NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

14 January 2014

IV-14-0002

Alleged Government Information System Misuse

This is a PRIVILEGED DOCUMENT. Further dissemination of this report outside of the Office of Inspector General, NSA, is PROHIBITED without the approval of the Assistant Inspector General for Investigations.

(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~~) This investigation was conducted in response to an allegation that [redacted] Q232, Associate Directorate for Security and Counterintelligence (ADS&CI), misused her accesses as a [redacted] to conduct an unauthorized search of [redacted]

(b)(6)

(U//~~FOUO~~) As part of her duties as a [redacted] is authorized to obtain credit bureau reports to assist in processing security clearances for contractors. Analysis of [redacted] credit bureau report search history revealed that on 18 September 2013, [redacted] obtained a credit report for [redacted] was not affiliated with NSA and obtaining her credit report was not authorized by ADS&CI. [redacted] testified that when she requested the credit report, she knew it was a misuse of her government information system. It was a "dumb" thing to do and she realized after the impulse that she might get caught and she would have to deal with the consequences if discovered. As (an ADS&CI) security employee, she knew her actions were inappropriate.

(U//~~FOUO~~) Further investigation revealed that on 29 August 2013, [redacted] attempted to use [redacted] to view her own online security jacket. The user guides and splash screen for the applications she used expressly prohibit self-searches. [redacted] testified that she did not know it was a violation of policy to review her own information. Furthermore, she did not think it was possible to see her own adjudicative criteria; she thought she would only be able to access the dates she was due for reinvestigation and polygraph as well as her start date, award dates, and promotion dates.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted]

1) misused her federal government communication system by querying a database for personal information pertaining to a family member in violation of 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property; Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities.

2) misused her position as a Security Information Specialist with access to government information systems to gather information about her family member for her own private gain in violation of 5 C.F.R. § 2635.702, Standards of Ethical Conduct for Employees of the Executive Branch, Use of Public Office for Private Gain.

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

3) misused her federal government communication system by querying a database for security information about herself in violation of 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property and Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities.

(U//~~FOUO~~) Copies of this report will be forwarded to MR, Employee Relations, for action deemed appropriate and D23, the Office of General Counsel (Administrative Law & Ethics) and ADS&CI, Q234 (Special Actions) for information.

II. (U) BACKGROUND

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

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

(U) Introduction

(U//~~FOUO~~) [redacted] has been a [redacted] in Q232, [redacted] processes clearances for contractors who [redacted]

(U//~~FOUO~~) On 30 September 2013, [redacted] contacted ADS&CI, Q2, Office of Personnel Security, regarding a notification she received from TransUnion credit bureau. According to the notification, [redacted] credit report was run on 18 September 2013 by the Maryland Procurement Office, Fort Meade, MD. Chief, Q2, subsequently referred the matter to the OIG for investigation.

(b)(6)

(U) Applicable Authorities

(U) The investigation considered possible violations of the following authorities. Full citations are contained in Appendix A.

- (U) 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property

- (U) 5 C.F.R. § 2635.702, Standards of Ethical Conduct for Employees of the Executive Branch, Use of Public Office for Private Gain

- (U) Joint Ethics Regulation, DoD Directive 5500.07-R, § 2-301, Use of Federal Government Resources

- (U//~~FOUO~~) NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities

III. (U) FINDINGS

(U//~~FOUO~~) **ALLEGATION 1**: *Did* [redacted] *Q232, use her federal government communication system for other than authorized purposes by querying a database for personal information pertaining to* [redacted] *in violation of 5 CFR §2635.704(a), Standards of Conduct for Employees of the Executive Branch, Use of Government Property; Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities?*

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

(U//~~FOUO~~) **ALLEGATION 2**: *Did* [redacted] *Q232, use her government position as a* [redacted] *for private gain by gathering personal information about* [redacted] *in violation of 5 CFR §2635.702, Standards of Conduct for Employees of the Executive Branch, Use of Public Office for Private Gain?*

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

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

(b) (6)

(U) Documentary Evidence

(U//~~FOUO~~) **Appendix B -** [redacted] **Credit Bureau Search History, 10/1/12-9/30/13**

(U//~~FOUO~~) On 18 September 2013, case requestor [redacted] obtained a TransUnion credit report for [redacted] Q209, verified that account [redacted] is assigned to [redacted] immediate supervisor, [redacted] Team Lead, [redacted] confirmed that [redacted] had no official justification or authorization to obtain [redacted] credit report. [redacted] verified that the remaining names queried by [redacted] had a legitimate contractor affiliation and were associated with ongoing clearance investigations.

(U//~~FOUO~~) **Appendix C – Credit Bureau Reports Web Login Screen**

(U//~~FOUO~~) When logging into the credit bureau reports website, users see the following banner, "Unauthorized access prohibited by law. Use of information from this website is governed by Federal and State Law. Illicit access or misuse may result in fines, imprisonment, or both."

(U//~~FOUO~~) [redacted] **Other Database Searches**

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

(U//~~FOUO~~) The OIG reviewed [redacted] requests for Local Agency Records[1] from 1 October 2013 – 30 September 2013. [redacted] verified that all of the records she requested were authorized.

(U//~~FOUO~~) The OIG also reviewed 6 months of [redacted] database searches. The OIG uncovered no evidence of misuse.

(U//~~FOUO~~) [redacted] use of the [redacted] application is discussed in allegation 3, below.

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

(U//~~FOUO~~) **Appendix D – Local Agency Record Request Form (SAMPLE)**

(U//~~FOUO~~) When conducting a Local Agency Record Request, which included requests for credit bureau reports, [redacted] digitally signed the request. The request contained the following statement, "I certify that this is an official request within the Investigative responsibilities of the Director, NSA as defined in DoD Directive 5100.23 (Administrative Arrangements for the National Security Agency). DCID 1/14 (Minimum Personnel Security Standards and Procedures Governing Eligibility for access to Sensitive Compartmented Information); and/or EO 12333 (United States Intelligence Activities."

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

(U) Testimonial Evidence

(U//~~FOUO~~) [redacted] (b)(6)

(U//~~FOUO~~) On 8 October 2013, [redacted] a civilian unaffiliated with NSA, was interviewed telephonically and provided the following testimony.

(U//~~FOUO~~) [redacted] received notifications from TransUnion, Equifax, and Experian credit bureaus that an inquiry about her credit was made in connection with an employment background investigation. [redacted] has not applied for a new job in seven years and has never applied for employment with NSA.

(U//~~FOUO~~) According to the notification, the credit inquiry was from the CBR Department of Defense. When she called the contact number listed on the notification, she learned that her credit report was obtained by the Maryland Procurement Office.

(U//~~FOUO~~) Because [redacted] has no affiliation with NSA and has not sought employment in many years, she speculated that [redacted] may have

---

[1] (U//~~FOUO~~) Local Agency Records may include Maryland State Police records, Motor Vehicle Administration Records, Credit Bureau Reports, and National Crime Information Center Records.

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

had something to do with the credit inquiry. [redacted] works in [redacted] at NSA. [redacted] considered the possibility that it was an accident having to do with [redacted] own reinvestigation, but thought it unlikely since they don't share first or middle names. She thought it more likely that [redacted] did it intentionally.

(U//~~FOUO~~) When asked what [redacted] motive might be, [redacted] said she did not know. She was reticent to provide more information, but alluded to [redacted] She said perhaps [redacted] did it to "check up on me."

(U//~~FOUO~~) When asked if [redacted] had a history of such behavior, she said [redacted]

As far as she knew, none of [redacted] previous intrusions had anything to do with her employment at NSA.

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

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

(U//~~FOUO~~) On 9 October 2013, [redacted] Q232, was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) To gather information for processing clearances, [redacted] stated she used the following tools for the following purposes:

1) [redacted]
2) MD Judiciary Search – To search for Maryland court case records related to local applicants.
3) CBR Credit Reports – To review an applicant's credit history.
4) Local Agency Checks – To review Motor Vehicle Administration Records, state police records, and National Crime Information Center records.
5) [redacted]
6) [redacted]
7) People Soft[4] – To verify an individual's employment status.

(b) (6)

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

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

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

[4] (U//~~FOUO~~) PeopleSoft is the NSA record of clearance processing information. It may be used to validate a person's employment with NSA only.

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

(U//~~FOUO~~) A couple of weeks ago, [redacted] obtained [redacted] credit report using her NSA accesses. Immediately after reviewing the credit report, [redacted] realized she had been "stupid" and knew it was prohibited. [redacted] She doesn't even remember printing the results; if she did, she destroyed them. When [redacted] ran [redacted] credit, she thought the credit report would show if [redacted]

(U//~~FOUO~~) When [redacted] pulled the credit report, she knew it was a misuse of her government information system. She was also aware that her activity could be monitored. It was just a "dumb" thing to do and she realized after the impulse that she might get caught and she would have to deal with the consequences if discovered. Being in ADS&CI, she knew her actions were inappropriate. She was not permitted to run searches on anyone except the subject of an investigation. Additionally, [redacted] puts a cover memo on her reports that contains a warning about potential misuse of the information.

(b) (6)

(U//~~FOUO~~) [redacted] also admitted to using her NSA unclassified computer to conduct MD judiciary searches on [redacted] From time to time, while looking up a subject on the MD judiciary website, she would check on [redacted] She did not consider this to be misuse since it is a public website that anyone can access from home. No special accesses were required for her to look up that information.

(U//~~FOUO~~) [redacted] stated that outside of the one-time check of [redacted] credit, she has never checked the credit of anyone not under investigation. She never conducted local agency checks on anyone but subjects under investigation. She never submitted any personal [redacted] requests. [redacted] emphasized that she has been a good employee for [redacted] years and has never previously been in trouble. She is proud to work for NSA and not being able to do her job anymore bothers her a great deal.

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

(U) Analysis and Conclusions

(U//~~FOUO~~) The following regulations restrict federal employees' use of federal property to authorized purposes only:

- 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property states that, "An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes."

- Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources states that, "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…"

- NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities states that, NSA/CSS information system (IS) users shall, "Use ISs for official government and/or mission-related purposes."

(U//~~FOUO~~) On 18 September 2013, [redacted] used her government information system for other than authorized purposes, in violation of the above regulations. She queried a database for and obtained a credit report concerning [redacted] According to [redacted] immediate supervisor, [redacted] Team Lead, [redacted] had no official justification or authorization to obtain [redacted] credit report; [redacted] testified that she acquired the report for personal reasons.

