~~TOP SECRET//SI//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



INSPECTOR GENERAL

REPORT OF INVESTIGATION

12 February 2016

IV-13-0077

Misuse of SIGINT Systems

(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.

Approved for Release by NSA on 30 September 2022, FOIA Case # 85643 Litigation

~~TOP SECRET//SI//NOFORN~~

(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.

Release 2022-10
NSA 21920

IV-13-0077

I. SUMMARY

(U//~~FOUO~~) This investigation was conducted in response to an allegation that [redacted] had misused the Signals Intelligence (SIGINT) System.[1]

~~(TS//SI//NF)~~ On 7 and 9 May 2013, the OIG received allegations that [redacted] had improperly tasked United States Person (USP) [redacted] phone numbers [redacted] for collection [redacted]

~~(TS//SI//NF)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

~~(TS//SI//NF)~~ The complainant (hereafter "the Source") alleged that [redacted] was collecting or attempting to collect USP [redacted] communications without proper authorization and without a foreign intelligence purpose (FIP).[3] The Source also claimed that the tasking records [redacted] entered had been improperly entered [redacted] The Source said [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) Many of the officials who had knowledge of the allegations attempted to assess the matter. However, their reviews were insufficient to determine whether [redacted] had violated

[1] (U//~~FOUO~~) [redacted] For a table of abbreviations and acronyms see Appendix A2; for definitions see Appendix A3.

[2] (U//~~FOUO~~) See Appendices F1 and F2 for emails from the Source to the OIG, dated 7 and 9 May 2013.

~~(S//SI//REL)~~ [redacted]

[3] (U//~~FOUO~~) Foreign intelligence is defined in EO 12333 as information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

[4] ~~(S//SI//REL~~ [redacted]

~~(S//SI//REL)~~ [redacted]

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

Release 2022-10
NSA 21921

Doc ID: 6789496

any law or regulation because, many of them told the OIG, they did not understand the work [redacted] performed. The OIG found that oversight officials and [redacted] management lacked an understanding of his work, did not believe that [redacted] was doing anything improper, and continued to approve his taskings. Several officials, including some in SV, stopped looking into the allegations after they learned of the OIG's investigation, even though the OIG had advised them to proceed in whatever manner they believed appropriate.

~~(TS//SI//REL)~~ **CONCLUSION**: Substantiated. [redacted]

[redacted] His activities resulted in, or were at least reasonably likely to result in, the unauthorized collection of communications to or from USPs or persons in the United States, or both. The preponderance of the evidence supports the conclusion that, by doing so, and failing to report the non-compliant activity, [redacted] violated the classified annex of DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* and its classified annex, NSA/CSS Policy 1-23, United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and U.S. Minimization Procedures*, and USSID SP0019, *NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy*.[5]

~~(TS//SI//REL)~~ In addition, [redacted] also violated USSID DA3511, *Data Acquisition Directorate and Data Flow Management*, [redacted]

~~(TS//SI//REL)~~ Finally, the preponderance of the evidence supports the conclusion that [redacted] violated [redacted] and USSID SP0019 when he [redacted] effected collection that resulted or was at least reasonably likely to result in the unauthorized collection of communications to or from [redacted] and did not report the non-compliant activity.[7]

(U//~~FOUO~~) OIG Investigations (D14) referred this matter to OIG Intelligence Oversight (D11), with a recommendation that D11 notify the NSA SIGINT Director of practices discovered during the investigation that may require his attention. [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[5] (U//~~FOUO~~) This matter has been referred to the NSA Office of General Counsel regarding the possible violation of Titles I and/or VII of the Foreign Intelligence Surveillance Act.

[6] (U//~~FOUO~~) The overarching authorities [redacted] violated are Executive Order (EO) 12333, *United States Intelligence Activities*, and Department of Defense (DoD) Directive 5240.01, *DoD Intelligence Activities*.

[8] (U//~~FOUO~~) See Appendix B1 for the memorandum to the SIGINT Director regarding compliance concerns.

Release 2022-10
NSA 21922

(U//~~FOUO~~) A copy of this report will be provided to Employee Relations. A summary of our findings will be referred to [redacted] supervisor and the Associate Directorate for Security and Counterintelligence, Special Actions (Q242).

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

II. (U) BACKGROUND

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

(U) Introduction

(U//~~FOUO~~) Since [redacted] has been assigned to the [redacted] within the Signals Intelligence Directorate (SID). [redacted] supports the Agency's [redacted]

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

(S//SI//REL) [redacted] performs [redacted] as part of his official duties. [redacted]

(S//SI//REL) As part of his official duties, [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(S//SI//REL) [redacted]

(S//SI//REL) [redacted]

(TS//SI//REL) The following is an organizational chart showing where [redacted] were located within the Signals Intelligence Directorate (SID) and where [redacted] was assigned at the time the OIG initiated this investigation.

[redacted]

[9] (S//SI//REL) [redacted]

[10] (S//SI//REL) [redacted]

[11] (U) [redacted]

IV-13-0077

Signals Intelligence Directorate (SID)

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

Release 2022-10
NSA 21925

(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) Employees from the following organizations were involved in trying to determine whether [redacted] had violated any law or regulation [redacted]

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

- Signals Intelligence Directorate (SID, [redacted]) at various organizational levels
- SID Oversight and Compliance (SV)
- Office of the Director of Compliance (ODOC)
- Office of the General Counsel (OGC)

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

(U//~~FOUO~~) In addition to interviewing [redacted], the OIG obtained sworn testimony from the following employees:

- Source [redacted]
- Senior Executive, Senior Technical Leader, [redacted]
- [redacted]
- GG15, Staff Officer and Compliance Officer, [redacted]
- GG15, Staff Officer and Compliance Officer [redacted]
- GG15, Manager, [redacted]
- Senior Executive, [redacted] Subject Matter Expert
- [redacted]

(U//~~FOUO~~) The OIG also attended meetings with the following employees regarding the matter under investigation and memorialized relevant information in Memoranda for the Record:

- Mr. Ronald Moultrie, Senior Executive, Deputy Director, SID
- [redacted]
- Senior Executive, Senior Technical Director, [redacted]
- Senior Executive, Deputy General Counsel for Litigation and Management, Office of the General Counsel (OGC) [redacted]
- Senior Executive, Deputy General Counsel for Operations, OGC
- [redacted]
- Senior Executive, Chief, SID Oversight and Compliance, SV
- GG14, Manager, [redacted] SID Office of Oversight and Compliance (SV)

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

Release 2022-10
NSA 21926

[redacted] GG12, Intelligence Analysis Technician, [redacted]
GG14, Intelligence Analysis Technician, [redacted]
[redacted] GG13, [redacted] Program Manager
[redacted] GG14, [redacted] Program Manger
[redacted] GG12, [redacted] Program Manger
[redacted] Contractor, [redacted] Program Manager, [redacted]
[redacted]
[redacted] Deputy, Office of Director of Compliance [redacted]

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

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

(U//~~FOUO~~) Due to the complexity of the work performed by [redacted], the OIG also received assistant from the following subject matter experts:

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

[redacted]

(U//~~FOUO~~) Additionally, the OIG obtained and reviewed relevant emails, data and metadata pertaining to [redacted], standard operating procedures for [redacted] and [redacted] training record.

(U) Applicable Authorities

(See Appendix A1 for a full table of authorities)

- (U) Executive Order (EO) 12333, *United States Intelligence Activities*, as amended
- (U) Department of Defense Directive (DoDD) 5240.01, *DoD Intelligence Activities*, 27 August 2007
- (U) Department of Defense (DoD) Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, and its Classified Annex
- (U) United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and U.S. Persons Minimization Procedures*, 25 January 2011
- (U) USSID SP0019, *NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy*, 13 November 2012, revised 7 May 2013
- (U) USSID DA3511, *Data Acquisition Directorate Targeting and Data Flow Management,* 28 November 2006
- (U) NSA/CSS Policy 1-23, *Procedures Governing NSA/CSS Activities That Affect U.S. Persons*, 11 March 2004, revised 30 July 2013
- [redacted]

- (U) USSID SD4000, *Signals Intelligence Development*, 6 April 2011 (USSID SD4000 was superseded by SID Implementing Directive, *Annex F Governance of the Signals Intelligence Mission*, 25 February 2013)

Release 2022-10
NSA 21928

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

III. FINDINGS

~~(TS//SI//NF)~~ ***ALLEGATION:*** *Did* [redacted] *misuse the SIGINT system, in violation of DoD 5240.1-R and its Classified Annex, NSA/CSS Policy 1-23, USSID SP0018, USSID SP0019* [redacted]

~~(TS//SI//REL)~~ **CONCLUSION**: Substantiated. [redacted] His activities resulted in, or were reasonably likely to result in, the unauthorized collection of communications to or from USPs or persons in the United States, or both. The preponderance of the evidence supports the conclusion that, by doing so, and failing to report the non-compliant activity, [redacted] violated the classified annex of DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* and its classified annex, NSA/CSS Policy 1-23, United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and U.S. Minimization Procedures,* and USSID SP0019, *NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy*.

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~ In addition, [redacted] also violated USSID DA3511, *Data Acquisition Directorate and Data Flow Management*, when he [redacted]

~~(TS//SI//REL)~~ Finally, the preponderance of the evidence supports the conclusion that [redacted] violated [redacted] and USSID SP0019 when he [redacted] effected collection that resulted or was at least reasonably likely to result in the unauthorized collection of communications to or from [redacted] and did not report the non-compliant activity.[13]

(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[12] (U//~~FOUO~~) The overarching authorities [redacted] violated are Executive Order (EO) 12333, *United States Intelligence Activities*, and Department of Defense (DoD) Directive 5240.01, *DoD Intelligence Activities*.

Release 2022-10
NSA 21929

(U) Documentary Evidence

(U//~~FOUO~~) Oversight and Compliance Training

(U//~~FOUO~~) [redacted] training record revealed that he had completed the following oversight and compliance training:

- *USSID SP0018 Training for Analytic Personnel* (OVSC1800), 6 May 2014, 20 June 2013, and 19 July 2012;[14]
- *Overview of Signals Intelligence Authorities* (OVSC1100), 10 February 2014, 10 April 2013, 2 August 2012, and 18 October 2011;
- *NSA FISA* (OVSC1201), 13 January 2014 and 12 February 2013;
- *NSA/CSS Intelligence Oversight Training* (OVSC1000), 4 November 2013 and 13 June 2012; and
- *Special Training on FISA* (OVSC1206), 15 May 2013.

(U//~~FOUO~~) Complaints Made to the OIG and Supporting Data

~~(TS//SI//NF)~~ The Source provided emails and data spreadsheets to the OIG in support of the allegations.[15]

(U//~~FOUO~~) Information provided to the OIG by [redacted]

~~(S//SI//REL)~~ During his interview with the OIG on 27 June 2013, [redacted] provided a copy of a paper he had written entitled, [redacted] The paper is at Appendix G1. He also provided a list of [redacted] which is at Appendix G2. [redacted] also provided a list of [redacted] The list is at Appendix G4.

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

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

[14] (U//~~FOUO~~) OVSC1800 was previously entitled, *Legal Compliance and Minimization Procedures*, which [redacted] completed on 17 October 2011 and 16 November 2010.

[15] (U//~~FOUO~~) See Appendix F for emails pertaining to the allegations. The data files the Source provided to the OIG in support [redacted] claims are labeled: [redacted] The data files were too voluminous to include as attached Appendices and are retained in electronic format in the OIG as Appendices B3.1 through B3.15. A chart summarizing the allegations is at Appendix B3.

Doc ID: 6789496

(U//~~FOUO~~) Information provided to the OIG by [redacted] Chief

(U//~~FOUO~~) In a 26 June 2013 email to the OIG, [redacted] provided a copy of briefing slides entitled [redacted] The slides, which are at Appendix H1, provide information on the [redacted]

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

~~(S//REL)~~ In a 28 June 2013 email to the OIG, [redacted] provided a copy of a Standard Processing Form (SPF) that he called a draft "Standard Operating Procedure" for work performed in the [redacted]

(U) Testimonial Evidence

(U//~~FOUO~~) The Source, Global Network Analyst[17]

(U//~~FOUO~~) The Source [redacted] was interviewed on 14 May 2013 and provided the following sworn testimony.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(S//SI//REL)~~ The Source [redacted]

~~(TS//SI//REL)~~ The Source believes that, since February 2013, [redacted] has been in violation of USSID SP0018 because he has been collecting or attempting to collect United States phone numbers without proper authorities and without a foreign intelligence purpose.

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

~~(TS//SI//REL)~~ The Source also believes that [redacted] has been collecting or attempting to collect [redacted] without approval from [redacted] and an appropriate [redacted] and without a foreign intelligence purpose, in violation of [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~ The collection or attempted collection, the Source said, was done using [redacted] which [redacted] tasked to the SIGINT system. The tasking records [redacted] in violation of USSID SP0018. Since October 2011 and in violation of USSID SP0018, the Source believes that [redacted] has collected or attempted to collect a large volume of telephone numbers without any foreign intelligence purpose. The

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

[16] (U) See Appendix H3 for SPF. Also see Appendix H2 for email from [redacted] to the OIG dated 31 July 2013 pertaining to the SPF.

[17] (U) Although the Source waived confidentiality, we have chosen to protect the Source's identity in the main body of this report.

