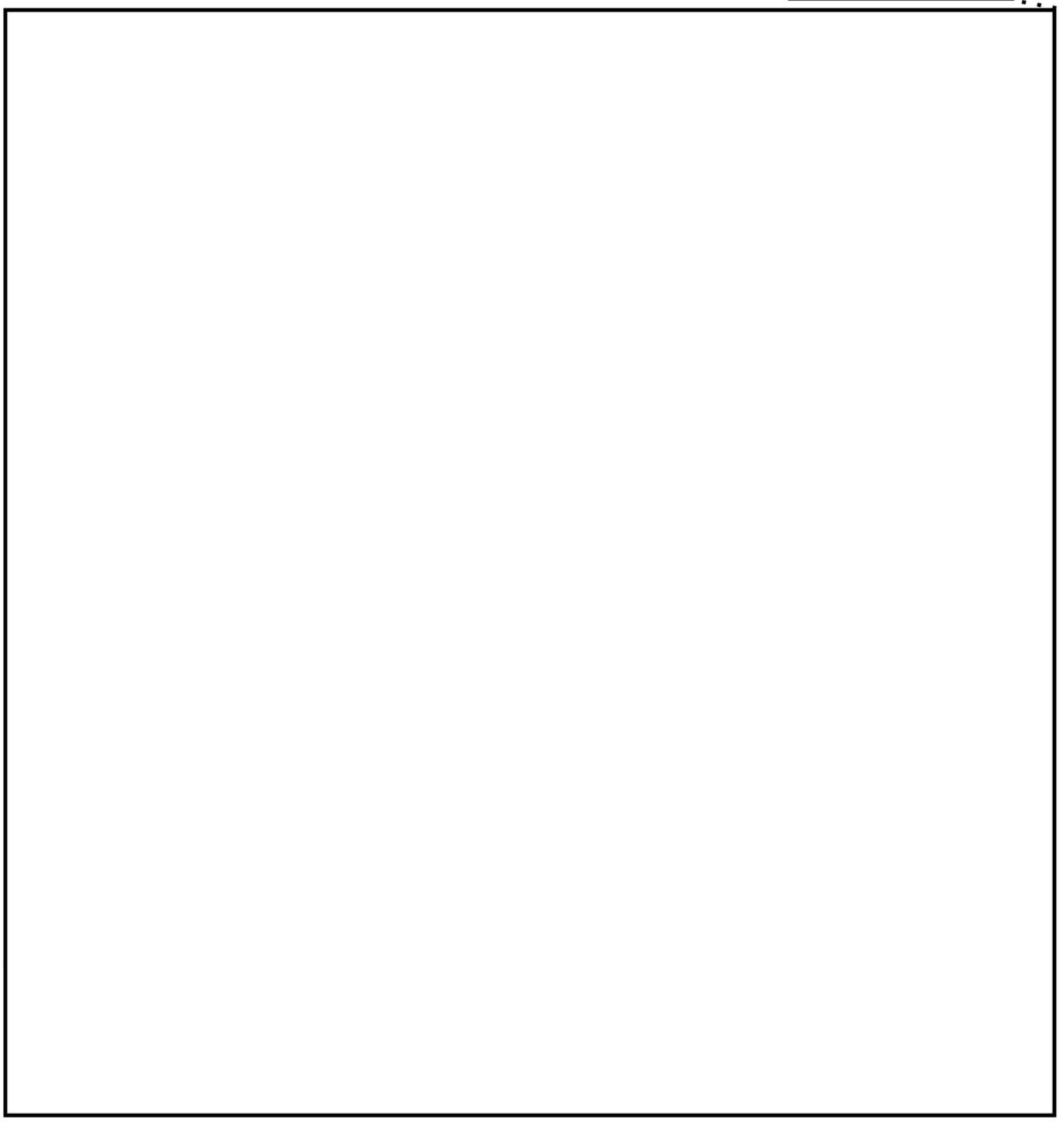
search history

(b)(6)