(b) (6)

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

(U//~~FOUO~~) 5 CFR §2635.702, Standards of Conduct for Employees of the Executive Branch, Use of Public Office for Private Gain states that, "An employee shall not use his public office for his own private gain…." When [redacted] obtained a credit report concerning [redacted] she misused her position. [redacted] testified that [redacted] By virtue of her position as a [redacted] had unique accesses to personal information (including financial, criminal, and other identifying information) that she could not have obtained by other means. Therefore, she used the position and the accesses she had been entrusted with for her own private gain in violation of this regulation.

(U//~~FOUO~~) [redacted] was familiar with the rules prohibiting unauthorized use of NSA information systems, as evidenced by her frequent use and certification of the Local Agency Request Form. [redacted] testified that she knew obtaining [redacted] credit report was a misuse of her government information system. She further stated that she was not permitted to run searches on anyone except the subject of investigation. [redacted] characterized the incident as "dumb" and "stupid" and emphasized that it was a one-time mistake.

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted]

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

1) misused her federal government communication system by querying a database for personal information pertaining to a family member in violation of 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property; Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities.

2) misused her position as a Security Information Specialist with access to government information systems to gather information about her family member for her own private gain in violation of 5 C.F.R. § 2635.702, Standards of Ethical Conduct for Employees of the Executive Branch, Use of Public Office for Private Gain.

(U//~~FOUO~~) ***ALLEGATION 3**: Did [redacted] Q232, misuse her federal government communication system by querying a database for security information about herself in violation of 5 CFR §2635.704(a), Standards of Conduct for Employees of the Executive Branch, Use of Government Property and Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resource?*

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

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

(U) Documentary Evidence

(U//~~FOUO~~) **Appendix E - [redacted] Search History, 29 August 2013**

(U//~~FOUO~~) Audit records for [redacted] use of the [redacted] (also known as [redacted][5] and [redacted] applications from 1 January 2013 – 21 October 2013, shows [redacted] used both applications during the time period.

(U//~~FOUO~~) On 29 August 2013, at 1351, [redacted] used the [redacted] application to search her own name (Appendix E). She was unable to retrieve any data in her security jacket.

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

---

[5] (U//~~FOUO~~) [redacted] application used to view online security jackets. [redacted]

[6] (U//~~FOUO~~) [redacted] application used to perform federated searches of any [redacted] data source for which the user has been granted access. [redacted] pulls data from the [redacted]

(U//~~FOUO~~) **Appendix F – [redacted] Splash Page**

(U//~~FOUO~~) Upon logging into the [redacted] application, the user must consent to the following conditions (by toggling the "I agree" button) before proceeding. "In accordance with ADS&CI Policy, [redacted] has an active auditing program in effect. By accessing [redacted] or the ADS&CI network, you are consenting to the auditing of your actions while using the application and network resources. Information in this system may not be shared without prior approval of ADS&CI management. You are NOT permitted to perform unauthorized searches. Example: ADS&CI personnel, Yourself, Celebrities, Politicians, Recent personalities in the news."

(U//~~FOUO~~) **Appendix G – [redacted] User Guide**

(U//~~FOUO~~) The Foreword of the [redacted] User Guide reads, "The use of this application constitutes consent to monitoring by [redacted] All activity is logged and reviewed. You are NOT permitted to perform unauthorized searches for: ADS&CI personnel, Yourself, Celebrities, Politicians, and Recent personalities in the news."

(U//~~FOUO~~) **Appendix H – [redacted] User Guide**

(U//~~FOUO~~) The Foreword of the [redacted] User Guide reads, "The use of this application constitutes consent to monitoring by [redacted] All activity is logged and reviewed. You are NOT permitted to perform unauthorized searches for: ADS&CI personnel, Yourself or others you know, Celebrities, Politicians, and Recent personalities in the news."

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

(U//~~FOUO~~) **Appendix I – [redacted] User Agreement**

(U//~~FOUO~~) On 15 September 2011, [redacted] signed the [redacted] User Agreement. By signing the document, she agreed to abide the provisions of the agreement. The agreement reads in part, "I understand that I may only perform searches of [redacted] data in support of my official duties. I further understand that unauthorized searches of any information contained in the [redacted] are in violation of this agreement. Unauthorized searches include queries about me, as well as any affiliate or non-affiliate for which an official purpose does not exist…."

(U) Testimonial Evidence

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

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

(U//~~FOUO~~) On 30 October 2013, [redacted] Q232, was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) used the when she was detailed there from approximately until the end of While detailed to she received her taskings for searches[7] from

(U//~~FOUO~~) When asked whether she had ever attempted to view her own security profile using initially denied it. However, when asked whether she had ever queried her own name while running the names of the individuals undergoing reinvestigation, she stated that she thought she had. "But I've never been told you can't look at your own stuff." She claimed she did not know it was a violation of policy to review her own information. Furthermore, she did not think it was possible to see her own adjudicative criteria. had firewalls that restricted one from seeing one's own security information. When asked why she attempted to view it if she knew it would blocked, she said she thought she could see the dates when she was due for reinvestigation and polygraph as well as her start date, award dates, and when she got promotions.

(U//~~FOUO~~) only queried names directly off of the list that was faxed to her from She never used the to query anyone who was not undergoing investigation. iteiterated that the only time she ever intentionally ran a search on someone she was not supposed to was credit report.

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

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

(U) Analysis and Conclusions

(U//~~FOUO~~) On 29 August 2013, used the government information system, via the in an unsuccessful attempt to retrieve information about herself. As noted previously, 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property; Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities prohibit the use of federal property for unauthorized or unofficial purposes. had no official purposes for querying her own security portfolio. She testified she was merely seeking her dates of adjudication and polygraph.

(U//~~FOUO~~) testified that she did not know it was a violation of policy to review her own information. She also stated that she did not believe the database would permit her to view any information she was not allowed to see. However, on 15 September 2011, signed the User Agreement, which informed users that queries about oneself are unauthorized. Additionally, the user guides and splash screen for the applications expressly prohibit self-searches. Regardless of the results she believed the application would return, the search itself was prohibited.

[7] (U//~~FOUO~~) When stated she ran searches, she was technically using the and applications by means of the

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused her federal government communication system by querying a database for security information about herself in violation of 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property and Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities.

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

IV. (U) RESPONSE TO TENTATIVE CONCLUSIONS

(U//~~FOUO~~) On 29 December 2013, [redacted] responded to the tentative conclusions reached in the investigation. [redacted] accepted full responsibility for querying [redacted] credit report without authorization. However, she maintained that she did so without "private gain."

(U//~~FOUO~~) [redacted] also wrote that she never used a [redacted] application to view her online security jacket. She stated that the program she used was in PeopleSoft. However, audit records indicate that [redacted] used the [redacted] application in an unsuccessful attempt to retrieve information about herself on 29 August 2013. [redacted] accessed [redacted] via the [redacted] the user interface that allows users to access applications for searching data.

(b) (6)

(U//~~FOUO~~) As [redacted] provided no new information that would impact the OIG analysis, the tentative conclusions became final.

(U//~~FOUO~~) A copy of [redacted] response is in Appendix J.

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

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

V. (U) CONCLUSION

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

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted]

1) misused her federal government communication system by querying a database for personal information pertaining to [redacted] in violation of 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property; Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities.

2) misused her position as a Security Information Specialist with access to government information systems to gather information about [redacted] for her own private gain in violation of 5 C.F.R. § 2635.702, Standards of Ethical Conduct for Employees of the Executive Branch, Use of Public Office for Private Gain.

3) misused her federal government communication system by querying a database for security information about herself in violation of 5 C.F.R. § 2635.704(a), Standards of Ethical Conduct for Employees of the Executive Branch, Use of Government Property and Joint Ethics Regulation, DoD Directive 5500.07-R, §2-301, Use of Federal Government Resources; and NSA/CSS Policy Manual 6-3, Chapter Two, Information System User and Supervisor Responsibilities.

(b)(6)

VI. (U) DISTRIBUTION OF RESULTS

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

1. M/ER for information and any appropriate action.
2. OGC, Administrative Law & Ethics, D23, for information, and;
3. Q234, Special Actions, for information and any appropriate action.

[redacted]
Investigator

Concurred by:

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

[redacted]
Assistant Inspector General
for
Investigations

APPENDIX A

(U) Applicable Authorities

(U) 5 C.F.R. § 2635.704, Standards of Ethical Conduct for Employees of the Executive Branch, - *Use of Government Property*

(a) Standard. An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes.

(b) Definitions. For purposes of this section:

(1) Government property.... The term includes office supplies, telephone and other telecommunications equipment and services, the Government mails, automated data processing capabilities, printing, and reproduction facilities, Government records, and Government vehicles.

(2) Authorized purposes are those purposes for which Government property is made available to members of the public or those purposes authorized in accordance with law or regulation.

(U) 5 C.F.R. § 2635.702, Standards of Ethical Conduct for Employees of the Executive Branch, - *Use of Public Office for Private Gain*

An employee shall not use his public office for his own private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or persons with whom the employee is affiliated in a nongovernmental capacity, including nonprofit organizations of which the employee is an officer or member, and persons with whom the employee has or seeks employment or business relations. The specific prohibitions set forth in paragraphs (a) through (d) of this section apply to this general standard, but are not intended to be exclusive or to limit the application of this section.

(U) The Joint Ethics Regulation (JER), DoD Directive 5500.07-R, Chapter 2: Standards of Ethical Conduct

Section 3. DoD Guidance

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…

b. Other Federal Government Resources…. Federal Government resources, including personnel, equipment, and property, shall be used by DoD employees for official purposes only….

(U) NSA/CSS Policy Manual 6-3, Chapter Two – *Information System User and Supervisor Responsibilities*

3. (U//~~FOUO~~) All NSA/CSS IS users shall:

b. (U) Use ISs for official government and/or mission-related purposes….