Release 2022-10
NSA 21931

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

IV-13-0077

Source believes that [redacted] which harms NSA mission, the tasking does not qualify [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//REL)~~ On 18 March 2013, the Source asked the [redacted] team [redacted] could assist with their workload. Another [redacted] employee told the Source that she had been trying to get [redacted] to [redacted] but he had refused to do so.[18] The Source began to research problems reported [redacted] and found that [redacted] discovered that [redacted] collection coming from [redacted] when it should not have been.

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

~~(TS//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(TS//SI//REL)~~ [redacted]

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

~~(TS//SI//REL)~~ The Source called [redacted] to discuss the fact that some of the [redacted] wanted to alert him, have him clean it up, and file an Intelligence Oversight incident report. [redacted]

~~(TS//SI//REL)~~ The Source said that, according to an [redacted] analyst, [redacted] had told the analyst that he was [redacted] Based on some of the comments [redacted] put in [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[18] (U) See Appendix C1 for related emails.

Release 2022-10
NSA 21932

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

~~(TS//SI//REL)~~ After the Source spoke with [redacted] called OGC for guidance on how to get [redacted] tasking shut down and the OGC suggested [redacted] Compliance Officer. The Source emailed [redacted] with a description of the incidents and, soon thereafter, [redacted] referred the matter to [redacted] Compliance Officer.[19]

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

~~(TS//SI//REL)~~ After the Source called, [redacted] sent an email to the Source's supervisor, [redacted] and [redacted] supervisor, [redacted] forwarded the email to [redacted] Division Chief, and [redacted] Deputy Division Chief.[20] The Source did not see the email, but [redacted] told the Source that it said that the Source had called [redacted] to tell him there was a problem with his tasking of United States [redacted] numbers and that [redacted] had hung up on the Source.

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

~~(S//SI//REL)~~ After [redacted] sent his email to [redacted] various [redacted] managers met, including [redacted] and perhaps [redacted] the [redacted] Technical Director and Intelligence Oversight Officer. There were no [redacted] at the meeting, and the management officials were expected to come to an agreement as to whether there was a compliance problem and if so, to inform the NSA Office of Compliance (SV). The Source believes that [redacted] does not understand what [redacted] is doing and only repeats whatever [redacted] tells him.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

~~(TS//SI//REL)~~ On two or three occasions [redacted] told [redacted] The Source did not think [redacted] understood that [redacted] which the Source also reported to [redacted]

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

(U//~~FOUO~~) Initially, the Source was working with [redacted] to document an IO incident, but this was never completed and to [redacted] knowledge, no one filed an IO incident report with SV. The Source said that [redacted] that [redacted] personnel had decided that nothing was wrong with what [redacted] was doing and they should drop the issue. [redacted] told the Source that [redacted] had decided that what [redacted] was doing was acceptable. The Source thought that [redacted] did not have the technical expertise to understand what [redacted] was doing and, because they did not consult with [redacted] they did not understand why it was a violation. The Source said that [redacted] and [redacted] agreed with the Source that what [redacted] was doing violated USSID SP0018.

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

[19] (U) See Appendix C2 for related emails.
[20] (U//~~FOUO~~) See Appendix C3 for email dated 18 March 2013 from [redacted] to [redacted]

Release 2022-10
NSA 21933

(U//~~FOUO~~)

(U//~~FOUO~~) , GG15, was interviewed on 27 June 2013 and provided the following sworn testimony.

~~(S//SI//REL)~~ Since has worked in the previously known as the He has performed for approximately years and considers himself the in the Intelligence Community.

~~(S//SI//REL)~~ said that he started his own (unnamed) project provided the OIG with a copy of a paper he had written entitled

~~(S//SI//REL)~~ The collection performs under his project, he said, falls under EO 12333.

~~(S//SI//REL)~~ said that the foreign intelligence purpose behind his project is to make the collection system healthier, the analytic process richer, and the system more efficient by

(U//~~FOUO~~) When began his project, he asked his senior manager at the time, if he should pursue it. said that did not give him a "straight answer," which interpreted as guidance for him to "be careful." decided he would work on his project until someone told him he should stop.[24]

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

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

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

---

[21] ~~(S//SI)~~

[22] (U//~~FOUO~~) See Appendix G1 for document.

[23] ~~(S//SI//REL)~~ To do so intentionally would be a crime.

[24] (U//~~FOUO~~) was second level supervisor— supervisor. The OIG interviewed under oath, and he told the OIG that did not ask for permission to pursue his project. When learned about

(U//~~FOUO~~) current supervisor, has been "fairly aware" of the project and has trusted to do the right thing.

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

(U//~~FOUO~~) has been accused of teaching other people how to task under his project. However, he has not done so because what he is doing is somewhat dangerous and unknown territory and he does not want anyone to end up in trouble by working on his project if it is determined that the project was not appropriate.

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

(~~TS//SI//REL~~)

(~~TS//SI//REL~~)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

(~~TS//SI//REL~~) provided the OIG a copy of a 26 June 2013 email, subject,

(~~S//SI//REL~~)

If he were training other people on the project, he said he would go through the process of determining appropriate audit mechanisms. said he was the only person

---

what was doing he said he was very clear when he told and that they should not do what was doing with and was to stop his project complete statement is included in this section of the report, following statement.

[25] (U) See Appendix G3 for email.

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

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

Release 2022-10
NSA 21935

working on the project, and each day he did not know what he might try to do, what made sense, was easily sustainable, repeatable, and defensible.

~~(S//SI//REL)~~

~~(S//SI//REL)~~

~~(S//SI//REL)~~

~~(S//SI//REL)~~ As of 27 June 2013, complaints from other analysts that it was causing problems because Some were saying that

~~(S//SI//REL)~~ There are approximately and other similar tools that analysts use

~~(TS//SI//REL)~~ gave the OIG a list of If one of the

[26] ~~(S//REL)~~

[27] (U) See Appendix G5 for a 24 September 2013 email from to the OIG stating he removed on 15 July 2013.

[28] ~~(TS//SI//NF)~~ The OIG, Program Managers, exchanged emails dated 2, 4, and 6 November 2013 pertaining to

(b)(3)-P.L. 86-36
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Doc ID: 6789496

numbers turned out to be a United States number, [redacted] would file an IO incident report and [redacted]

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

~~(TS//SI//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(TS//SI//REL)~~ [redacted] is one hundred percent sure that he has never [redacted] a United States number [redacted] he said there has never been any proof that the numbers [redacted]

~~(S//SI//REL)~~ [redacted]

~~(TS//SI//REL)~~ [redacted]

~~(TS//SI//REL)~~ [redacted] To [redacted] knowledge, he has never collected [redacted] from a United States [redacted] person.[31]

~~(TS//SI//REL)~~ [redacted]

[29] ~~(U//FOUO)~~ The list of [redacted] are at Appendix G2. Following the interview, [redacted] sent an email to the OIG dated 27 June 2013 and included an updated printout of the [redacted] See Appendix G4 for email and attachment.

[30] ~~(S//SI//REL)~~ During a meeting on 28 June 2013, [redacted] from OGC informed the OIG that [redacted] This meeting is documented in the OIG's MFR dated 28 June 2013.

[31] ~~(S//SI//REL)~~ [redacted]

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

Release 2022-10
NSA 21937

~~(S//SI//REL)~~ [redacted] did not know if entering these types of comments in [redacted] is a breach of policy but, if it is, he could delete the comments.[32]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

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

~~(S//SI//REL)~~ Only the analysts in the [redacted] have access to the comments that [redacted]

~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ As of early 2013, [redacted]

~~(S//SI//REL)~~ [redacted] has never filed an Intelligence Oversight incident report, although some of his taskings may have resulted in IO incidents. [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

- ~~*(TS//SI//REL)*~~ *The OIG investigator presented to* [redacted] *copies of emails dated 27 and 29 March 2013, which he,* [redacted] *had exchanged. In the documents,* [redacted] *expressed concern about numbers* [redacted] *had tasked,* [redacted]

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

[32] (U//~~FOUO~~) Although [redacted] stated the identifying comments appeared in [redacted] the evidence showed the comments appeared [redacted]

[33] ~~(S//SI//REL)~~ [redacted]

[34] ~~(S//SI//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

Release 2022-10
NSA 21938

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

~~(TS//SI//REL)~~ [redacted] explained that the numbers were [redacted] [redacted] said that he supposes he would have to file an incident report. [redacted]

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

~~(S//SI//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(TS//SI//REL)~~ [redacted]

- *~~(TS//SI//REL)~~ The OIG investigator reminded [redacted] that he had stated his criterion was* [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~ [redacted] responded that, sometimes, [redacted] If the number is of concern and could result in a violation, [redacted] will remove it from tasking.

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

- *~~(TS//SI//REL)~~ The OIG investigator asked [redacted] about a 27 March 2013 email between [redacted] in which [redacted] asked about a number [redacted] had tasked that* [redacted]

~~(TS//SI//NF)~~ [redacted] believed there were about [redacted] which did not pertain to [redacted]

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

[35] (U) See Appendix C5 for email.

Release 2022-10
NSA 21939

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(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) (6)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~ did not know that the [redacted] were of concern because no one told him that his project was causing a problem with the [redacted] did not know how to exclude something from his collection. While working on his project, [redacted] would be excluded from [redacted] collection.

~~(U//FOUO)~~ [redacted] has been proceeding with his project in a "kind of [by the] seat of the pants" mode, and, if he does receive approval to continue work on his project, he will need some guidance on the limitations for taskings. He is willing to "really tighten the reins" [redacted] and thinks that an SOP should be written to cover the scope, purpose, and minimization procedures for his project. Currently, he believes that his project may not be worth documenting, except as a case of bad judgment.

~~(TS//SI//REL)~~ [redacted] read USSID SP0018 as part of his mandatory training requirement. He knows it is unlawful to target United States persons, and he never intended to and to his knowledge never has. [redacted] denied any willful wrongdoing or knowingly tasking a United States [redacted] person. He started his project to help find potential problems. Other than the [redacted] he has no doubt that numbers tasked through his project were not United States [redacted] persons.

(U//~~FOUO~~) [redacted] Division Chief, [redacted]

(U//~~FOUO~~) [redacted] GG15, was interviewed on 14 November 2014 and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] has spent most of his career working on [redacted]. From around 2006 to 2012, he served as Branch Chief [redacted]. In 2009, the [redacted] team moved to his Branch; [redacted] was a member of the [redacted] team. In 2010, [redacted] became the Division Chief of the organization.

~~(S//SI//REL)~~ When the [redacted] team joined [redacted] was the [redacted] Lead and was a direct report to [redacted] was a direct report to [redacted] has been doing [redacted] work for many years; he was the senior person in the [redacted] and he was good at it.

(U//~~FOUO~~) Within the first year of [redacted] working for [redacted] he read in [redacted] monthly notes that he was using a new technique to help determine how to [redacted] numbers. When [redacted] asked [redacted] what the technique was, [redacted] could not explain it very well, so [redacted] met with [redacted] for an explanation.

~~(S//REL)~~ [redacted] told [redacted] that there were [redacted] had already started to [redacted]

IV-13-0077

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

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

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

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

~~(TS//SI//REL)~~ [redacted]

[redacted] He had already begun doing this, without asking [redacted] for permission. None of the other analysts were using [redacted] technique.

~~(S//REL)~~ [redacted] told [redacted], "You cannot do that," because he was intentionally [redacted]

When the OIG Investigator told [redacted] that [redacted] had told the OIG that [redacted] never gave him a straight answer about pursuing his new technique, [redacted] stated he had been very clear when he told [redacted] to stop the activity. He did not know whether [redacted] had lied to the OIG, but perhaps [redacted] does not remember the conversation clearly because [redacted] has known [redacted] to sometimes forget things he has been told.

~~(U//FOUO)~~ [redacted] believed that, after he told [redacted] to stop using his technique, [redacted] complied. However, he did not know if, at some point, [redacted] began using it again. [redacted] has had a lot of experiences with [redacted] not remembering conversations they have had. He could see where [redacted] may have restarted using his technique because he did not remember that [redacted] had told him to stop using it. After [redacted] told [redacted] to stop using his technique, he did not see mention of it again in [redacted] monthly notes. [redacted] did not tell [redacted] more than once that he should stop using his technique.

~~(TS//SI//NF)~~ [redacted] did not believe that any USP [redacted] collection had occurred for which an incident report had to be filed. There did not appear to be any United States numbers on the link, and [redacted] However, he was still [redacted] cautioned [redacted] that he could be [redacted] phone numbers, and [redacted] pushed back stating something like: "Show me a case where that happened." [redacted] told him that he did not have to show him an actual occurrence because the possibility of it occurring was enough; therefore, he could not do it any longer. [redacted] did not think [redacted] agreed with his decision.

~~(TS//SI//NF)~~ [redacted]

Release 2022-10
NSA 21941

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

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

(U//~~FOUO~~) was auditor. He knew that had problems with what was doing, and he knew that had told not to use his technique anymore. did not believe that understood the nuances of activity. He did not think that understood that was intentionally

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(TS//SI//NF)~~

(U//~~FOUO~~) Chief,

(U//~~FOUO~~) GG14, was interviewed on 13 August 2015 and provided the following sworn testimony.

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

(U//~~FOUO~~) In August 2007, was assigned as chief, later called the , which was part of USSID 4000, *Signals Intelligence Development*, states that has the authority for signal development and discovery.