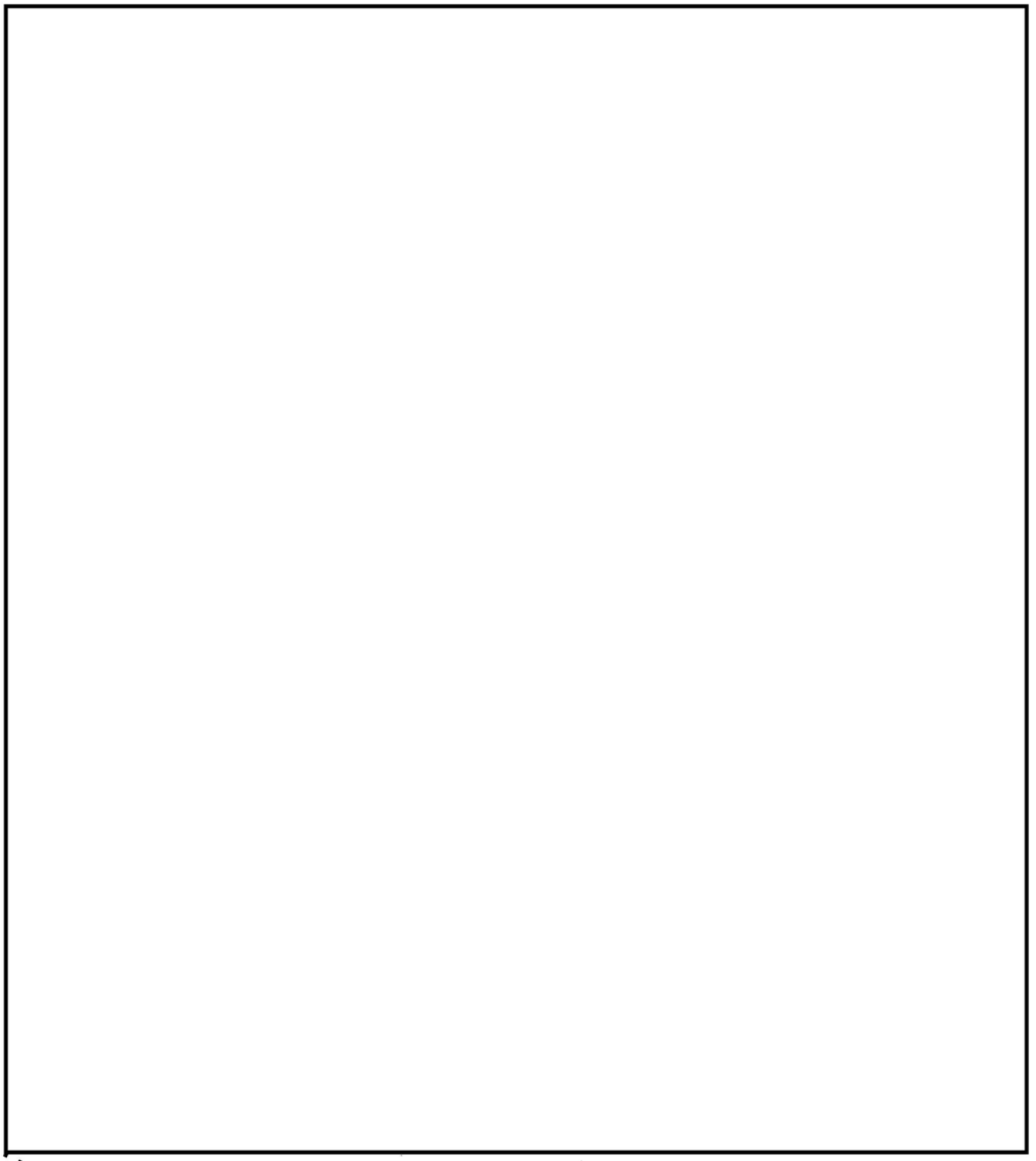


~~SECRET//REL TO USA, FVEY~~



Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20390501~~

~~SECRET//REL TO USA, FVEY~~

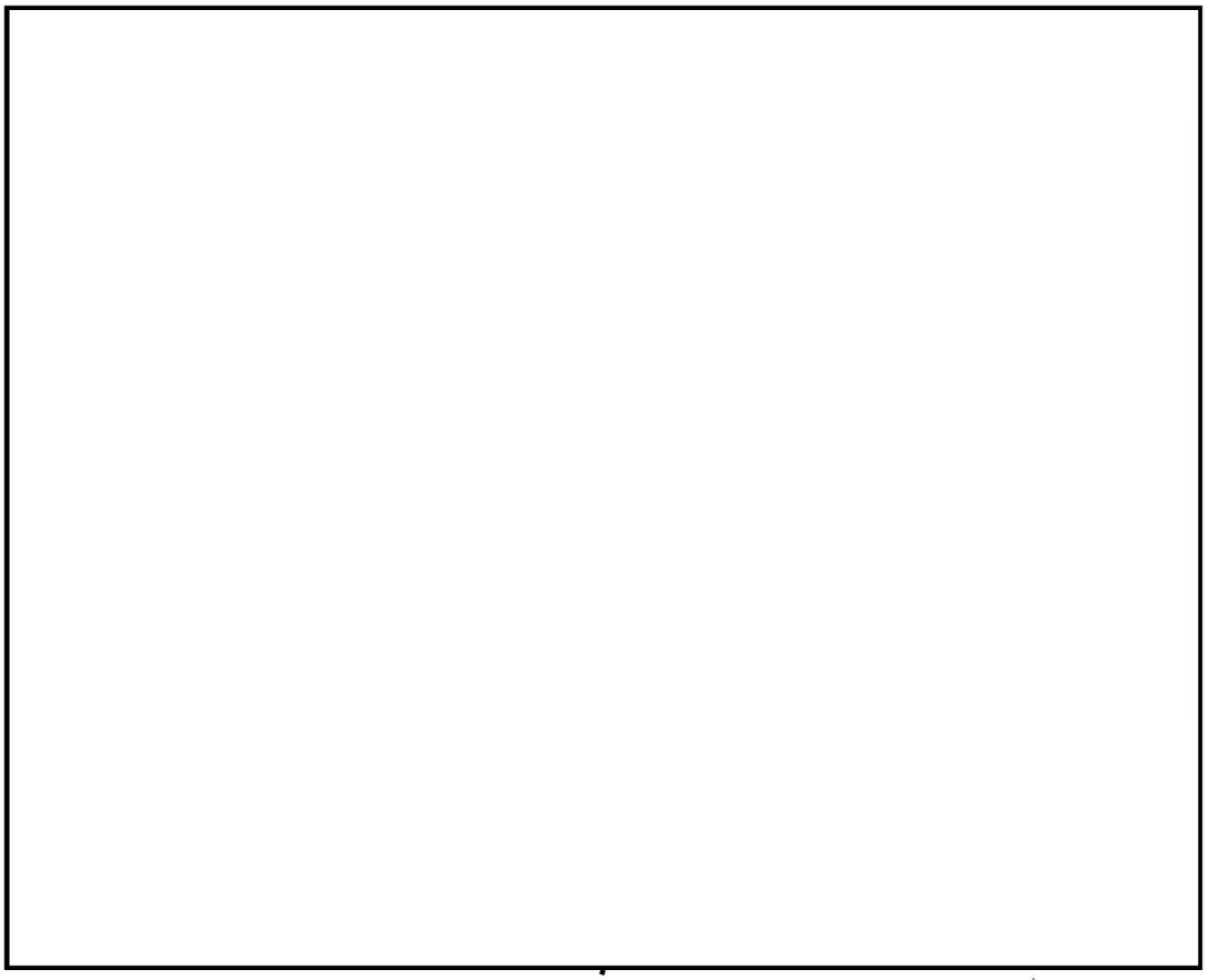


(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20390501

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

~~SECRET//REL TO USA, FVEY~~



~~(S//REL)~~ Recommendation: Recommend forwarding to the IG as user continues to engage in the same activity for which he was previously counseled.

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

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

Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20390501~~

~~SECRET//REL TO USA, FVEY~~

APPENDIX C

Email Correspondence

From: [redacted]
To: [redacted]
Cc:
Subject: RE: (U) Follow-up for Information
Date: Wednesday, May 20, 2015 8:22:16 AM

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

[redacted]

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

My branch chief at the time was [redacted] However, he was not involved, that I know of, in any aspect of this. My predecessor on that team was an Army Sergeant First Class that was retiring. When I came in as team lead, he had told me that was what he did with his account and that he had gotten the "go-ahead" for it. It was my choice to not question what I was told and just continue that process. The research aspect of which I was speaking had to do with [redacted] The Air Force/military aspect of it is quite simple. If you've ever worked with anyone in the military or been in the military yourself, you know that a lot of taskers get sent down to military personnel that have to be done on the low-side and, quite often, involve a CAC reader for log-in purposes. I cannot recall at any time [redacted] ever speaking to me about the allegation or the computer use and policy. I understand that you're trying to de-conflict and get as clear a picture as possible. However, it was nearly 6 years ago and I'm having a hard time recalling everything in detail. I'm not trying to be evasive, but I am also not trying to pass the buck to anyone else or start a "naming names" process, which this is starting to feel like. The onus is on me and me alone. If this is not sufficient information, please let me know. Thanks

[redacted]

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

From [redacted]
Sent: Tuesday, May 19, 2015 9:44 AM
To: [redacted]
Cc: [redacted]
Subject: RE: (U) Follow-up for Information

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]

Thanks for the quick response. I am not sure you need to continue looking for anything related to the 2009 allegation unless you believe there are any relevant emails. However, I still have a few questions. First, who was your supervisor at the time of the 2009 allegation

and did you have any discussions with him or her concerning either the sharing of your unclassified account or the OIG allegation?