APPENDIX B

(U) [redacted] Credit Bureau Search History

10/1/12-9/30/13

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

Lawson #	Case Id	Consumer Name	Case Requestor	Order Date	Rebill Type Desc	Units	Billing Amt	Credit Amt	Net Amt

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

UNCLASSIFIED

UNCLASSIFIED

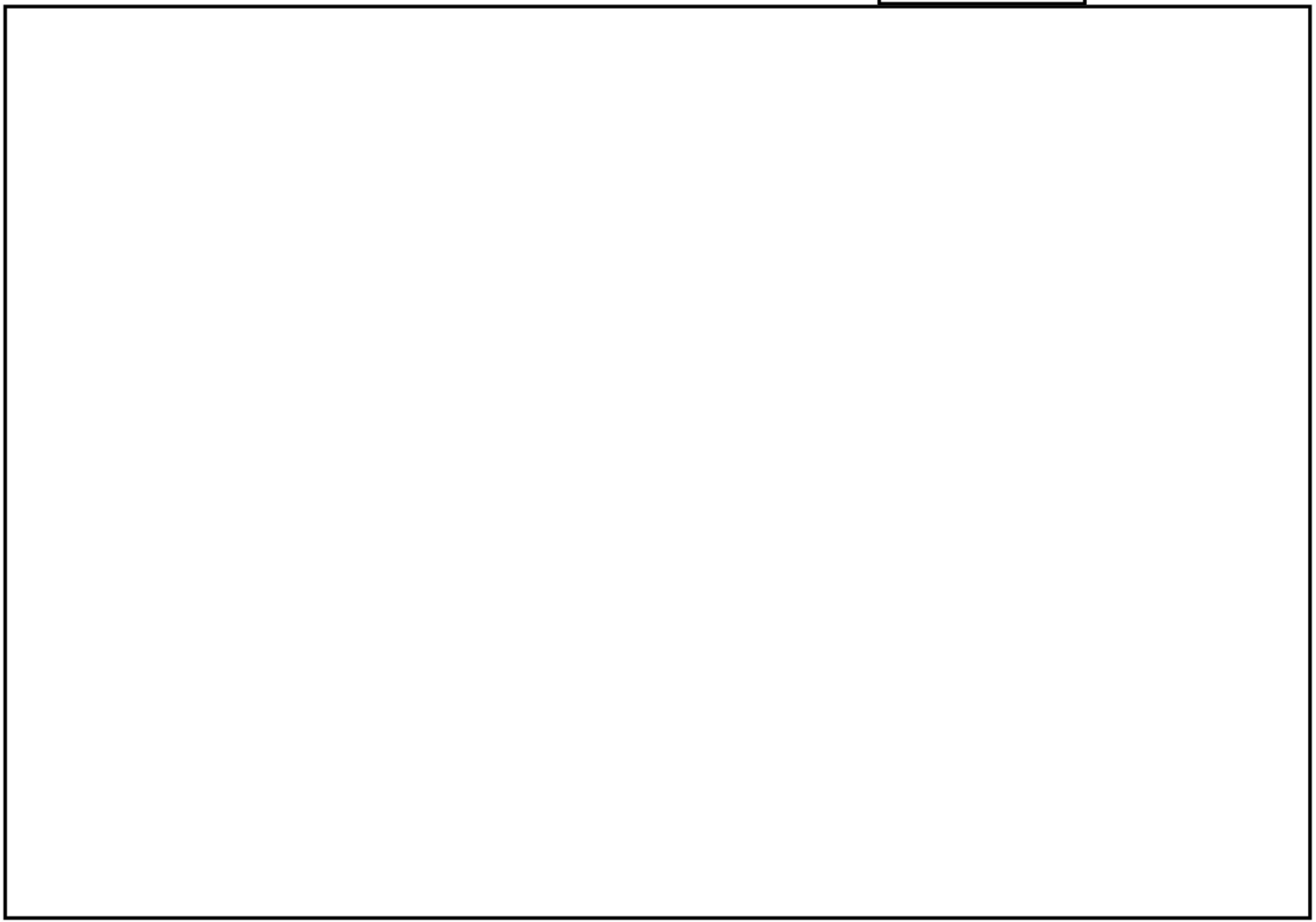
(b)(3)-P.L. 86-36
(b)(6)

UNCLASSIFIED

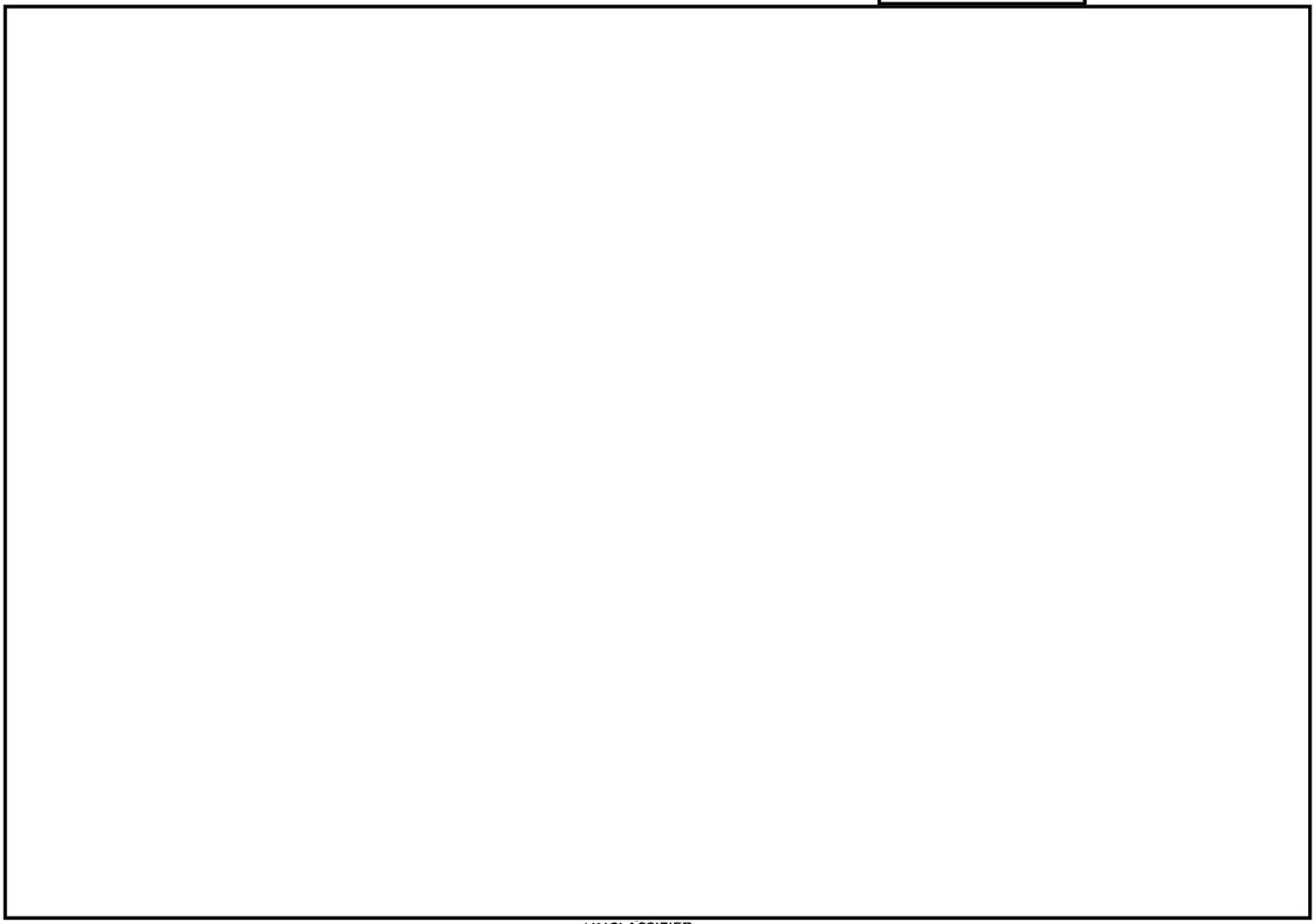
UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED



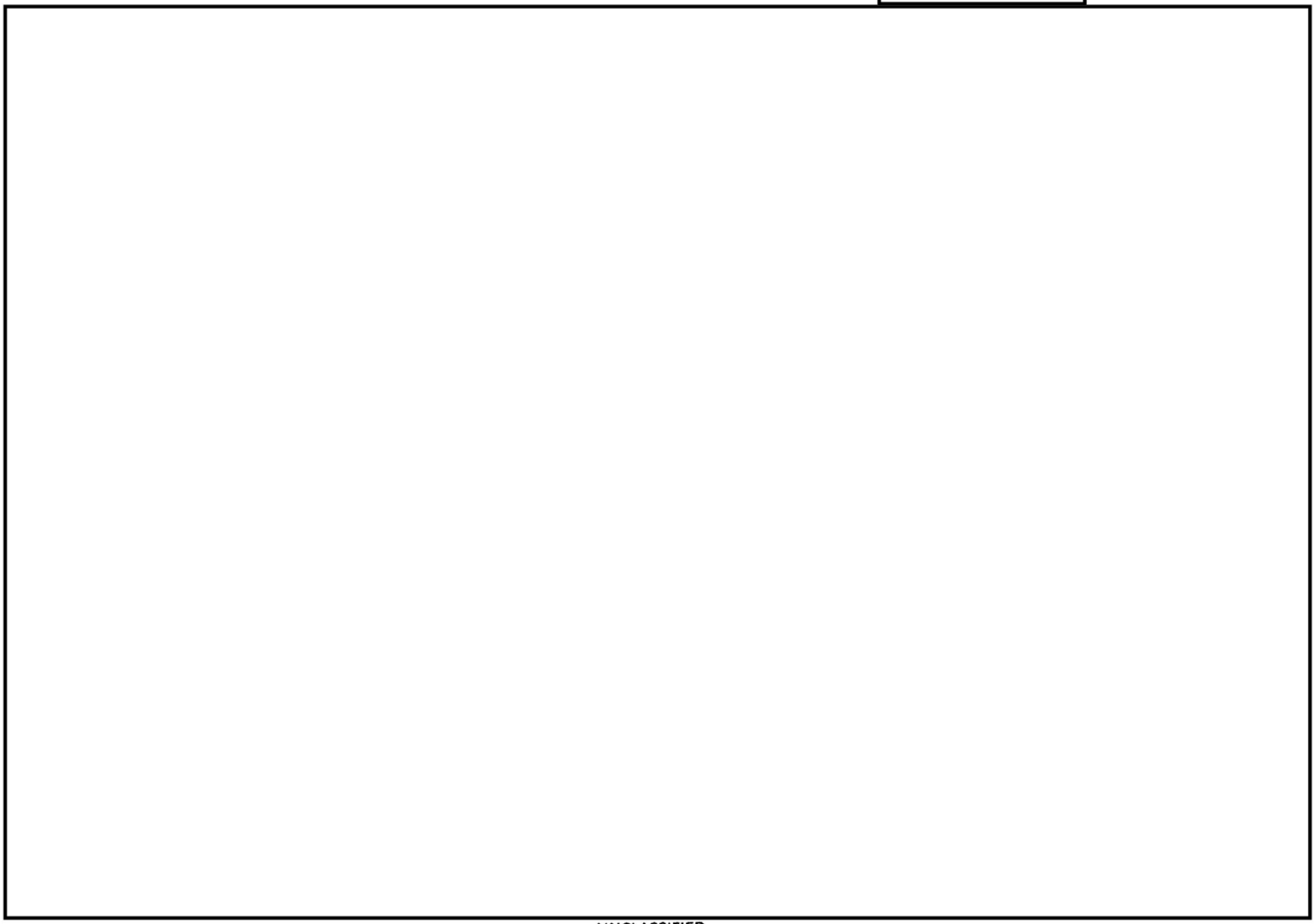
(b)(3)-P.L. 86-36
(b)(6)