(U//~~FOUO~~) In 2009, was transferred from took with it authority for was not clear where the authority for mission was documented or whether it was still USSID 4000.

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

(U//~~FOUO~~) personnel do not receive guidance from upper management on how to perform their mission because no one understands it. is the sole authority for mission. No decision has been made on whether mission requires scrutiny.

~~(TS//SI//REL)~~ said that, in a memorandum dated 28 September 2011, OGC, provided approval [36] did not formally document process or seek approval within his chain of command to conduct because, based on his experience, no one outside cared about what they did. The process and procedures for are found in working notes stored in shared directory.

[36] (U) See Appendix H4 for the OGC opinion and related emails.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(C//REL)~~

(U//~~FOUO~~) In 2013, after allegations had been made to the OIG about compliance officer asked to write a standard operating procedure (SOP). documented process in a Standard Processing Form.[37]

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

(U//~~FOUO~~) In late 2013 and through 2014, a new SOP was drafted for but it was never finalized, and does not know why. The new SOP states that the Chief is responsible for reporting to the compliance officer However, personnel never reported to their compliance officer any

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

(U//~~FOUO~~) Currently, there are including These are the numbers on which experiment focused.

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

~~(TS//SI//REL)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(TS//SI//REL)~~ did not seek approval from or discuss anything with OGC or SV about project When the project started, immediate supervisor was Other than telling that was not aware of project. may have mentioned his project to but

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[37] (U//~~FOUO~~) " " the matter under investigation, was based on Throughout his interview, referred to this activity as "project" or "experiment," and it is referred to as such in this section of the ROI.

[38] (U//~~FOUO~~) According to the technical experts who assisted the OIG in reviewing the data related to the allegations,

Doc ID: 6789496

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

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

never said whether could do the project. did not provide direction or ask about experiment.

~~(TS//SI//REL)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//REL)~~ was the only one using decided that he did not want anyone else using techniques until he and determined whether the experiment was worthwhile. When the OIG investigator told that evidence existed showing that he had approved requests for another said that he approved several other than because was having problems with for

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(TS//SI//REL)~~

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

~~(TS//SI//REL)~~ When submitted a he would informally talk with about what he did Documentation may have received from about has been destroyed.

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

~~(U//FOUO)~~ always approved requests because he believed that knew what he was doing.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(C//REL)~~

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

[39] ~~(C//SI//REL USA, FVEY)~~

[40] ~~(C//REL USA, FVEY~~

Release 2022-10
NSA 21944

(U//~~FOUO~~) [redacted] trusts [redacted] to do the right thing.

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

~~(C//REL)~~ [redacted]

~~(S//REL)~~ [redacted]

~~(C//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

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

(U//~~FOUO~~) The value of [redacted] project was to [redacted] said: "To be honest with you, it was a work in progress. It had not been fully thought out as far as what you do with it at the end of the day."

~~(C//REL)~~ No intelligence oversight incident reports have been filed as a result of [redacted] work. [redacted] relies on [redacted] to tell him if his collection resulted in USP communications.

(U//~~FOUO~~) [redacted] never received a request to [redacted]

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

~~(C//REL)~~ After the complaints had been filed with OIG, the [redacted] compliance officer suggested that a warning go out [redacted]. [redacted] never sent the warning because the activity stopped. He was not sure if anyone else sent a warning.

[41] ~~(C//REL)~~ [redacted]

Release 2022-10
NSA 21945

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//REL)~~ said he had never seen the data before and, obviously, had made an error and the data in the file was problematic. The collection from this activity should have resulted in an IO incident report, . In hindsight, what he did was probably not the best approach.

~~(TS//SI//REL)~~

~~(TS//SI//REL)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(TS//SI//REL)~~

~~(TS//SI//REL)~~

~~(TS//SI//REL)~~

Release 2022-10
NSA 21946

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

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

(U//~~FOUO~~) ***Special Authorities and Compliance Lead for***

(U//~~FOUO~~) GG14, was interviewed on 20 June 2013 and provided the following sworn testimony.

(U//~~FOUO~~) is assigned to Since March, 2010, she has served as the Special Authorities and Compliance Lead and is responsible for matters associated with collection authorities and for ensuring that compliance procedures are followed.

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

~~(TS//SI//FVEY)~~ In March 2013, received a telephone call from the OIG Source, who expressed concern that was deliberately tasking and collecting information associated with phone numbers that were potentially United States

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) sent an email to dated 20 March 2013 and asked what he was doing and why he thought that what he was doing was appropriate. She explained that, if he had created an Intelligence Oversight (IO) incident, he would be responsible for submitting an incident report. She then called to discuss the matter, but he hung up on her. He later called back, apologized for hanging up, and told her to go through his chain of command if she had questions about his work.

(U//~~FOUO~~) In a 20 March 2013 email, the OIG Source told that

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

(U//~~FOUO~~) In a 20 March 2013 email, asked the Compliance Officer, to look into the matter, verify what was happening, and determine if an IO incident had occurred. told that she wanted the Source and the other who had concerns about to document the concerns into one summary. was not sure whether the summary was ever prepared.

~~(TS//SI//REL)~~ On 28 March 2013, and met with who provided a demonstration of the work does and why they believed that tasking, was appropriate. They explained that,

Release 2022-10
NSA 21947

[redacted] numbers are collected appropriately and only when authorized. They told [redacted] that EO 12333 was the authority for this activity.

~~(TS//SI//REL)~~ [redacted] understood the [redacted] process when [redacted] and [redacted] explained it to her, but the work was "over [her] head" and she did not believe that she could adequately describe it. To her understanding, [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

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

~~(TS//SI//REL)~~ [redacted]

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

~~(TS//SI//REL)~~ [redacted] concluded there were no IO violations with regard to [redacted] work. [redacted] who had worked in the NSA Oversight and Compliance (SV) organization, had told [redacted] that she did not believe that an IO violation had occurred. [redacted] told [redacted] that she wanted to document [redacted] activity and the process he used so that it would be clearly understood by all that his activity was authorized. [redacted] did not know if the documentation had been completed, but she knew that [redacted] had been working with all involved to document the activity. She felt confident that [redacted] would have contacted SV, if she believed that an IO incident had occurred.

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

~~(TS//SI//REL)~~ Following her meeting with [redacted] management, [redacted] received a call from [redacted] of OGC, who told her that the OIG Source had reported [redacted] activity to him as a problem. [redacted] did not believe that [redacted] thought that [redacted] activity was a problem, but he wanted [redacted] to look into the matter to make sure. [redacted] told [redacted] Technical Director and Intelligence Oversight Officer, that she had received a call from OGC about [redacted] work. [redacted] told [redacted] that he had already tried to explain to the OIG Source that [redacted] work was authorized, and, if [redacted] still had concerns, [redacted] should talk with [redacted] management, rather than OGC.

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

~~(TS//SI//REL)~~ [redacted] did not believe that [redacted] had tasked anything [redacted] although she did not confirm this. She did not believe that the [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Release 2022-10
NSA 21948

[redacted] was now concerned that [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~ [redacted] believed that an allegation from the OIG Source that [redacted] was [redacted] should be examined. If [redacted] was doing what had been alleged, he should stop the activity and fix the tasking so that he only collects what he is authorized to collect and not United States numbers. [redacted] thought that the activity was stupid and that [redacted] However, if [redacted] was looking to see [redacted] she could understand, but the description and purpose of the activity should be documented; there should be no tasking of numbers without documentation.

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

(U//~~FOUO~~) [redacted] did not have concerns about [redacted] technical ability and did not believe that [redacted] was doing anything malicious. She did, however, have some concerns about his work activity and planned to consult with [redacted] and [redacted] leadership to obtain documentation that explained what [redacted] was doing, how he was doing it, and why.

(U//~~FOUO~~) [redacted] Compliance Officer, [redacted]

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

(U//~~FOUO~~) [redacted] GG15, was interviewed on 24 June 2013 and provided the following sworn testimony.

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

(U//~~FOUO~~) From 2006 through 2009, [redacted] worked on Foreign Intelligence Surveillance Act matters in the SID Oversight and Compliance Office (SV). For the past year and half she has served as a Compliance Officer in [redacted]

~~(TS//SI//REL)~~ On 20 March 2013, [redacted] received an email from [redacted] the [redacted] Compliance Officer, stating that OGC had contacted her regarding a complaint OGC had received that [redacted] of the [redacted] was collecting on United States telephone numbers. [redacted] wanted [redacted] to look into the matter.

(U//~~FOUO~~) [redacted] and [redacted] Chief [redacted] told [redacted] that they did not believe that there were compliance concerns with [redacted] work. However, because of the concerns raised, they agreed to [redacted] was using until they met and reached an understanding that there were no compliance concerns.[42] [redacted] did not verify [redacted] In follow-on discussions with [redacted] management, it was determined there were no compliance concerns, and [redacted]

[42] (U) See Appendix C4 for emails related to [redacted]

(U//~~FOUO~~) On 22 March 2013, [redacted] attended a meeting with [redacted] Chief of Staff, [redacted] Branch Chief, to discuss [redacted] work. [redacted] explained the work his branch was doing, and [redacted] said that some training might be needed so that [redacted] all have the same understanding of the procedures. Everyone seemed to agree that what [redacted] was doing was acceptable. [redacted] management said the authority for [redacted] work was USSID 4000.

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

~~(S//SI//REL)~~ [redacted] had to rely on management's technical explanations because [redacted] is a very complicated process. She asked [redacted] and [redacted] management if they were familiar with EO 12333 procedures, its privacy protections, minimization procedures and protection for United States Person communications. Emphatically and unequivocally, they all said "yes". This included [redacted] [redacted] Chief, and [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(TS//SI//REL)~~ [redacted]

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

~~(TS//SI//REL)~~ [redacted] had emails from [redacted] the [redacted] Technical Director, stating that he had spoken to [redacted] and understood what [redacted] was doing. [redacted] only concern was [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) Following the meeting with [redacted] management, [redacted] emailed the OIG Source and informed [redacted] that the meeting had occurred, the issue had been resolved, and the Source's manager would follow-up with the Source. The Source still had problems with what [redacted] was doing and sent many emails to [redacted] that included much technical detail. [redacted] told the Source that she could not make an assessment based on the level of technical detail [redacted] was providing and suggested the Source meet with [redacted] management so they could understand [redacted] concerns because, as far as [redacted] knew, the Source's manager had already determined that there was no problem with [redacted] work.

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

(U//~~FOUO~~) [redacted] repeatedly went back to [redacted] asking for a coordinated position on their concerns, but never received one. She also notified her leadership, as well as the [redacted] Chief of Staff about the Source's concerns.

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

(U//~~FOUO~~) [redacted] management continued to discuss the matter in email and in person. [redacted] had several emails from management asserting that the matter had been resolved by management. However, the OIG Source continued to email [redacted] who would refer the Source back to management and technical directors.

(U//~~FOUO~~) Several weeks later, [redacted] Technical Director [redacted] contacted [redacted] and told her that the Source had contacted him. [redacted] said that he asked [redacted] and [redacted] of his organization look into the matter.

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

(S//SI//~~REL~~) On 15 April 2013, [redacted] and [redacted] management met. Everyone understood what was being done, and the only concern [redacted] raised was that [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(TS//SI//~~REL~~) [redacted] suggested to [redacted] management that they prepare a SOP or SPF that described the technical operation of [redacted] project and the procedures. [redacted] prepared an SPF that described the operation, mitigation procedures, and oversight measures that protect against collection of United States Person communications. The SPF was forwarded to [redacted] for comment.

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

(U//~~FOUO~~) In the SPF, [redacted] asked [redacted] for help in creating [redacted] which [redacted] had said that his organization would help to create. However, several weeks went by with no response from [redacted] Eventually, [redacted] told [redacted] that [redacted] personnel had been too busy to review the SPF or help [redacted] but that they would eventually do both.

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

(U//~~FOUO~~) [redacted] Target and Tasking Subject Matter Expert

(U//~~FOUO~~) [redacted] Senior Executive, was interviewed on 11 December 2014 and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] has been assigned to [redacted] since July 2013. Before that, he had been assigned to the [redacted] where, starting in August 2004, he served as the Deputy Chief and about three to four years later became the Technical Director.

(TS//~~REL~~) Around 4 April 2013, the Source told [redacted] that something strange was occurring [redacted] and asked him to look into the matter. The Source said that [redacted]

(TS//SI//~~NF~~) [redacted]

Release 2022-10
NSA 21951

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

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

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

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

~~(G//REL)~~ After the Source reported the concern to he sent an email on 4 April 2013 to colleagues in and asked them to check In a 4 April 2014 email to

~~(TS//REL)~~ On 4 April 2013, told Compliance Officer, that he suggested that he speak with Compliance Officer.

~~(TS//REL)~~ was concerned that

~~(TS//SI//NF)~~ Around that time, met with Chief and some others. could not remember who else was in the meeting or whether was present. said they were

[43] ~~(S//SI//REL)~~ See Appendix C6 for emails. At Appendix J1 is an email dated 28 June 2013 from

[44] (U) See Appendix C6 for email.

Release 2022-10
NSA 21952

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//REL)~~

~~(TS//REL)~~

~~(TS//REL)~~

~~(TS//REL)~~ Because the data collected was EO 12333 data,

~~(TS//SI//NF)~~ Another concern

~~(TS//REL)~~ In a 17 April 2013 email to asked for guidance on

[45] (U) See Appendix C7 for email.