Next, during our interview you stated that "we were given authorization for investigative purposes for our particular mission to allow other individuals to use that [your unclassified account/terminal]," while below you state "[t]he determination was made by me to allow them to use my account." Could you please elaborate as to the apparent distinctions between these statements? Finally, could you elaborate on your statement that the "purpose of the account use was for them to do research and AF/military requirements that required a CAC card reader?"

As with your previous testimony and email responses, this request is also voluntary.

R/

[redacted]

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

(U//~~FOUO~~)

[redacted]

Senior Investigator
NSA/CSS OIG, Office of Investigations, D14
[redacted]
963-0924(s) [redacted]

From: [redacted]
Sent: Thursday, May 14, 2015 1:51 PM
To [redacted]
Cc [redacted]
Subject: RE: (U) Follow-up for Information

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

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

[redacted]

I'm trying to remember but it has been some years. There were three individuals on my team that were Air Force. I'm trying to find old information but most of my emails and documents were purged in the move from [redacted] I know that one of the persons was a [redacted] I believe he has PCS'd. There was also a SSgt and a female SrA. I will try to find names for you if I can. There was no formal SOP for the account. As I believe I told you last week, I was responsible for the account. The purpose of the account use was for them to do research and AF/military requirements that required a CAC card reader. The determination was made by me to allow them to use my account as it was taking so long to get an account as it was and they each only had a few months left on the team. Following the incident, I spoke with them collectively and told them that, going forward, they would no longer be allowed to use the account. I did not elaborate as to why. I told them that, should they need to have something researched, I would do it for them. In the end, it was my account and I must take responsibility for anything and everything that happened on it.

I know that this probably isn't enough detail for you and I will do my best to try to find anything that can shed greater light. I just wanted to get you at least some form of answer as quickly as possible. Please let me know what else you need from me and I will do what I can to get it for you. Like I said in our meeting, I will be as helpful and forthcoming as I can be.

Thank you

(U//~~FOUO~~) **********

[redacted]

****

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

From: [redacted]
Sent: Thursday, May 14, 2015 1:23 PM
To: [redacted]
Cc: [redacted]
Subject: (U) Follow-up for Information

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

During our interview last week we discussed the notification my office sent you in 2009, as well as your written response, concerning computer misuse (accessing adult-oriented material - attached). In our discussions, you denied any wrongdoing as to the 2009 allegation, explaining that the respective unclassified account/terminal was shared within your office and that the misuse was attributable to other individuals. More specifically, you stated that you were the only member on your team that had an account, and that you were given authorization, for investigative research purposes to support [redacted] mission related to your Branch, to allow other individuals to use your unclassified account. Additionally, you conveyed to us that you told, in 2009 via phone conversations, all of the aforementioned information to the OIG, but were told that you were responsible as it was your account. Finally, in the context as to why the shared use aspect is not mentioned in your written 2009 reply to the OIG, you believe that your written response captured what you told the OIG (i.e., statements such as "I will be more careful about what I type into

search engines" equated to your intention to be more careful by ending the sharing of access to your unclassified account).

In an effort to ensure accuracy regarding both the 2009 scenario and the current issues, I would like you to please provide additional details about the 2009 incident. Please include additional detail as to the approval aspect of the 2009 sharing arrangement, your supervisor at that time in 2009, individuals you believe would be able to corroborate the information, including any related context (e.g., discussions you may have had with an individual concerning the sharing or team meetings explaining SOPs/expectations concerning the account, etc.). Any relevant emails would be helpful as well.

As with your previous testimony, this request is also voluntary. I am attempting to obtain this information via email, vice another interview, as a matter of convenience. However, please let me know if you would prefer to discuss in person and we will do so.

Finally, please let me know if you have any questions or think that any of the information in this email is inaccurate.

Thanks,

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

(U//~~FOUO~~) [redacted]
Senior Investigator
NSA/CSS OIG, Office of Investigations; D14
[redacted]
963-0924(s) [redacted]

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

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

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

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