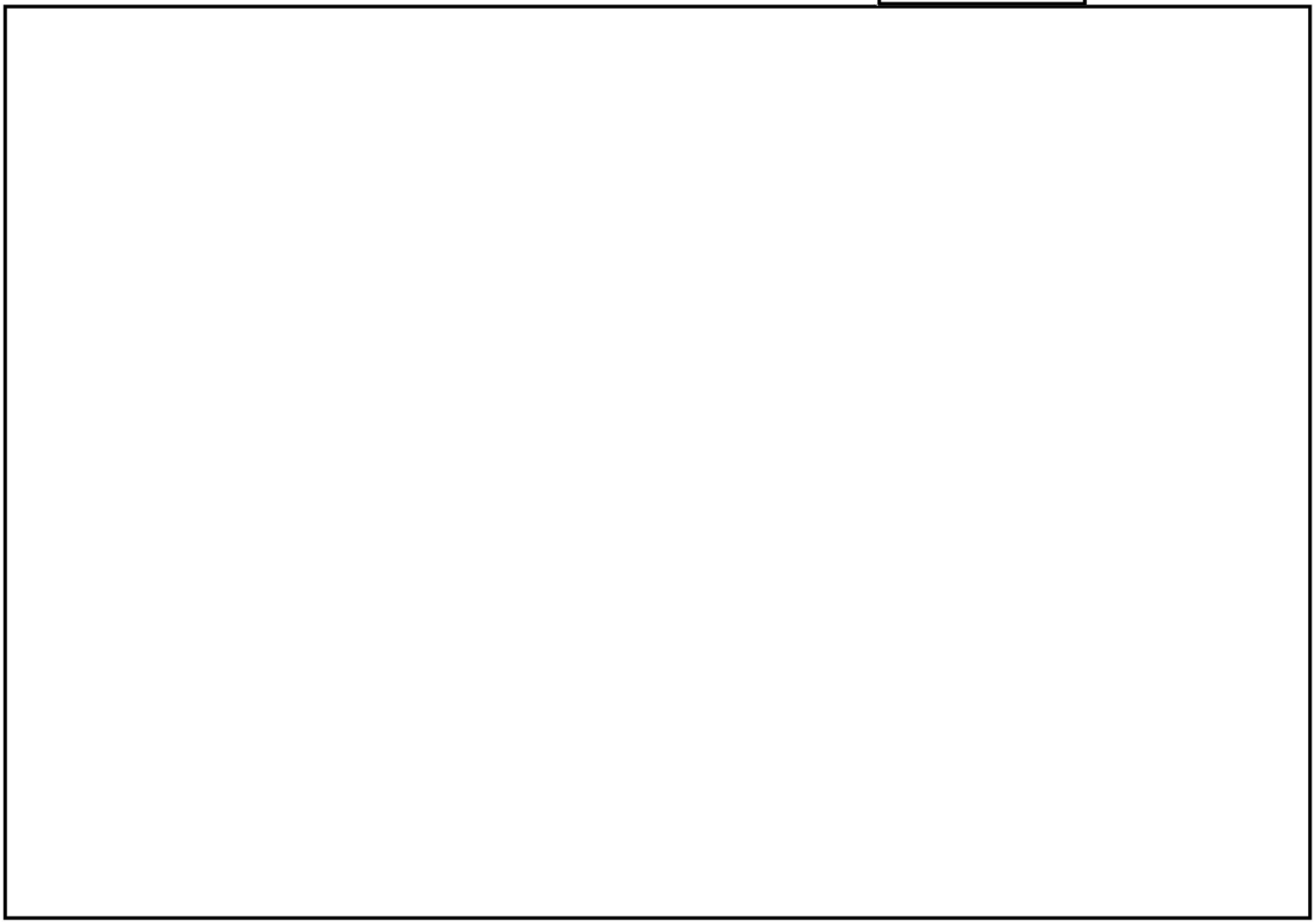


UNCLASSIFIED

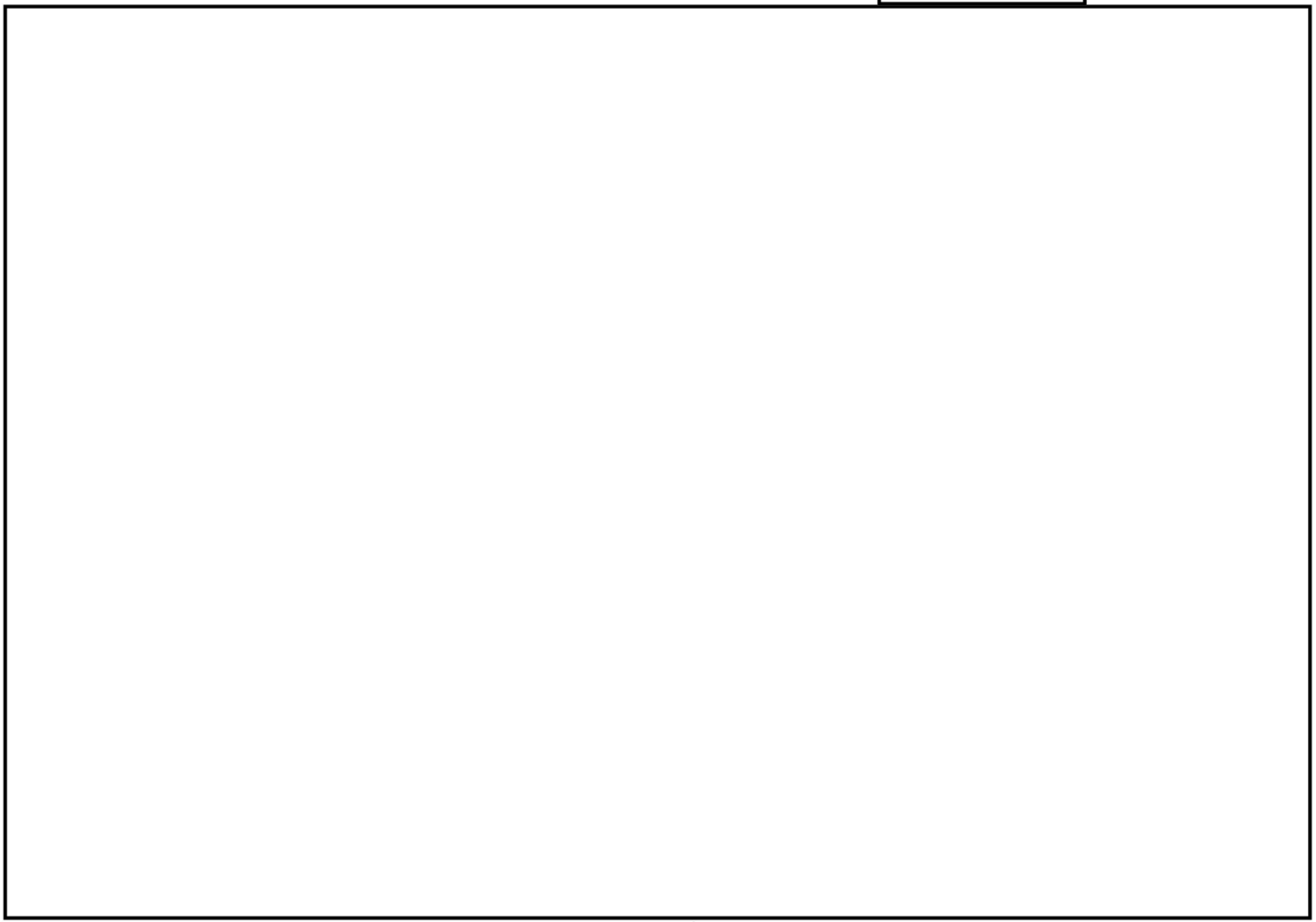
UNCLASSIFIED

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



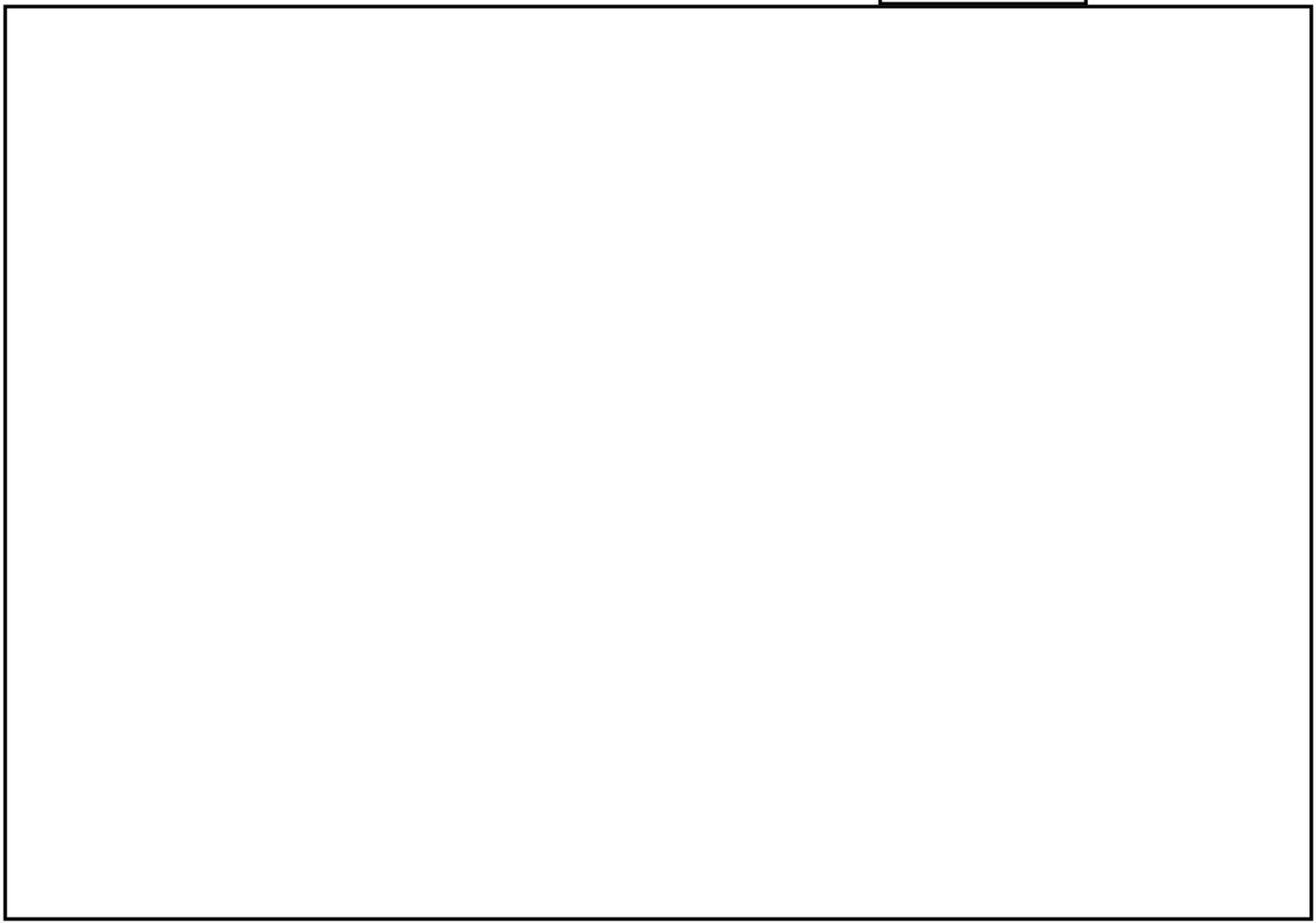


(b)(3)-P.L. 86-36
(b)(6)



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

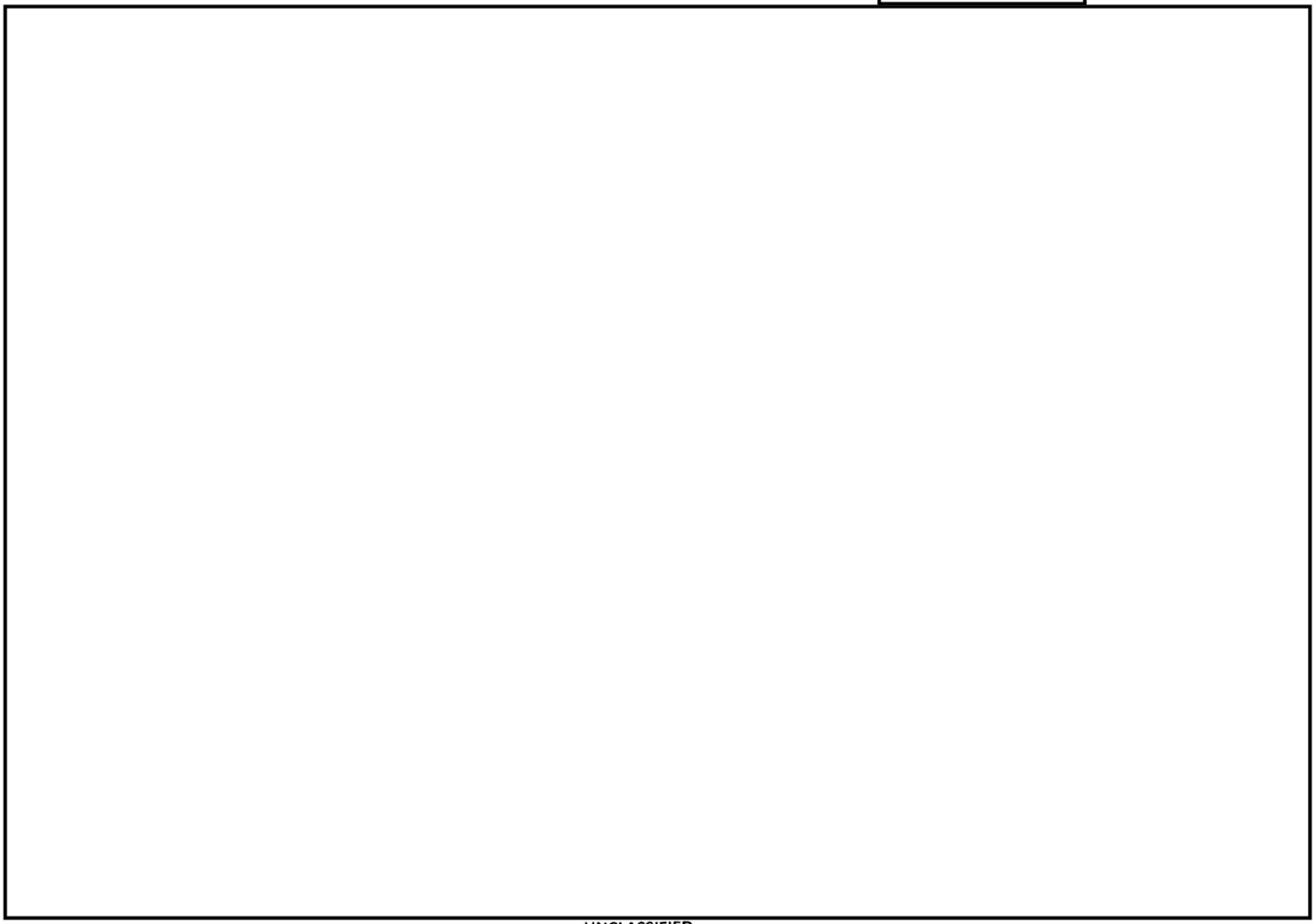
(b)(3)-P.L. 86-36