Release 2022-10
NSA 21953

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//REL)~~

~~(TS//SI//NF)~~ In a 30 April 2013 email,

~~(TS//REL)~~

~~(TS//REL)~~

~~(TS//REL)~~

~~(TS//REL)~~

~~(TS//REL)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

[46] (U) See Appendix C7 for email.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//REL)~~

~~(TS//REL)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(U//~~FOUO~~) did not believe that was trying to get past people who would stop him from what he is trying to do. He probably simply saw his project as an easy way to accomplish his targeting and collection.

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

(U//~~FOUO~~) did not think was doing anything malicious in his targeting and collection efforts, but he did think he was being careless and clumsy.

(U//~~FOUO~~) would not expend resources that is trying to

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

(U//~~FOUO~~) Technical Director and Intelligence Oversight Officer (IOO)

(U//~~FOUO~~) GG14, was interviewed on 19 June 2013 and provided the following sworn testimony.

(U//~~FOUO~~) is assigned to the and serves as the Technical Director. He has served as the IOO for about two years and is responsible for submitting IO incident reports to the Office of the Inspector General for the IO quarterly report.

~~(S//SI//REL)~~ Near the end of March 2013, the OIG Source and some other analysts claimed that was doing something unusual

~~(S//SI//REL)~~ To better understand what was doing, posed some questions to him in writing, to which responded in an email dated 27 March 2013.[47]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[47] (U) See Appendix C5 for email.

~~(S//SI//REL)~~ [redacted] did not fully agree with how [redacted] was going about his work but believed that it fell under technical development, which, perhaps, made it acceptable. [redacted] [redacted] supervisor, told [redacted] that the work fell under USSID 4000 as technical development or protocol development, which made it okay.

~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

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

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

~~(S//SI//REL)~~ [redacted] did not know of any instances of [redacted] activities having a negative impact [redacted] He asked the OIG Source and the other [redacted] analysts if they had examples of this, but they did not provide any.

~~(S//SI//REL)~~ [redacted] was particularly concerned that [redacted]

~~(S//SI//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[48] (U//~~FOUO~~) Inadvertent collection occurs when NSA has intentionally targeted and collected communications to, from or about a valid foreign target, which later turns out to be a U.S. person.

Doc ID: 6789496

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ [redacted] was conducting, and he did not believe that the work was auditable.

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

(U//~~FOUO~~) [redacted] Compliance Officer [redacted] told [redacted] that she wanted to understand his position on the matter before moving forward. [redacted] was supposed to have followed up with [redacted] but never did. He drafted an email to [redacted] but never sent it. He had wanted to discuss the email content with [redacted] first but forgot to.[50]

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

(U//~~FOUO~~) [redacted] believed that, if [redacted], who had worked in the Oversight and Compliance Office (SV), had concerns about [redacted], she would raise those concerns with SV or tell [redacted] to stop his activity.

(U//~~FOUO~~) [redacted] told [redacted] that she had spoken with [redacted], understood what he was doing, and was comfortable with it. [redacted] took no further action.

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

(U//~~FOUO~~) Based on [redacted] judgment, [redacted] told the [redacted] analysts that what [redacted] was doing fell under technical development and there were no concerns. A few of the analysts shook their heads in disagreement, and the OIG Source remained adamant that [redacted] activity was improper. [redacted] described analysts in [redacted] and [redacted] as "fighting cats," and he believed that [redacted] and the OIG Source do not like each other.

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

(U//~~FOUO~~) [redacted] has no reason to doubt [redacted] technical abilities and does not believe that [redacted] is doing anything malicious or illegal. [redacted] served as the Technical Director of the organization before [redacted].

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

(U//~~FOUO~~) [redacted] is not entirely sure that what [redacted] is doing is legitimate. He is about 98% sure. In hindsight, [redacted] felt he should have checked with Oversight and Compliance and did not know whether anyone else advised Oversight and Compliance Office or the Office of the General Counsel of the concerns, but he believes that perhaps they should have been raised to those offices.

---

[49] (U//~~FOUO~~) See Appendix L5 for a copy of [redacted] email dated 21 August 2013 stating [redacted]

[50] (U//~~FOUO~~) [redacted] provided a copy to the OIG of the draft email. See Appendix C5.

Release 2022-10
NSA 21957

(U//~~FOUO~~) Assessments of data related to [redacted] taskings

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

(U//~~FOUO~~) Due to the complexity of the work [redacted] performed, the OIG consulted with two technical experts, [redacted] Both reviewed [redacted] and they provided assessments to the OIG. Their assessments have been consolidated in a chart at Appendix B3.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(U//~~FOUO~~) [redacted] and [redacted] provided their comments regarding the [redacted] SOP covering [redacted] (See Appendices D3 and E7)

~~(TS//SI//NF)~~ [redacted] concluded that [redacted]

~~(S//SI//REL)~~ [redacted]

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted]

~~(TS//SI//NF)~~ [redacted]

(b) (6)

[51] (U//~~FOUO~~) [redacted] Since [redacted] he has been assigned as a Technical Leader to the National Threat Operations Center (NTOC, [redacted] Previously, he served as the Intelligence Analysis Technical Leader/Director in the SIGINT Development Strategy and Governance [redacted] Emails associated with [redacted] assessment are at Appendix D. From 2006 to 2009, [redacted] served as the Technical Director for [redacted] He was responsible for overall [redacted] From 2009 until the present, he is the subject matter expert for data quality, [redacted] analysis are addressed later in this report and in an appendix.

[52] (U//~~FOUO~~) On 1 July 2013 OIG personnel attended a meeting with [redacted] OGC, and others. During the meeting [redacted] to which [redacted] has access are limited to approximately [redacted]

Release 2022-10
NSA 21958

(U//~~FOUO~~) Senior Executive, Senior Technical Leader,

(U//~~FOUO~~) DISL, was interviewed on 18 December 2013 and provided the following sworn testimony.[53]

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

(U//~~FOUO~~) has served as the Technical Director (TD) for the Data Acquisition Organization since January 2008 and the TD for the SIGINT Mission Functional Architect organization since April 2013. He will continue to serve in both positions until a replacement is identified for the TD position.

~~(S//SI//REL)~~ recently attended meetings with representatives of and to discuss SIGINT activities. The consensus was that, if see

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

(U//~~FOUO~~) an OGC Attorney, was present for the discussions and work. , as well as and management, The general conclusion was that the probably should put some procedures in place, but everyone in the meeting believed that the work was doing was acceptable.

(b) (3)-P.L. 86-36
(b) (5)

~~(S//SI//REL)~~ believes that However, they should ensure that their process and policy was documented

~~(S//SI//REL)~~ did not always understand the pertaining to

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

~~(S//SI//REL)~~ was surprised to learn that

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

[53] (U//~~FOUO~~) Before the OIG interviewed he attended several meetings and exchanged many emails about activities. discussed concerns about activities with OGC, and others. Emails are at Appendix L. The OIG memorialized the meetings the OIG participated in with ; see Appendix M for memoranda for the record of those meetings.

(U//~~FOUO~~) Using a computer projection screen, [redacted] pertaining to [redacted] work along with [redacted] and provided his assessment.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(S//SI//REL)~~ In general, [redacted] said he would defer to [redacted] assessment.

[redacted]

~~(S//SI//REL)~~ However, other analysts who looked at [redacted]

[redacted]

~~(S//SI//REL)~~ [redacted] said that [redacted] had concluded that many of [redacted] files

[redacted]

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

(U//~~FOUO~~) [redacted] reviewed the following data files.

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

(U//~~FOUO~~) File: [redacted] (Appendix B3.7)

~~(TS//SI//NOFORN)~~ [redacted]

[redacted]

(U//~~FOUO~~) File: [redacted] (Appendix B3.2)

~~(S//SI//REL)~~ [redacted] stated that in [redacted] assessment of this file, [redacted]

[redacted]

and so he was deferring to [redacted] assessment and believed that [redacted] activity in this file "doesn't look good."[54]

[54] ~~(C//SI//REL USA, FVEY)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) File: **(Appendix B3.9)**

~~(S//SI//REL)~~

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(U//~~FOUO~~) File: **(Appendix B3.6)**

(U//~~FOUO~~) Although did not fully understand the data in this file, he agreed with assessment that

(U//~~FOUO~~) File: **(Appendix B3.5)**

~~(S//SI//REL)~~ agreed with assessment of this file:

(U//~~FOUO~~) Files: **(Appendix B3.4)**

~~(S//SI//REL)~~ agreed with written assessment of these files. written assessment stated:

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) Office of the General Counsel (OGC)

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

(U//~~FOUO~~) On 18 June 2013, the OIG received a telephone call from GG15, Senior Operations Counsel, OGC. He said that the Source had contacted him with concerns about and he did not fully understand what was allegedly doing. He was considering scheduling a meeting with the Source and to obtain additional information and was seeking additional information from the OIG about the allegations. The OIG responded to by email on the same day and informed him of the allegations.[55]

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

(U//~~FOUO~~) On 28 June 2013, the OIG met with and Technical Director, to discuss conduct and obtain legal opinion about whether was breaking any law or regulation.[56]

[55] (U) See Appendix I1 for email. Appendix I2 includes emails that were exchanged between and

[56] (U//~~FOUO~~) This meeting is documented in the OIG's MFR dated 28 June 2013.

~~(TS//SI//NF)~~ wrote the following example on a white board for discussion purposes:

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)
(b)(6)

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

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

~~(S//SI//REL)~~ In an email dated 2 July 2013 from to the OIG, , the Source, , and summarized a meeting all the email recipients had attended on 1 July 2013.[58]

- is responsible for reviewing targeting, and is satisfied that it is permissible and that the Source's concerns are unfounded.

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

[57] (U) USSID SP0018 defines "communicant" as a sender or intended recipient of a communication.

[58] ~~(S//SI//NF)~~ See Appendix I3 for email. Other points from the meeting documented in the OIG's MFR include

(b)(3)-P.L. 86-36
(b)(5)

IV-13-0077

- [redacted] and [redacted] approval of them. Typically, Oversight and Compliance would do this, but, since the OIG is involved, [redacted] was not sure how the matter would be addressed.
- [redacted]
- [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

(U//~~FOUO~~) The OIG met with [redacted] TD, and [redacted] OGC, on 20 August 2013.[59]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)
(b)(6)

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

- (~~S//SI//REL~~) [redacted]
- (~~TS//SI//NF~~) [redacted]
- (U//~~FOUO~~) [redacted] was concerned that [redacted] seemed to be making changes in the [redacted] with no oversight.
- (~~S//SI//REL~~) [redacted] said that EO 12333 would be violated [redacted]
- (~~S//SI//REL~~) [redacted] said that the Foreign Intelligence Surveillance Act (FISA) would be violated [redacted]

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

[59] (U//~~FOUO~~) This meeting is documented in the OIG's MFR dated 20 August 2013.

Release 2022-10
NSA 21963

- ~~(TS//SI//NF)~~
- ~~(TS//SI//NF)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)
(b) (6)

(U//~~FOUO~~) an OGC attorney who provided counsel to alleged improper use of the SIGINT system, provided an email to that, in summary, states

(b) (3)-P.L. 86-36
(b) (5)

(U//~~FOUO~~) SID Oversight and Compliance (SV)[61]

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

(U//~~FOUO~~) On 14 November 2013, the OIG met with the Source and to discuss some of the Source's concerns about use of the SIGINT system.[62]

~~(TS//SI//NF)~~ said that, if the possibility existed to collect on a USP, the incident should have been reported.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(TS//SI//NF)~~

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

(U//~~FOUO~~) On 13 August 2015, during a meeting with the OIG, said that SV did not provide a super audit of queries to the OIG because the only data that could audit applied to The system

[60] (U//~~FOUO~~) See Appendix L11 for the email.
[61] (U) See Appendix K for documentary evidence pertaining to or SV provided to the OIG.
[62] (U//~~FOUO~~) This meeting is documented in the OIG's MFR dated 14 November 2013.

(b)(3)-P.L. 86-36
(b)(5)

[redacted] Thus, SV was unable to determine whether [redacted] had caused an intelligence oversight incident because SV was [redacted] acknowledged that SV's support to the OIG regarding this investigation was disjointed because a number of people were involved. When [redacted] first became involved, the Source was not able to articulate the allegation properly and OGC [redacted]

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

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

~~(S//REL)~~ [redacted] asserted that, [redacted]

~~(S//REL)~~ Upon review of some of the file labeled [redacted] suggested that OGC determine whether the matter should be reported to DOJ because, even though the data had been collected under E.O. 12333, because of [redacted] it may be of interest to DOJ. [redacted] stated that, if [redacted] reported as an IO incident.

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

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted] quickly reviewed [redacted] recent queries and said that he noticed [redacted]

(U//~~FOUO~~) Information Obtained from SIGINT System Program Managers

(U//~~FOUO~~) In a 28 June 2013 email, [redacted] Program Manager told the OIG [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(6)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ In a 17 September 2013 email to the OIG, [redacted]

[63] (U//~~FOUO~~) The OIG included in the Management Advisory at Appendix B the fact that SV [redacted] queries [redacted] provided this information in an email to the OIG dated 13 August 2015, which is at Appendix K8.