(b)(6)



UNCLASSIFIED

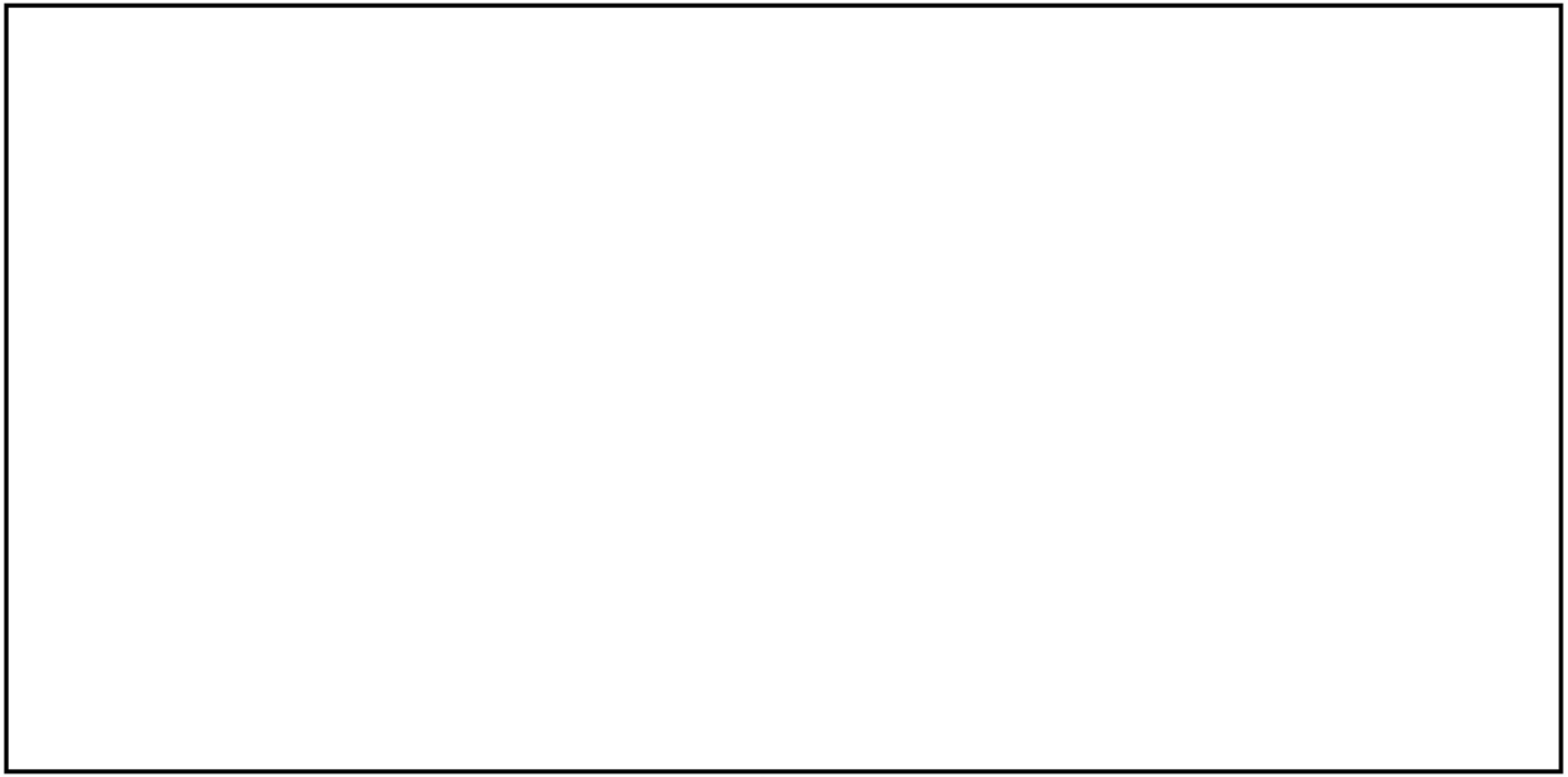
UNCLASSIFIED

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



UNCLASSIFIED

UNCLASSIFIED



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

APPENDIX C

(U) Credit Bureau Reports Web Login Screen

(b)(3)-P.L. 86-36
(b)(4)

APPENDIX D

(U) Local Agency Record Request Form (Sample)