[64] ~~(C//REL)~~ See Appendix J1 for 28 June 2013 email. According to [redacted]

[65] (U) See Appendix J3 for email.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] Technical Director, gave the OIG [redacted] records from [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

[redacted]

66 ~~(C//SI//REL)~~ [redacted]

(U) Analysis and Conclusions

(U) **DoD 5240.1-R** implements DoD Directive 5240.01 and EO 12333, Section 2.3. This regulation contains the Attorney General-approved procedures for all DoD IC components and has a classified annex that governs SIGINT activities.[67] The Classified Annex to DoD 5240.1-R states that communications of or concerning USPs may be intercepted intentionally or selected deliberately only under certain specific circumstances. The Classified Annex requires the Director of NSA (DIRNSA), or his designee, to issue directives and instructions implementing the procedures found in the Classified Annex. USSID SP0018 is the Agency directive that implements the classified annex.[68]

(U//~~FOUO~~) **NSA/CSS Policy 1-23**, paragraph 1, states that NSA/CSS shall collect, process, retain, and disseminate information about USPs only as prescribed in DoD Directive 5240.1, DoD 5240.1-R and its Classified Annex, and the Foreign Intelligence Surveillance Act (FISA). Paragraph 3 states that the SIGINT mission of the NSA/CSS is to collect, process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions. Paragraph 3 also states that NSA/CSS shall intentionally collect only foreign communications and shall not intentionally collect U.S. person communications without proper legal authorization.

(U//~~FOUO~~) **USSID SP0018** § 3.1 also states that it is the policy of the U.S. SIGINT System (USSS) to target or collect only foreign communications and the USSS will not intentionally collect communications of or about USPs or persons or entities in the United States, except as set forth in USSID SP0018.[69]

~~(S//SI//REL~~) **USSID SP0018** § 4.1 states that communications known to be to, from, or about a USP, [redacted] will not be intentionally intercepted, or selected through the use of a selection term, except in certain specified instances with the approval of the Foreign Intelligence Surveillance Court (FISC), the Attorney General, or DIRNSA. USSID SP0018 § 4.1(c)(5) also states that voice and facsimile communications with one communicant in the United States may be targeted for collection only with the prior approval

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[67] (U) DoD 5240.1-R and its Classified Annex were approved by the Attorney General prior to the creation of the Director of National Intelligence and the requirement for consultation with the Director of National Intelligence.

[68] (U//~~FOUO~~) USSID SP0018 incorporates the requirements of all the higher level authorities listed above; so compliance with USSID SP0018 generally ensures compliance with those higher level authorities. A violation of USSID SP0018, however, does not necessarily result in a violation of a higher level authority. In cases of noncompliance with USSID SP0018, the misconduct must also be examined against the requirements of the higher level authorities to determine whether additional violations have occurred.

[69] (U) In accordance with USSID SP0018, section 9.18.e., a person known to be currently in the United States will be treated as a USP unless that person is reasonably identified as a non-USP or circumstances give rise to a reasonable belief that such person is not a USP. A person known to be outside the United States, or whose location is not known, will not be treated as a USP unless such person is reasonably identified as such or circumstances give rise to a reasonable belief that such person is a USP.

Release 2022-10
NSA 21967

of DIRNSA (when the approval of the Attorney General or the FISC is not required[70]) if technical devices (e.g., [redacted] are employed that limit acquisition by the NSA to communications when the target is a non-USP outside the United States [redacted].[71]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI)~~ **USSID DA3511** states that the [redacted]

[redacted]

~~(S//SI//REL)~~ Accordingly, SIGINT collection is permissible only if it is reasonably designed not to intentionally target communications of or about USPs, or persons in the United States, unless targeting a specific USP or person in the United States pursuant to the prior approval of the FISC, Attorney General, or DIRNSA.

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

~~(S//SI//REL)~~ [redacted] activities violated these restrictions. Not only were his activities not reasonably designed not to intentionally target communications of or about USPs, his activities did in fact target and collect such communications.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ [redacted] told the OIG that he started his own [redacted] project in 2012.[72] [redacted]

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

[70] (U) FISA requires FISC authorization for the acquisition of the contents of wire communications to or from a person in the United States, without consent, if such acquisition occurs in the United States. 50 U.S.C. 1801(f)(2).

[71] ~~(S//SI//REL)~~ The Classified Annex has similar provisions in § 4.A.1. Thus, a violation of § 4 of USSID SP0018 would also result in a violation of the Classified Annex, DoD 5240.1-R, DoDD 5240.01, NSA/CSS Policy 1-23, and EO 12333.

[72] ~~(S//REL)~~ In 2012, [redacted] worked in [redacted] According to [redacted] second-level supervisor at the time he began to work on his project, he told [redacted] to stop the work because he was not allowed to [redacted] told the OIG that [redacted] never gave him a "straight" answer about working on his project and, therefore, [redacted] decided he would work on it until someone told him he should stop. [redacted] told the OIG that [redacted] was unaware of [redacted] project, unless [redacted] had mentioned it to him, and if he did, [redacted] provided no guidance to [redacted] or [redacted]. In March 2013, [redacted] approved its own procedures that described [redacted] work (SPF signed by [redacted] at Appendix H3). As discussed above, the March 2013 procedures were revised significantly in May 2014 to include several restrictions after OGC review (Appendix L11).

[73] ~~(TS//SI//NF)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (9) (C)
(b) (9) (C)
50 USC 3605

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

Release 2022-10
NSA 21968

[redacted]

~~(S//SI//REL)~~ [redacted] Well-established procedures exist to request and document exceptions to these safeguards when validated foreign intelligence needs necessitate the targeting and collection of U.S. selectors.

~~(TS//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ [redacted] resulting in [redacted] reasonably likely to result in the interception of communications to or from a USP [redacted]

- ~~(S//SI//REL)~~ [redacted]
- ~~(TS//SI//NF)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[74] ~~(S//REL)~~ A sample of [redacted] The list is at Appendix J10.

[75] ~~(S//REL)~~ See Appendix B3 and B3.1, B3.2, B3.3 for data regarding [redacted]

[76] ~~(S//SI//REL)~~ OIG findings regarding the examples were based on the assessments of data files performed by the technical experts with whom the OIG consulted. A summary of their assessments for all of the data files they reviewed, including the examples listed at this section, are at Appendix B3. Their complete assessments are at Appendices D and E.

[77] ~~(S//SI//REL)~~ The data file reviewed by the technical experts regarding this example [redacted] which is at Appendix B3.7.

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

- ~~(TS//SI//NF)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ Although told the OIG that he was completely sure that he had the evidence shows that he did. He told the OIG in an email that he was going to Further, during his testimony,

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

~~(TS//SI//NF)~~

[78] ~~(S//SI//REL)~~ The data files reviewed by the technical experts regarding this example are entitled which are at Appendices B3.2 and B3.3.

[79] ~~(S//SI//REL)~~ The data file reviewed by the technical experts regarding this example is entitled which is at Appendix B3.6. Non-foreign communications shall be promptly destroyed unless the Attorney General or the DIRNSA waives the destruction requirement. Non-foreign communications are either communications solely between persons in the United States or solely between USPs. In the first case, only the Attorney General may waive the destruction requirement; in the second case, the DIRNSA may waive the destruction requirement, under certain conditions documented in USSID SPOO18.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[80] ~~(TS//SI//NF)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

Release 2022-10
NSA 21970

Doc ID: 6789496

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(TS//SI//NF)~~ [redacted] contends that his activity was compliant [redacted] We disagree. [redacted] did not obtain approval from the Foreign Intelligence Surveillance Court, the Attorney General of the United States, the NSA Director, or the Signals Intelligence Director before [redacted] targeting and collection of USPs without proper authority and without following established procedures violated USSID SP0018 §§3.1 & 4.1 and USSID DA 3511, which in turn resulted in a violation of NSA/CSS Policy 1-23 §1, and DoD 5240.1-R, classified annex.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ Furthermore, because [redacted] did not report and cease the non-compliant activity combined with the above described activities, he violated USSID SP0019 §3.6 which states:

> ...every individual must comply with applicable laws, statutes, directive, and regulations by: reporting any non-compliant activity to management, an IOO, SV, and OIG; taking measures to reduce the risk of non-compliant activity and to prevent future non-compliant activity; and exercising due diligence to remain compliant, i.e., make every reasonable attempt to adhere to the rules and standards.

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

(U//~~FOUO~~) Section 4.8 of USSID SP0019 defines reportable activity as any conduct that may be non-compliant with an Executive Order, Presidential Directive, or DoD policy or regulation. Section 4.10 states that, when non-compliant activities are detected, the activity that caused the non-compliant situation must be stopped immediately and the situation closely monitored to verify that the problem has been resolved.

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

~~(S//SI//NF)~~ **Signals Intelligence Directorate** [redacted]

[redacted]

[81] ~~(TS//SI//NF)~~ See Appendices C1, C8, F3, and F11 for related emails.

Release 2022-10
NSA 21971

Doc ID: 6789496

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(S//SI//REL)

(U//~~FOUO~~) Foreign Intelligence Purpose

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ Many witnesses questioned whether for his activities.[84] Some witnesses, including OGC personnel, were willing to accept that however, they were unsure because they had difficulty understanding his complex and technical work. Other witnesses, including subject matter experts, agreed that

(b) (3)-P.L. 86-36
(b) (5)
(b) (6)

(U//~~FOUO~~) The OIG concludes that determining whether had a valid foreign intelligence purpose for each of his activities is unnecessary because, even assuming that he did, he failed to comply with the authorities and procedural safeguards governing SIGINT activities that target and collect USP communications.

~~(TS//SI//REL)~~ said that, when the was transferred to , it took with it the authority for was unsure where the authority for mission was documented but believed that it may have been USSID4000.

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

[82] ~~(S//NF)~~

[83] ~~(S//SI//REL)~~ The data file reviewed by the technical experts regarding this example, which is at Appendix B3.7.

[84] (U//~~FOUO~~) EO 12333, §1.7(c) states that NSA shall conduct its SIGINT activities "for foreign intelligence and counterintelligence purposes to support national and departmental missions."

Release 2022-10
NSA 21972

Doc ID: 6789496

"Signals Intelligence Development."[85] However, it is unclear whether [redacted] activities were SIGDEV as defined and described in USSID SD4000. Assuming his activities were SIGDEV, [redacted] (and [redacted]) failed to comply with USSID SD4000 (and Annex F) because, for example:

- USSID SD4000 says that [redacted] governs SIGDEV activities, but [redacted] initiated his project on his own with no coordination with [redacted] (or anyone else);[86]
- USSID SD4000 requires that all SIGDEV activities comply with EO 12333, USSID SP0018, etc.; however, as discussed above, [redacted] activities did not comply with those authorities; and
- USSID SD4000 requires auditing of queries; however, SV is unable to audit [redacted] queries because the system [redacted] that [redacted]

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

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

(U//~~FOUO~~) [redacted] actions should be considered in context of the conflicting guidance he was given. Although [redacted] was told by different supervisors, oversight officials, and attorneys that his activities were acceptable, he was also told by others to stop immediately. Many officials involved in trying to determine what [redacted] was doing and whether he had violated policies or regulations relied on [redacted] explanations or on other officials involved in the matter because they did not fully understand the technical details of [redacted] project. More detailed information regarding the actions or non-actions of individuals with regard to [redacted] activities will be forwarded to appropriate Agency officials in a separate report.[88]

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(S//REL)~~ The OIG found that, even if [redacted] was truly unaware that he had tasked and collected USP [redacted], and whether or not his management or officials responsible for intelligence oversight directed [redacted] to stop his project due to non-compliant activity, [redacted] acted with reckless disregard of the regulations, policies, and procedures that govern the use of the SIGINT system when he started his project and continued to work on it.

~~(TS//SI//REL)~~ [redacted] is an experienced analyst who has worked [redacted] years. He touts himself as [redacted] [redacted] acknowledged to the OIG that he had been proceeding with his project in a "kind of [by the] seat of the pants" mode and that his project was "kind of dangerous . . .and is unknown territory . . .at the very least." He said that he had not trained anyone else on the techniques of his project because he did not want anyone to end up in trouble, if it was determined that the project was not appropriate. [redacted] acknowledged that he needed guidance on the limitations for his

---

[85] (U//~~FOUO~~) USSID4000 was superseded by SID Implementing Directive, Annex F, *Governance of the Signals Intelligence Mission*, 25 February 2013.

[86] (~~TS//SI//REL~~) See Appendix H3 for [redacted] dated 6 May 2009, which formalized an agreement between [redacted] started his project in 2012, after the mission had been transferred to [redacted]

[87] (U//~~FOUO~~) The new [redacted]

[88] (U//~~FOUO~~) See Appendix B2 for the memorandum to the SIGINT Director regarding management accountability.

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

Release 2022-10
NSA 21973

Doc ID: 6789496

taskings. He also told the OIG that his project may not be worth documenting except "as a bad choice of judgment."

~~(TS//SI//REL~~) Based on his technical knowledge, experience, and self-awareness that his project was, at minimum, questionable, [redacted] was careless and exercised poor judgment when he started his project without having his project officially and completely vetted through his management chain and the Agency offices responsible for oversight of such activities, such as SV and OGC.

~~(TS//SI//REL)~~ [redacted] said that he knew that no one was [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(TS//SI//REL~~) Although [redacted] contends that his activity was compliant and he did not task U.S. selectors or collect USP [redacted] the OIG found that [redacted] had tasked and collected on USP [redacted], an analyst with extensive experience in [redacted] and trained on the use of and rules pertaining to the SIGINT system, knew or should have known that his taskings, at the very least, were likely to result in the interception of communications to or from USPs [redacted] without the requisite prior approvals.

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

~~(TS//SI//REL~~) **CONCLUSION**: Substantiated. [redacted] His activities resulted in, or were at least reasonably likely to result in, the unauthorized collection of communications to or from USPs or persons in the United States, or both. The preponderance of the evidence supports the conclusion that, by doing so, and failing to report the non-compliant activity, [redacted] violated the classified annex of DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* and its classified annex, NSA/CSS Policy 1-23, United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and U.S. Minimization Procedures,* and USSID SP0019, *NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy.*

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~ In addition, [redacted] also violated USSID DA3511, *Data Acquisition Directorate and Data Flow Management*, when he [redacted]

[89] (U//~~FOUO~~) The overarching authorities [redacted] violated are Executive Order (EO) 12333, *United States Intelligence Activities,* and Department of Defense (DoD) Directive 5240.01, *DoD Intelligence Activities.*

Release 2022-10
NSA 21974

~~(TS//SI//REL~~) Finally, the preponderance of the evidence supports the conclusion that [redacted] violated [redacted] and USSID SP0019 when he [redacted] effected collection that resulted or was at least reasonably likely to result in the unauthorized collection of communications to or from [redacted] and did not report the non-compliant activity.[90]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

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

[90] (U) [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Release 2022-10
NSA 21975

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//~~FOUO~~) The OIG provided a copy of the tentative conclusion to [redacted] on 18 December 2015. [redacted] provided his response to the OIG in three emails dated 18 December 2015 and one email dated 21 December 2015.[91]

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

V. (U) CONCLUSION

(U//~~FOUO~~) [redacted] response provided no new or substantive information relative to the conclusion or requiring additional investigation; therefore, the conclusion remains unchanged.

[91] (U) See Appendix N for a copy of [redacted] responses to the OIG's tentative conclusion.

Release 2022-10
NSA 21976

VI. (U) DISTRIBUTION OF REPORT

(U//~~FOUO~~) OIG Investigations (D14) will refer this matter to OIG Intelligence Oversight (D11), with a recommendation that D11 notify the NSA SIGINT Director of practices discovered during the investigation that may require his attention. Some practices appear to increase the risk of unauthorized collection and mishandling of USP [redacted] information and have the potential for misuse of the SIGINT system.[92]

(U//~~FOUO~~) A copy of this report will be provided to Employee Relations. A summary of our findings will be referred to the Associate Directorate for Security and Counterintelligence, Special Actions (Q242), and [redacted] supervisor.

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

[redacted]
Senior Investigator

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

[redacted]
Assistant Inspector General
for
Investigations

[92] (U//~~FOUO~~) See Appendix B1 for the memorandum to the SIGINT Director regarding compliance concerns.

APPENDICES

(U//~~FOUO~~) The following appendices are included as attachments to this ROI.

- Appendix A
  - A1: Table of Authorities
  - A2: Table of Abbreviations and Acronyms
  - A3: Definitions

- Appendix B
  - B1: Memorandum for the SIGINT Director - Intelligence Oversight of [redacted] Activities
  - B2: (*not used*)
  - B3: Summary Chart of Allegations, Data File References, and Technical Experts' Assessments of Data

- Appendix N: [redacted] response to the OIG's tenative conclusion.

(U//~~FOUO~~) The following appendices are on file in the OIG and are available upon request.

- Appendices B3.1 through B3.15 : Data files referenced in Appendix B3
- Appendix C: Documentary evidence covering events prior to the filing of the OIG complaint.
- Appendix D: Assessment of technical expert #1
- Appendix E: Assessment of technical expert #2
- Appendix F: Emails and other documentary evidence from the Source regarding the allegations
- Appendix G: Documentary evidence provided by or pertaining to [redacted]
- Appendix H: Documentary evidence provided by or pertaining to [redacted] Chief [redacted]
- Appendix I: Documentary evidence provided by or pertaining to the OGC
- Appendix J: Documentary evidence provided by various [redacted] Program Managers
- Appendix K: Documentary evidence provided by or pertaining to SID Oversight and Compliance (SV)
- Appendix L: Documentary evidence provided by or pertaining to [redacted] Management (other than [redacted]
- Appendix M: OIG Memoranda For The Record

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

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

Release 2022-10
NSA 21978

APPENDIX A.1

Table of Authorities

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

Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20390901

Release 2022-10
NSA 21979

APPENDIX A.1

(U) Applicable Authorities

- **(U) Executive Order 12333, United States Intelligence Activities (As amended by Executive Orders 13284 (2003) 13355 (2004) and 13470 (2008))**

  (U) Part 2.3 Collection of information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

  > (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;...

- **(U) Department of Defense Directive Number 5240.01, DoD Intelligence Activities, dated 27 August 2007**

  (U) POLICY. It is DoD policy that:
  4.1. All DoD intelligence and CI activities shall be carried out pursuant to the authorities and restrictions of the U.S. Constitution, applicable law, E.O. 12333…and other relevant DoD policies… Special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. persons.

- **(U) Department of Defense Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, dated December 1982.**

  (U) C5. CHAPTER 5
  (U) PROCEDURE 5. ELLECTRONIC SURVEILLANCE

  > (U) C5.3 PART 3: SIGNALS INTELLIGENCE ACTIVITIES
  >
  > > (U) C5.3.1. Applicability and Scope
  > >
  > > > (U) C5.3.1.1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection, retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.

Release 2022-10
NSA 21980

(U) C5.3.1.2. This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the Attorney General. That regulation shall provide that signals intelligence activities that constitute electronic surveillance, as defined in Parts 1, and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the Attorney General.

(U) C5.3.3. Procedures.

(U) C5.3.3.1. Foreign Communications. The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure.

Classified Annex E to Department of Defense Procedures Under Executive Order 12333 [Annex to DoD 5240.1-R]

(U) Sec. 3: Policy

(U) The Director, National Security Agency, is assigned responsibility for signals intelligence collection and processing activities and communications security activities. In order to assure that these activities are conducted in accordance with the provisions of Executive Order 12333, the Director, or his designee, will issue appropriate directives and instructions implementing these procedures and governing the conduct of the United States Signals Intelligence System and the activities of communication security entities.

~~(C)~~ It is the policy of the United States Signals Intelligence System to collect, retain, and disseminate only foreign communications and military tactical communications. It is recognized, however, that the United States Signals Intelligence System may incidentally intercept non-foreign communications, including those of or concerning United States persons, in the course of authorized collection of foreign communications. The United States Signals Intelligence System makes every reasonable effort, through surveys and technical means, to reduce to the maximum extent possible the number of such incidental intercepts acquired in the conduct of its operations.

…Specific communications sent from or intended for receipt by United States persons are not intercepted deliberately by the United States Signals Intelligence System unless specific authorization for such interception has been obtained in accordance with these procedures.

(U) Sec. 4: Procedures

(U) A.1. Collection.

(a) ~~(S//SI)~~ Communications of or concerning a United States person may be intercepted intentionally or selected deliberately through use of a selection term or otherwise only:

(1) with the consent of such United States person…; or

Release 2022-10
NSA 21981

(2) with specific prior court order pursuant to the Foreign Intelligence Surveillance Act of 1978 where applicable…; or

(3) with the specific prior approval of the Director, National Security Agency …; or

(4) with specific prior approval by the Attorney General…

- **(U) United States Signals Intelligence Directive USSID SP0018, Legal Compliance and U.S. Persons Minimization Procedures, dated 25 January 2011**

Section 3 – (U) Policy

3.1 (U) The policy of the USSS is to target or collect only foreign communications. The USSS will not intentionally collect communications to, from or about U.S. persons or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently collects such communications, it will process, retain and disseminate them only in accordance with this USSID.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Section 4 - (U) Collection

4.1 ~~(S//SI//REL~~) Communications which are known to be to, from or about a U.S. person [redacted] will not be intentionally intercepted, or selected through the use of a selection term, except in the following instances:…

4.1.a. (U//~~FOUO~~) With the approval of the United States Foreign Intelligence Surveillance Court either under the conditions outlined in Annex A of this USSID or as permitted by other FISA authorities.

4.1.b. (U) With the approval of the Attorney General of the United States, if:…

4.1.c. (U//~~FOUO~~) With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHSS), so long as the collection need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General...

- **(U) United States Signals Intelligence Directive USSID SP0019, NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy, dated 13 November 2012, Revised 7 May 2013**

Section 3 – (U) Responsibilities

(U) Individuals and Managers

3.6. (U) Every individual must comply with applicable laws, statutes, directive, and regulations by:

- (U//~~FOUO~~) Reporting any non-compliant activity to management, an IOO, SV, and OIG;
- (U) Taking measures to reduce the risk of non-compliant activity and to prevent future non-compliant activity; and
- (U) Exercising due diligence to remain compliant, i.e., make every reasonable attempt to adhere to the rules and standards.

Section 4 – (U) Policy and Procedures

4.5 (U//~~FOUO~~) …All personnel engaged in activities that include access to SIGINT or visibility of raw SIGINT data must successfully complete OVSC1100,

"Overview of Signals Intelligence Authorities;" and either OVSC1800, "Legal Compliance and Minimization Procedures" or OVSC1806 …
4.8 (U//~~FOUO~~) What is reportable activity? …Non-compliant activity includes, but is not limited to:

(U) Mishandling of U.S. persons information;

(U//~~FOUO~~) Queries against raw SIGINT data which are inadvertently, intentionally, or carelessly likely to target/retrieve United States or Second Party communications;…

4.10 (U) When non-compliant activities are detected, the following actions must be taken:

(U//~~FOUO~~) The activity/action that caused the non-compliant situation must be stopped immediately and the situation closely monitored to verify that the problem has been resolved. Specific corrective actions depend on the situation, but my include de-tasking of selectors, stopping database queries, cancelling reports, etc. …

- **(U) NSA/CSS Policy 1-23, Procedures Government NSA/CSS Activities That Affect U.S. Persons, dated 11 March 2004, Revised 30 July 2013**

(U) POLICY.
1. (U) NSA/CSS shall collect, process, retain, and disseminate information about U.S. persons only as prescribed in DoD Directive 5240.1, DoD Regulation 5240.1-R, orders issued by the Foreign intelligence Surveillance Court…, and the Classified Annex to DoD Procedures under Executive Order 12333 (hereafter referred to as the Classified Annex…)
2. (U) NSA/CSS shall follow compliance standards to protect the privacy rights of U.S. persons during the conduct of NSA/CSS missions.
(U) PROCEDURES
3. (U) Signals Intelligence. The signals intelligence (SIGINT) mission of the NSA/CSS is to collect, process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions. NSA/CSS shall intentionally collect only foreign communications. NSA/CSS shall not intentionally collect U.S. person communications without proper legal authorization. The Director, NSA/Chief, CSS (DIRNSA/CHCSS) may authorize exceptions only pursuant to the procedures contained in DoD Regulation 5240.1-R (Reference e) and the Classified Annex thereto (Reference f).

- **(U) NSA/CSS PMM, Chapter 366: Personal Conduct**

Section 1-2 Responsibilities

B. If an employee violates any of these standards, management officials are responsible for initiating the appropriate action.

J. Avoid the appearance of violating the law or these standards.

Section 1-3 General Principles for On-The-Job Conduct
Generally, every employee is expected to:

E. Give thorough, efficient, and industrious service in the performance of assigned duties including...exercising courtesy and respect in dealings with fellow

Release 2022-10
NSA 21983

workers and the public; and exercising reasonable care in carrying out one's assigned duties;...

Section 5 Reporting Suspected Violations

Executive Order 12333, "United States Intelligence Activities," imposes responsibilities and restrictions on all employees of the intelligence community concerning their role in the conduct of intelligence activities. All violations of the provisions of Executive Order 12333 will be reported to the OIG.

- **(U//~~FOUO~~) United States Signals Intelligence Directive USSID DA3511, Data Acquisition Directorate Targeting and Data Flow Management, dated 28 November 2006**

Section 1 – (U) Purpose

1.2. (U//~~FOUO~~)

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

Section 2 – (U) Policy

(U) Selector Management.

2.2 ~~(S//SI)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

- **(U//~~FOUO~~) Signals Intelligence Directorate**

~~(S//NF)~~ General Guidelines for Targeting

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Release 2022-10
NSA 21984

(U) Targeting.

2. (~~S//SI//NF~~) "Targeting" applies to

(U) Standard Guidelines.

3. (~~S//NF~~) The following charts depict the standard guidelines governing the targeting

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) Targeting

(U)

5. (~~S//SI//NF~~)

(U) Incident Reporting

33. (~~S//NF~~)

Release 2022-10
NSA 21985

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

34. (U) The following conditions require submitting an incident report:

~~(S//NF)~~ [redacted]

35. ~~(S//NF)~~ [redacted]

36. ~~(S//NF)~~ [redacted]

(U) SID Implementing Directive, Annex F, Governance of the Signals Intelligence Development Mission, dated 25 February 2013[1]

1.1 (U//~~FOUO~~) The Associate Deputy Directorate for SIGINT [redacted] is responsible for developing requirements for, and providing governance of discovery activities in all elements performing SIGDEV functions across the USSS.