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

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

APPENDIX E

(U) [redacted] Search History

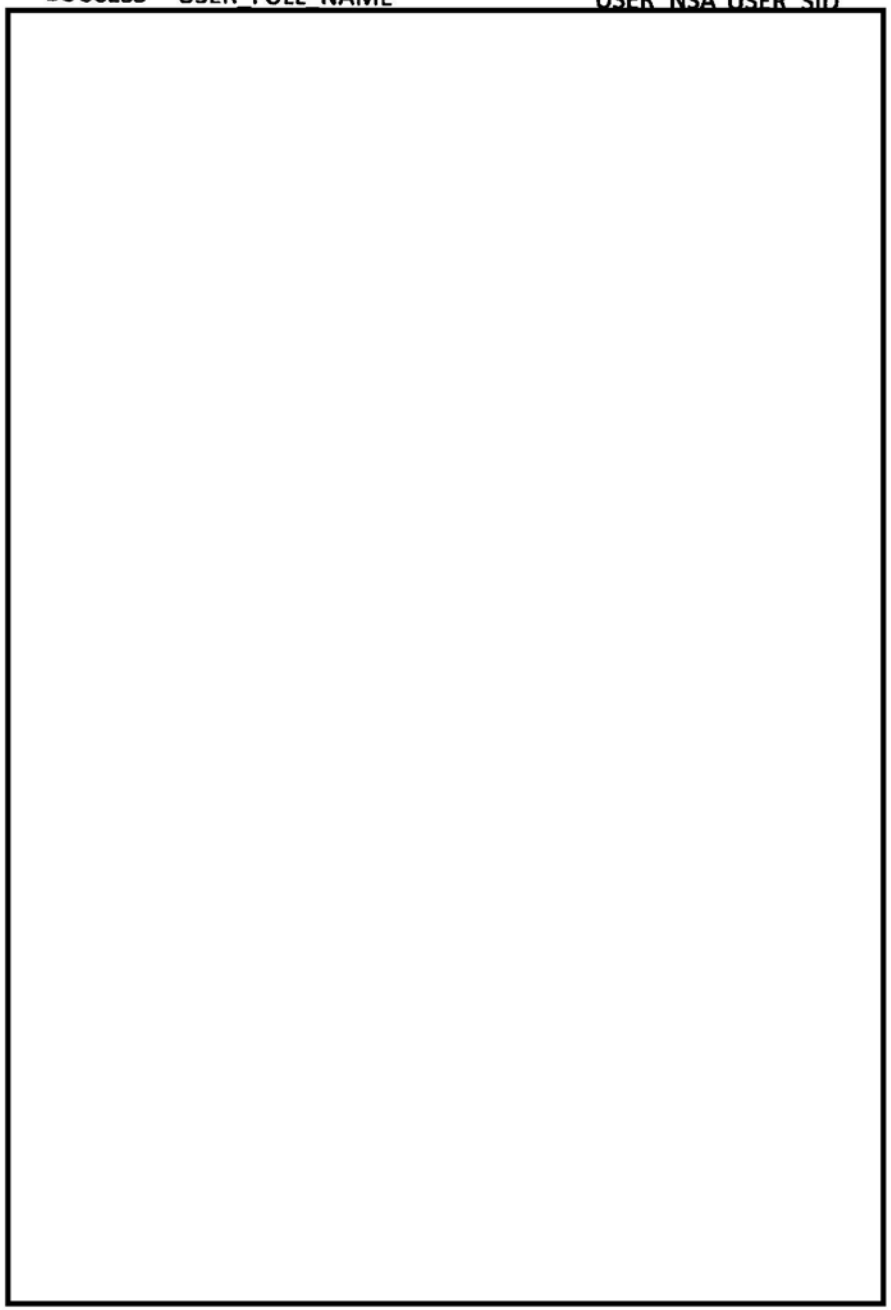
29 August 2013

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

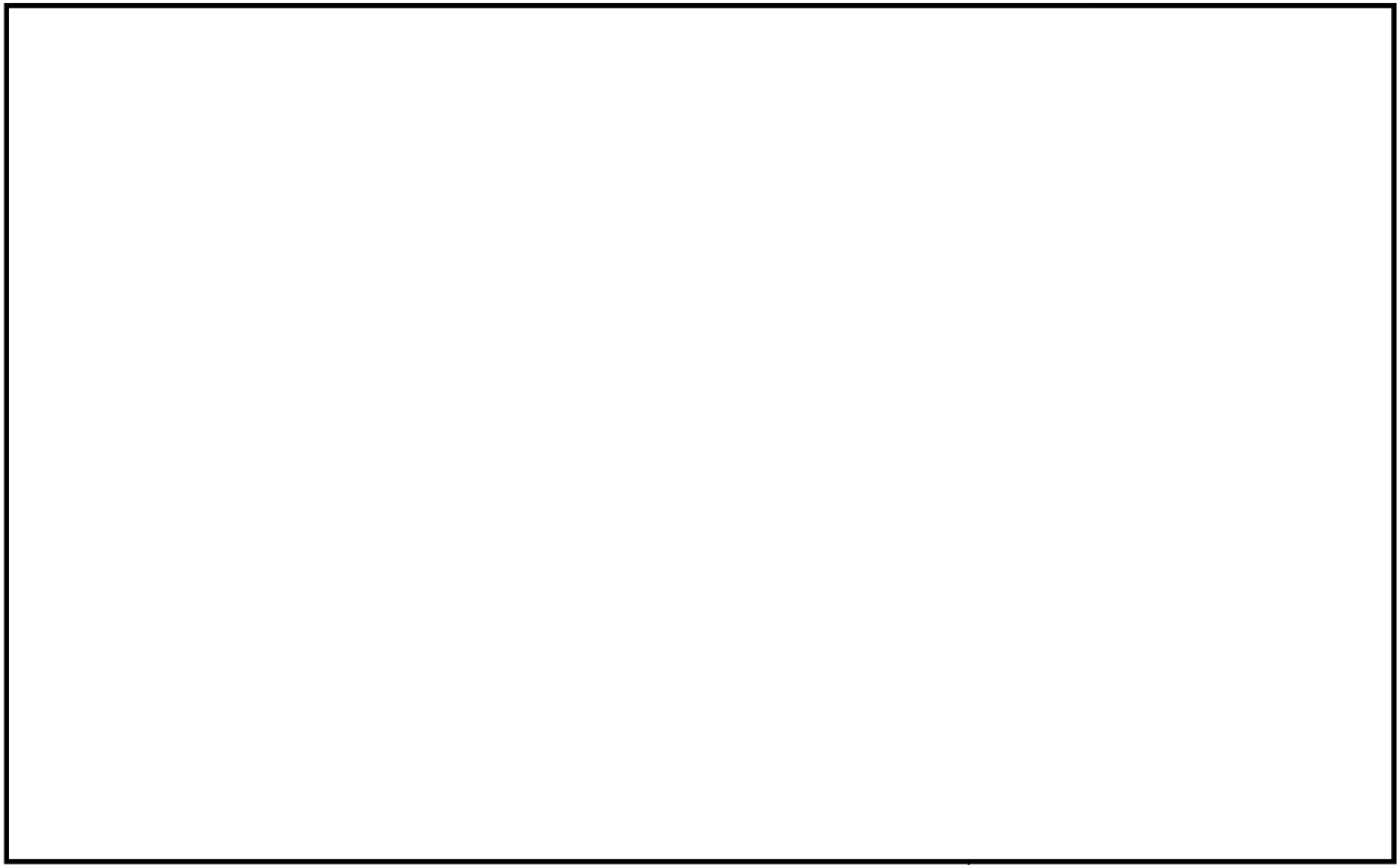
AUDIT_EVENT_ID	EVENT_DATE	EVENT_TEXT	EVENT_TYPE	SOURCE	SUBJECT_NAME	SUBJECT_I

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

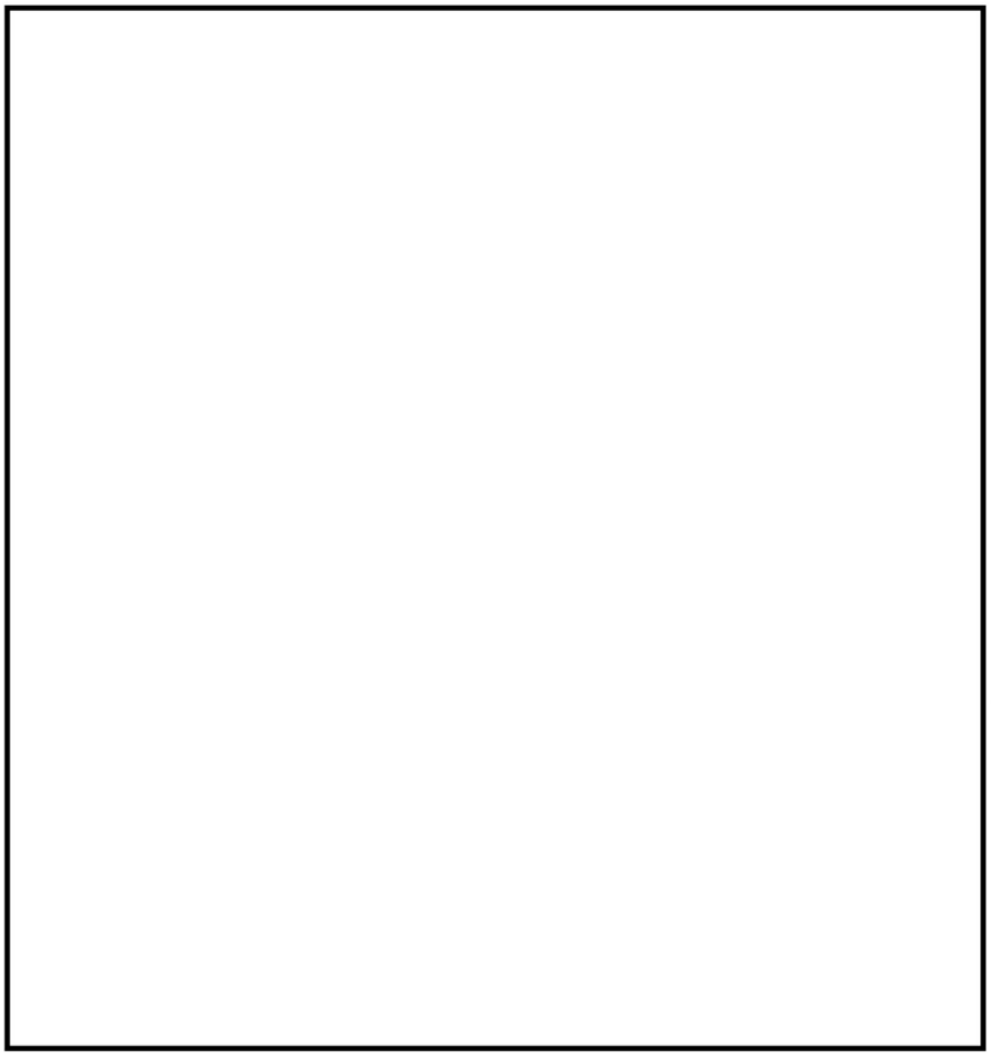
SUCCESS USER_FULL_NAME USER_NSA_USER_SID