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

[1] (U//~~FOUO~~) Annex F superseded USSID4000

Release 2022-10
NSA 21986

APPENDIX A.2

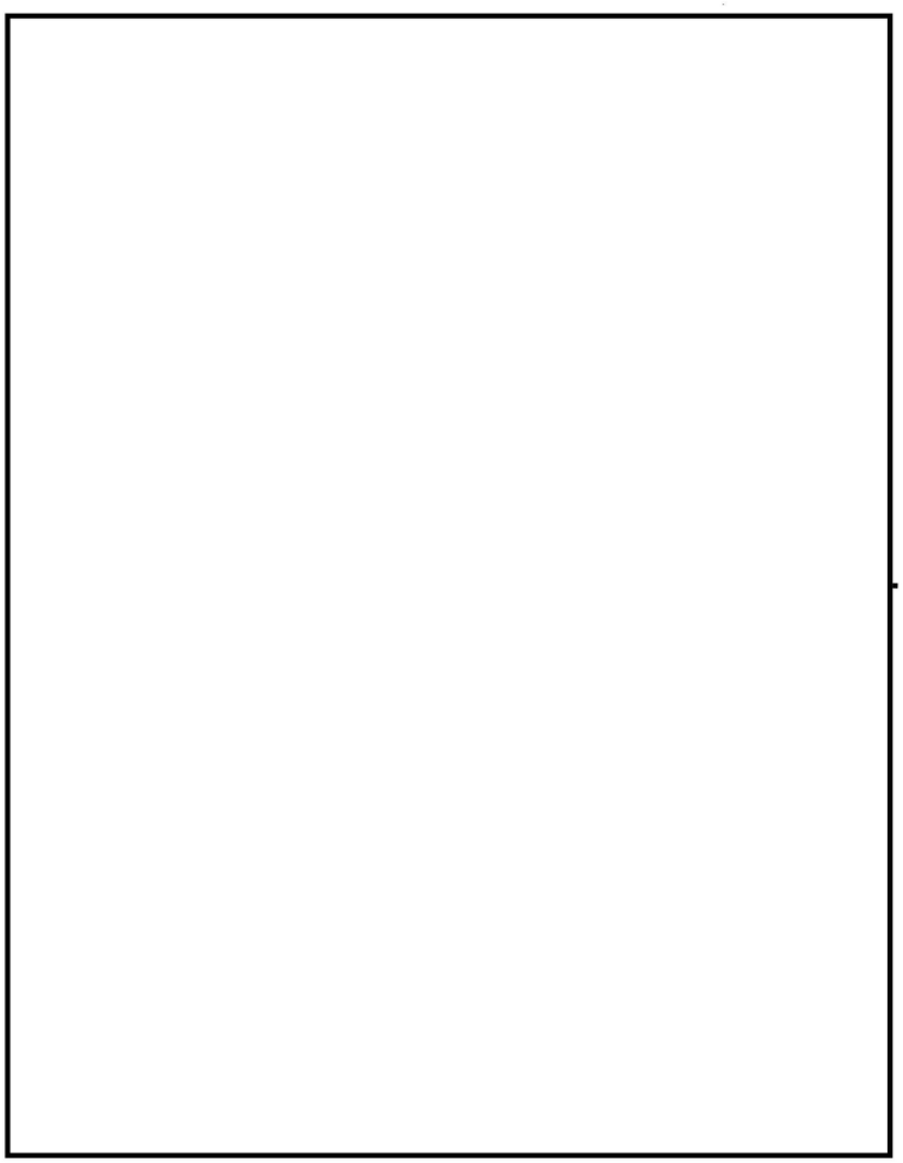
Abbreviations and Acronyms

Release 2022-10
NSA 21987

Appendix A.2

Table of Abbreviations and Acronyms

% is a wildcard for an undefined character length.



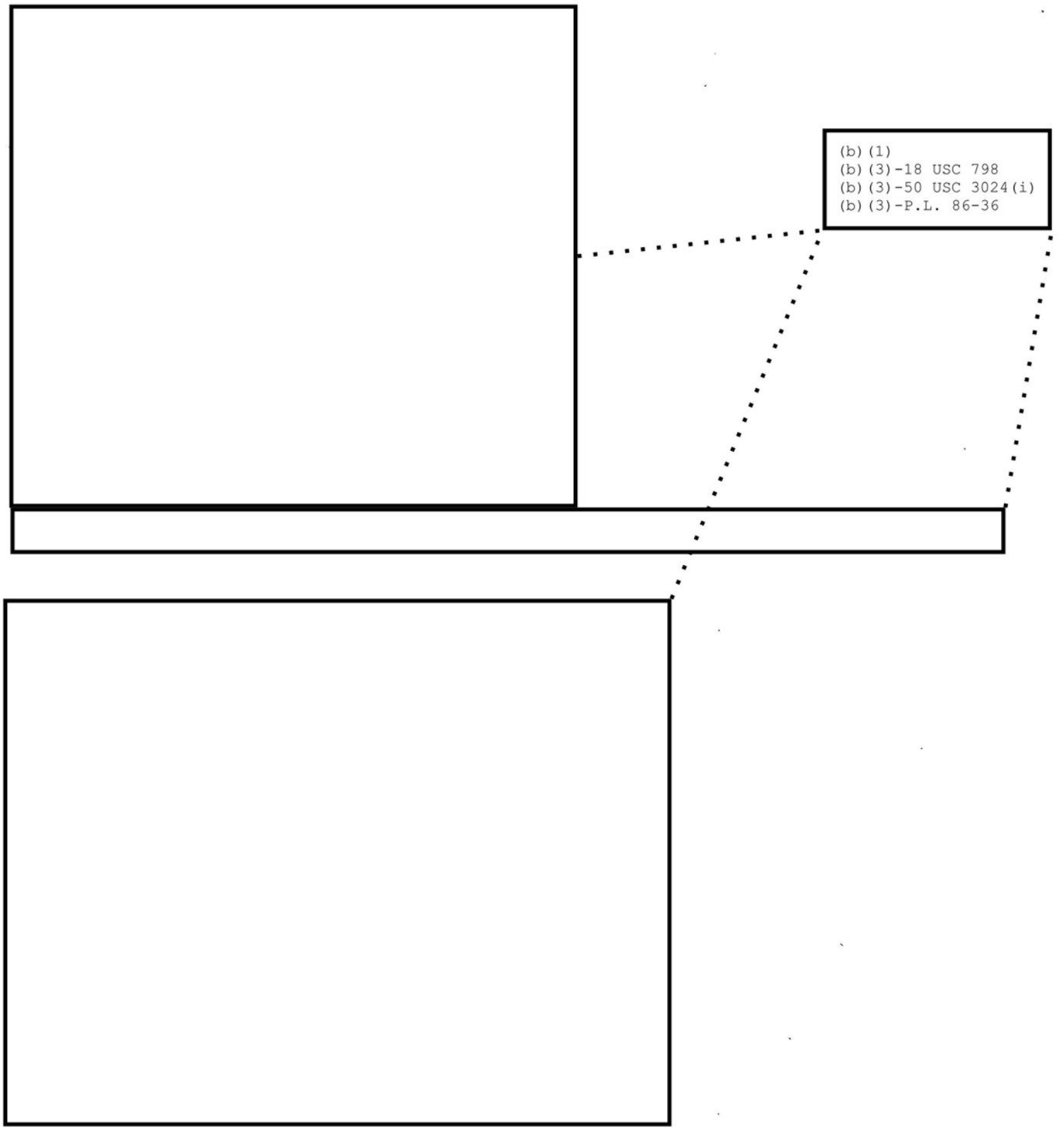
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

F

FIP - Foreign intelligence purpose

G

GCM – Global Capabilities Manager



[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

USP - United States person

APPENDIX A.3

Definitions

Release 2022-10
NSA 21991

Appendix A.3

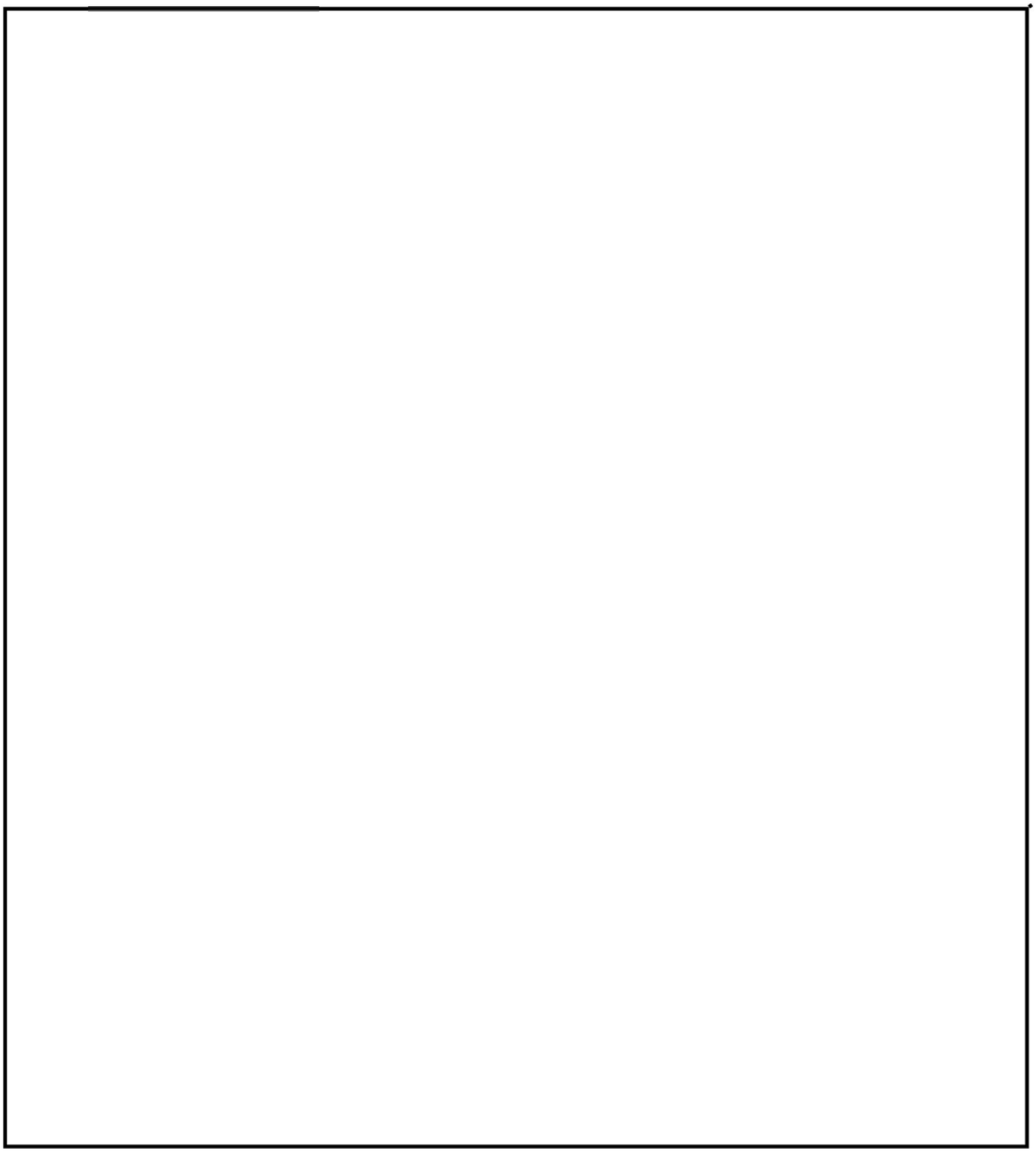
Definitions

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) **Communicant** is defined in USSID SP0018 as a sender or intended recipient of a communication. (Source: USSID SP0018)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) **FIP - Foreign intelligence (foreign intelligence purpose)** is defined in EO 12333 as information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

[redacted]

I

(U//~~FOUO~~) **Inadvertent collection** occurs when NSA has intentionally targeted and collected communications to, from or about a valid foreign target which later turns out to be a U.S. person. (*You think your target is foreign, but it ends up being U.S.*)

(U//~~FOUO~~) **Incidental collection** occurs when collection is directed against legitimate foreign intelligence targets result in the acquisition of information to, from, or about U.S. persons or entities (See USSID SP0018 Section 4.3) (*You targeted a valid number (knew it was foreign) and got a USP (because the foreign target was talking to a USP*).

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

L

(U//~~FOUO~~) [redacted] is the Agency's [redacted] collection software.

M

(~~C//SI//REL USA, FVEY~~) **Minimization** is a process that provides for the protection of U.S. person information during the phases of SIGINT collection and processing. It involves the identification of U.S. person information and then decisions regarding how that information may be used or identified during the various phases of SIGINT production. These phases include SIGINT collection, SIGINT processing, SIGINT retention and SIGINT dissemination.

N

(~~S//SI//REL~~) [redacted]

(~~C//SI//REL USA, FVEY~~) [redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(C//SI//REL USA, FVEY)~~

~~(C//REL)~~

~~(S//SI//REL)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

O

~~(C//SI//REL USA, FVEY)~~

P

~~(S//SI//REL)~~

~~(C//SI//REL USA, FVEY)~~

R

~~(S//SI//REL)~~

~~(S//SI)~~

S

(U//~~FOUO~~)

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Release 2022-10
NSA 21995

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

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

~~(S//SI//REL)~~ **SIGINT system** is any system or capability that is used for one or more of the following SIGINT functions:

~~(C//SI//REL USA, FVEY)~~

T

~~(C//REL USA, FVEY~~)

(U//~~FOUO~~) responsible for reporting on a given topic.