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



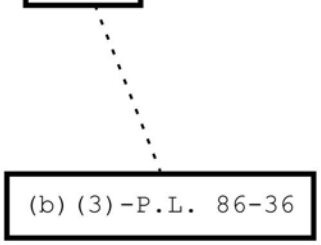
(b)(3)-P.L. 86-36
(b)(6)

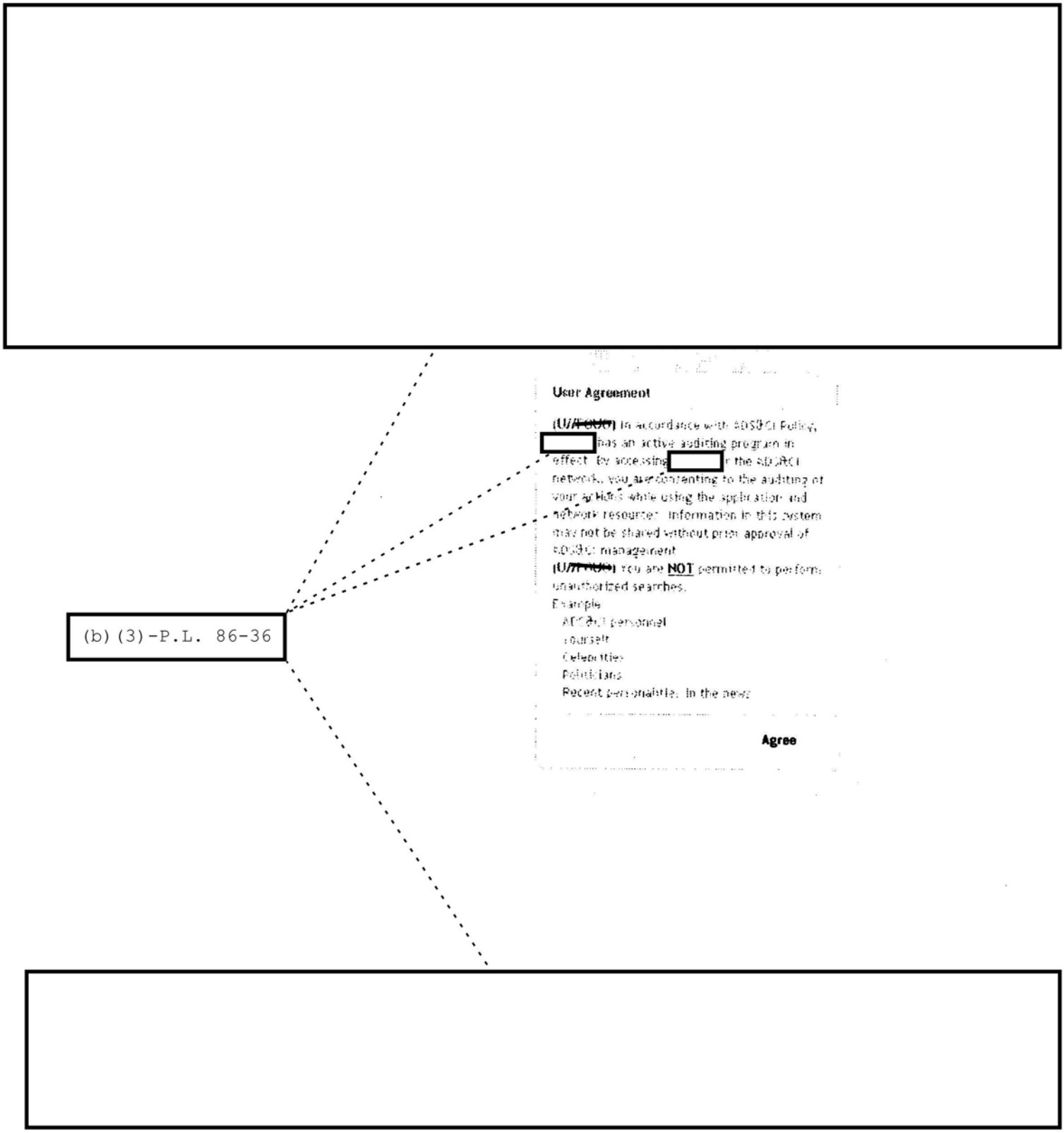


(b)(3)-P.L. 86-36
(b)(6)

APPENDIX F

(U) [redacted] Splash Page

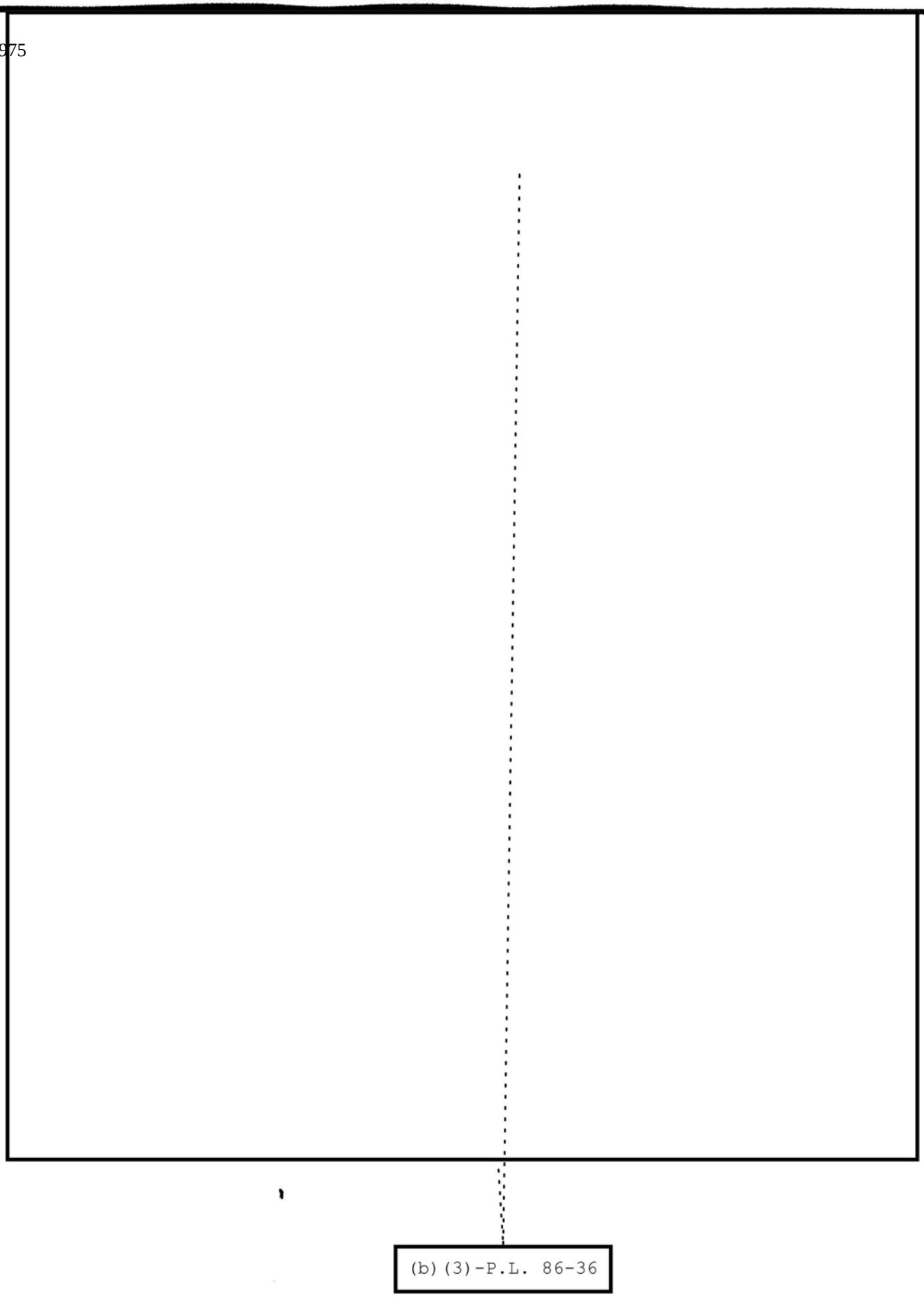



User Agreement
(U/FOUO) In accordance with SOSO CI Policy, has an active auditing program in effect. By accessing the SOCAC network, you are consenting to the auditing of your activities while using the application and network resources. Information in this system may not be shared without prior approval of SOSO CI management.
(U/FOUO) You are NOT permitted to perform unauthorized searches.
Example
SOCAC personnel
Yourself
Celebrities
Politicians
Recent personalities in the news
Agree
(b)(3)-P.L. 86-36

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

APPENDIX G

(U) [redacted] User Guide



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

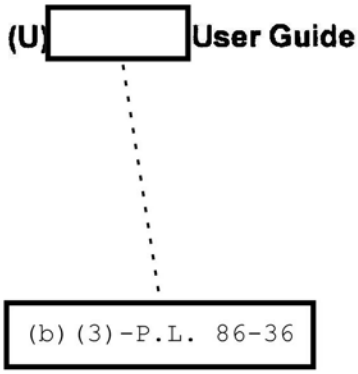
(b)(3)-P.L. 86-36

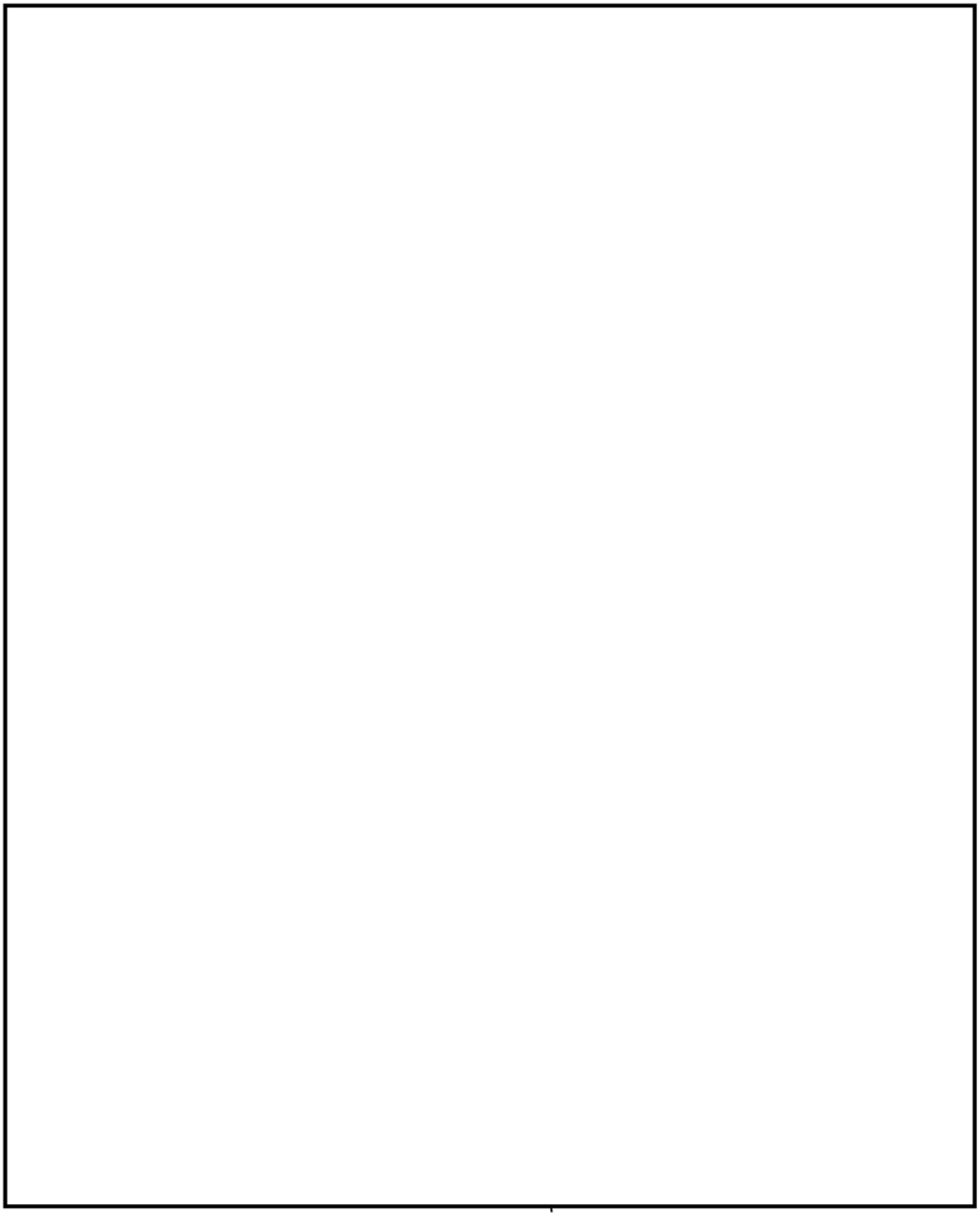
(b)(3)-P.L. 86-36

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

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

APPENDIX H





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

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

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

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

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

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

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

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

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

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

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

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

APPENDIX I

(U) [redacted] User Agreement

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

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

(U) [redacted] User Agreement

(U//~~FOUO~~) As part of my duties at NSA which will include access to sensitive data stored in the [redacted] I agree that I will be governed by and I will comply with the provisions of this user agreement.

1. (U//~~FOUO~~) I will abide by the guidance of this agreement as a condition of being given a computer account for the [redacted] data, in the context of this agreement, means the information contained in the [redacted] This includes personnel security information, intelligence community reporting, and other data supporting [redacted] operations.

2. (U//~~FOUO~~) I understand that Federal Law, including the Privacy Act of 1974 (5 U.S.C. § 552a), and other applicable statutes, regulations issued by the Attorney General, and orders and/or directives of the President of the United States, prohibit the loss, misuse, and/or unauthorized disclosure of the kinds of data used in the [redacted]

3. (U//~~FOUO~~) I understand that unauthorized disclosure of [redacted] data could result in impairment of national security; place human life in jeopardy; result in denial of due process to a person or persons who are subjects of an investigation; or prevent the NSA or other agencies from discharging their responsibilities.

4. (U//~~FOUO~~) I agree that I will not divulge, publish, reproduce, or provide any [redacted] data in any form to any unauthorized recipient. Unauthorized recipients include anyone outside ADS&CI. Authorized release outside of ADS&CI requires Q32 approval. Q32 will coordinate for release with data owners as necessary. For example, Q2 [redacted]

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

5. (U//~~FOUO~~) I understand that I may only perform searches of [redacted] data in support of my official duties. I further understand that unauthorized searches of any information contained in the [redacted] are in violation of this agreement. Unauthorized searches include queries about me, as well as any affiliate or non-affiliate for which an official purpose does not exist. DOD 5240.1-R, "Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons", provides more information on this topic. I understand that user actions in the [redacted] are reviewed and audited regularly by [redacted] and by my own management chain, as appropriate, to ensure compliance with this user agreement.

6. (U//~~FOUO~~) I understand that the [redacted] is only to be used to support my official duties. Such access does not give me the authority to make decisions outside of my assigned duties. I understand that clearance adjudication and all personnel security actions are the purview of the Office of Personnel Security (Q2). [redacted] Questions on authorities must always be resolved by coordination with the appropriate ADS&CI office or by contacting [redacted] for assistance. Failure to coordinate with the proper authorities in these matters is considered a violation of this agreement.

7. (U//~~FOUO~~) I understand that any violation of this agreement may result in the cancellation of my account, adverse and/or disciplinary personnel action(s), clearance suspension and/or revocation, and/or employment termination. In addition, I understand that any unauthorized disclosure of information by me may constitute a violation or violations of the United States criminal laws, including but not limited to Title 18, United States Code, or may lead to criminal prosecution for obstruction of lawful government functions.

(U//~~FOUO~~) I accept the above provisions as conditions of my access to the [redacted] and the sensitive data contained therein. I agree to comply with these provisions both during my assignments which provide me access to this data and at all times thereafter. I have read this agreement carefully and my questions, if any, have been answered.

Name:	Signature:	Date:
		15 Sept. 2011

Version 3 - 23 Feb 2011

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

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

APPENDIX J

[redacted] Response to the OIG's 12 December 2013 Notification of Tentative Conclusions

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

29 December 2013

Re: OIG Investigation
Subject: Response to 12 December 2013 notification of tentative conclusion

Below, please find my response to those allegations:

*Misuse of [redacted] application: I have never used a [redacted] application to view my own online security jacket. The program I have used is in PeopleSoft. There is a list of queries that you can choose to review. [redacted]

The other query is under Reinvestigations which only shows your history, including dates of all polygraphs and reinvestigations. There is no detail concerning the findings of these processes, only dates and who conducted the polygraphs and reinvestigations. Also included is your exact EOD date, which not needing that date very often, I do get the month and day confused, so on processes that require an exact EOD date, I do review so that I can use the correct date of EOD.

*Information on [redacted] via CBR: I absolutely assume full responsibility for querying [redacted] credit report with extenuating circumstances.

(b)(6)

[redacted] I did not print the CBR or print it. I was under great duress that day and did not thoroughly and did not think through what the result of my actions would be. I did indeed know that our computers are constantly monitored, so I was not trying to sneak behind the Agency's back. There was no "private gain" for me. I do believe that I briefly discussed my situation with [redacted] but am not certain if the recorder was still running at that time.

I don't feel that accusing me of misusing a "federal government communication system" to obtain information about myself is a fair assessment. There is nothing in those queries except generic information and in no way reflects what is contained in my security file. If I wanted to see information about myself, I could request a file review, but even in a file

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

review, you are not given complete information. Items are withheld from you and not allowed to be reviewed. If these are not allowed to be reviewed, then why not deny access, like the

The programs that I used, at the time of my suspension were (not trained to use CBR request and PeopleSoft. I did not have access to until never prior to that date. 3 to 4 requests were made through I previously told that the requests were sent to but that was incorrect. I only dealt with When I was almost immediately tasked to to help I worked in years ago and the process for requesting investigations was easier and very basic. I had no training of the new process. The training that was scheduled on my first week of returning to work, I was not given the note by my supervisor, until it was too late to attend. If I was given this information when it came to I would have had ample time to get the training and ask questions. I was told by and that I ask too many questions, so they removed me from that tasking. Lists of names were emailed to me by and These names were the only names I ever ran queries on. These queries were part of the new process, to determine

Having extensive handling and processing these security files (a complete review of the file) which contains the in depth information about the Subject. I was also never made aware of the fact that I could not retrieve my own information in that limited program.

I have always been respectful and mindful of following rules, no matter what the rules apply to; life, work, etc. I have always been fair dealing with employees/people as a former supervisor in my last employment for years. I feel that in the last 5 years in I have not been treated fairly by co-workers of my supervisors. All I ask of you is that same fairness.

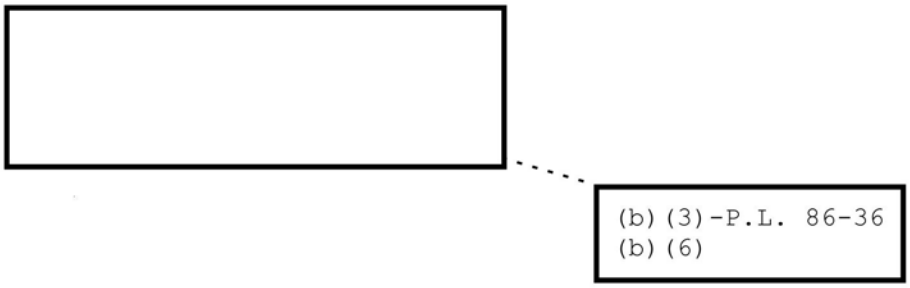
THE ONLY QUERY I PROCESSED THAT WAS NOT ACCORDING TO AGENCY GUIDELINES WAS THE CBR ON

The additional accusations aside from the CBR are not correct. I have been completely honest with Since this suspension was put into effect , September 2013, I have been so ashamed of myself due to breaching the trust of the Agency and I am sincerely sorry. I love my country and would never do anything to cause harm to it.

I made a bad decision that day, which resulted in the situation that I am currently in. I, in no way intended to cause harm to my country and would never cause harm to my country. I felt compelled I will do anything to maintain my employment with NSA, even if it means that my clearance is limited.

Sincerely,

(b)(6)


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