~~(S//REL TO USA, FVEY)~~

~~(S//SI//REL)~~

~~(C//SI//REL USA, FVEY)~~

U

~~(S//SI//REL~~

(U) **United States person (USP)** is defined in USSID SP0018 as: a. A citizen of the United States; b. An alien lawfully admitted for permanent residence in the United States; c. Unincorporated groups and associations of a substantial number of members of which constitute a. or b. above, or d.; Corporations incorporated in the United States including United States flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

W

(U//~~FOUO~~)

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

Y

~~(S//SI//REL)~~

Z

~~(S//SI//REL)~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

APPENDIX B1

Memorandum for SIGINT Director

Release 2022-10
NSA 21998

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

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL

12 February 2016
IG-11850-16

(U) MEMORANDUM FOR SIGINT DIRECTOR

SUBJECT: (U//~~FOUO~~) Intelligence Oversight of [redacted] Activities—ACTION MEMORANDUM

(U//~~FOUO~~) The Office of the Inspector General (OIG) identified practices in the Signals Intelligence Directorate (SID) that are inconsistent with NSA/CSS policies and procedures. [redacted]; they therefore require your attention.

I. (U//~~FOUO~~) Improper Use of [redacted]

~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ [redacted]

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[1] (U//~~FOUO~~) This information resulted from an OIG investigation of a [redacted] alleged misconduct. Questions concerning that investigation should be directed to the Assistant IG for Investigations.

[2] (U) Association analysis, also called link analysis or network analysis, is a method to gain analytic insight by visualizing social, business, and other connections among people and groups, as well as infrastructure, logistics, and production chains.

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20410212

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

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(C//SI//REL)~~ The OIG consulted with SID technical experts, who concluded that, on some occasions, [redacted]

[redacted]

II. (U//~~FOUO~~) Bypassing Controls

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

~~(C//SI//REL)~~ [redacted]

[redacted]

B. (U) Wildcards

~~(S//SI//REL)~~ [redacted]

[redacted]

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

[redacted]

[3] (U) [redacted]

[redacted]

[4] ~~(S//SI//REL)~~ [redacted]

[redacted]

[5] ~~(S//SI//REL)~~ [redacted]

Release 2022-10
NSA 22000

C. (U//~~FOUO~~)

~~(S//SI//REL)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

III. (U//~~FOUO~~) Deficient Auditing

~~(C//SI//REL)~~ SID Oversight and Compliance (SV) could not audit all queries

~~(C//SI//REL)~~ Although an audit log of all transactions performed in

IV. (U//~~FOUO~~) Negative Effect on Mission

(U//~~FOUO~~) When we attempted to verify in

~~(C//SI//REL)~~ The collection resulting from

[6] (U//~~FOUO~~) Data verification was based on capabilities available in September 2013.

[7] (U//~~FOUO~~) Non-foreign communications must be promptly destroyed unless the Attorney General or the DIRNSA waives the destruction requirement. Non-foreign communications are either communications solely between persons in the United States or solely between USPs. In the first case, only the Attorney General may waive the destruction requirement; in the second case, the DIRNSA may waive the destruction requirement, under certain conditions documented in USSID SP0018.

[8] (U//~~FOUO~~) Some numbers collected under this project

Release 2022-10
NSA 22001

Doc ID: 6789496

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

V. (U//~~FOUO~~) Potential Violation of NSA Minimization Procedures and Internal Policies

(U//~~FOUO~~) The investigation uncovered targeted telephone numbers that were at least reasonably likely associated with a USP [redacted] Because it is possible that this activity constitutes a violation of Title I and/or Title VII of the Foreign Intelligence Surveillance Act as a result of targeting telephone numbers used by USPs and/or persons in the United States that require preauthorization by the Foreign Intelligence Surveillance Court or the Attorney General, this matter has been referred to the Office of General Counsel (OGC).

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(~~C//SI//REL~~) FINDING: Some [redacted] practices increase the risk of mishandling USP [redacted] information and have the potential for abuse and misuse of the SIGINT collection system.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) RECOMMENDATION 1

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

a. **(U//~~FOUO~~) A risk assessment of [redacted] has been completed and a mitigation strategy has been developed and**

b. **(U//~~FOUO~~) Procedures are established to ensure that [redacted] are transparent, documented, and approved by SID management with the advice of the OGC.**

(ACTION: NSA Washington (NSAW)/SID Director, with OGC)

(U//FOUO) Accepted for action by:
(U) Target Completion Date:

(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

(U) RECOMMENDATION 2

(~~C//SI//REL~~) [redacted]

(ACTION: NSAW/SID Director, with OGC)

(U//FOUO) Accepted for action by:
(U) Target Completion Date:

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

[2] (~~C//SI//REL~~) [redacted]

Release 2022-10
NSA 22002

(b)(3)-P.L. 86-36
(b)(5)

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

(U) RECOMMENDATION 3

(U//~~FOUO~~)

(ACTION: NSAW/SID Director, with OGC)

(U//FOUO) Accepted for action by:
(U) Target Completion Date:

(U) RECOMMENDATION 4

(U//~~FOUO~~)

(ACTION: NSAW/SID Director)

(U//FOUO) Accepted for action by:
(U) Target Completion Date:

(U//~~FOUO~~) If you require clarification or additional information, please contact on 963-2623 (s) or by e-mail at

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

(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

George Ellard

DR. GEORGE ELLARD
Inspector General

(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.

Copy:
General Counsel
CLPO

Release 2022-10
NSA 22003

Doc ID: 6789496

APPENDIX B3

Summary Chart of Allegations, Data File References, And Technical Experts' Assessments of Data

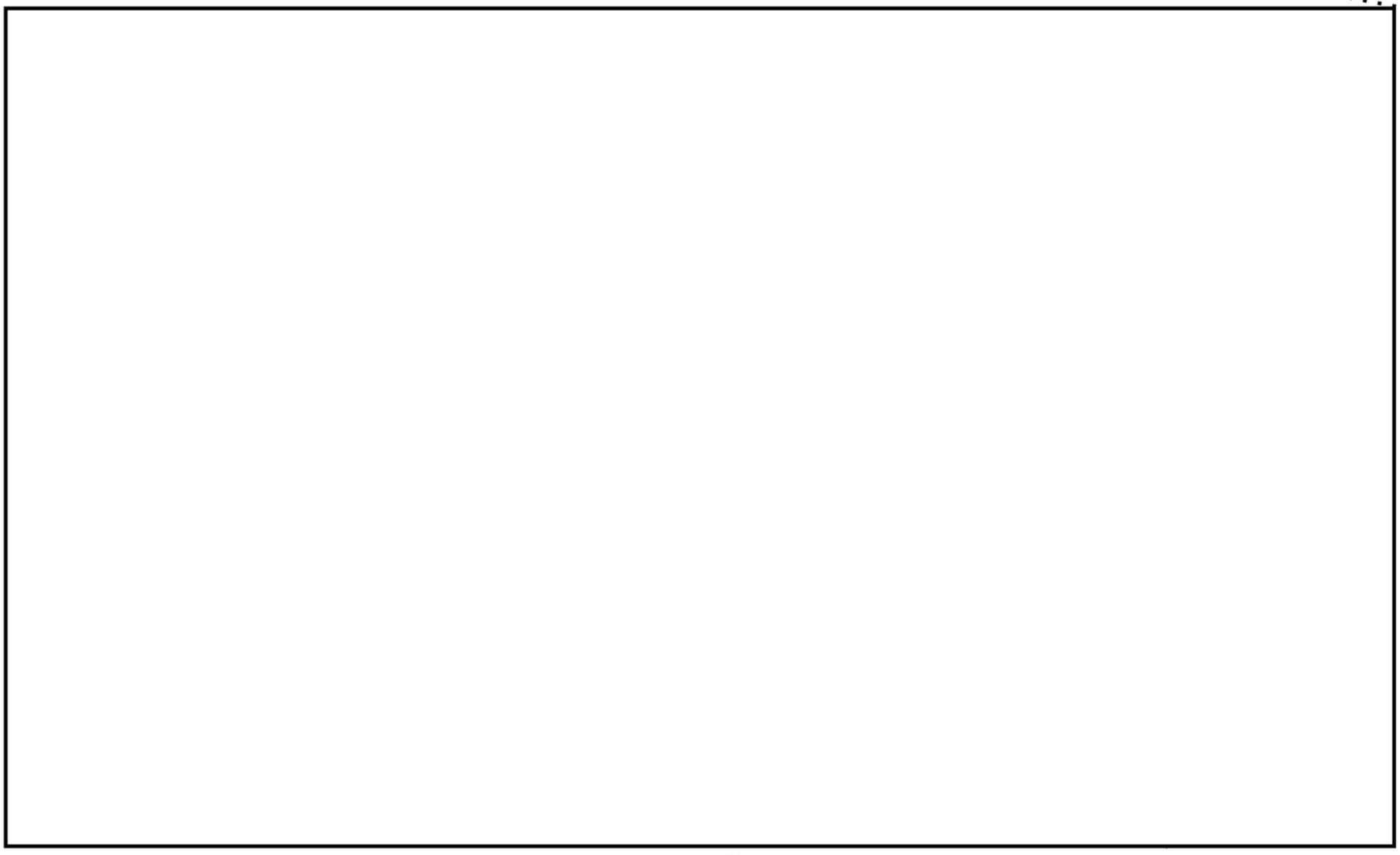
(b)(3)-P.L. 86-36

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20410201

Release 2022-10
NSA 22004

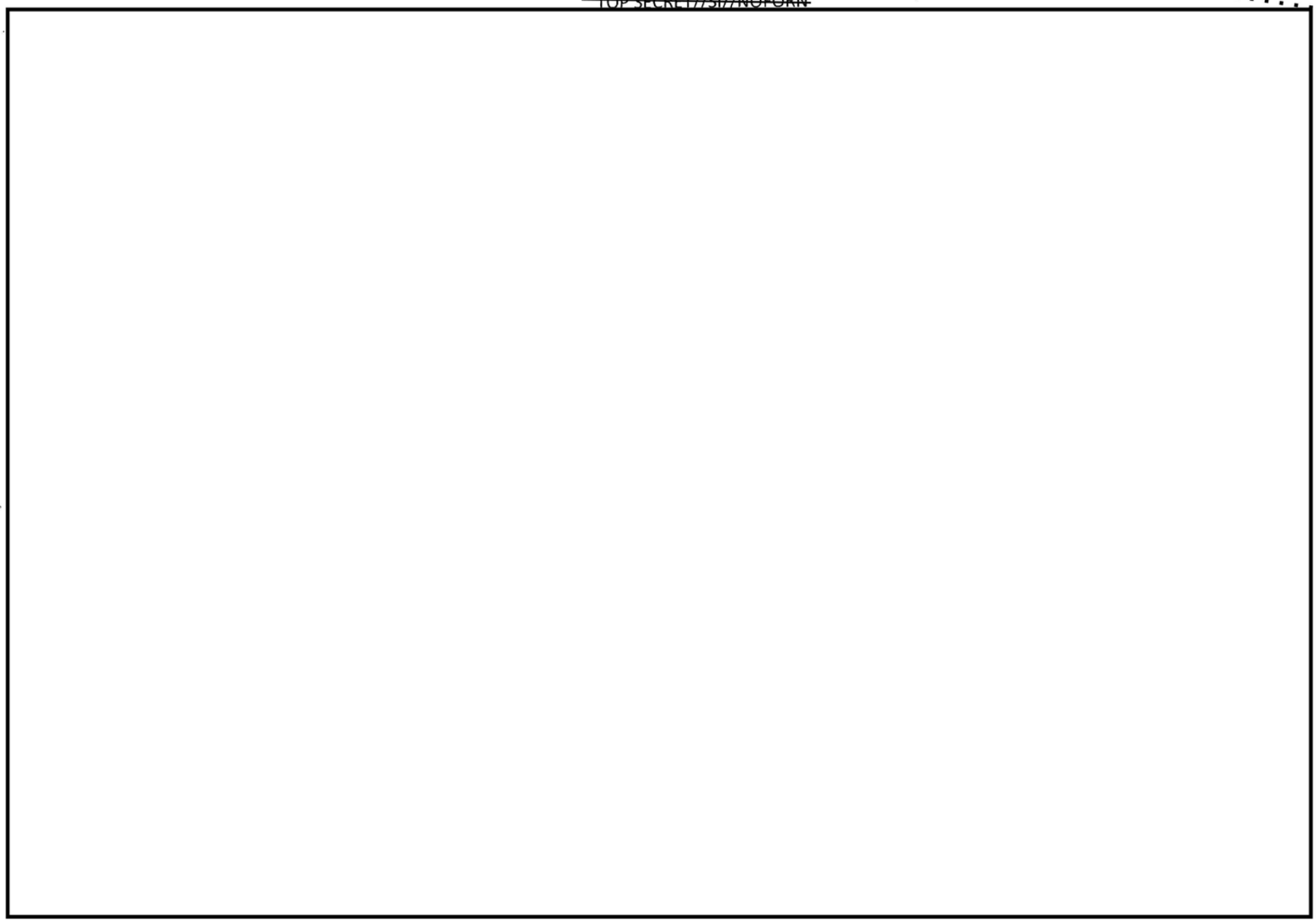
Doc ID: 6789496

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)



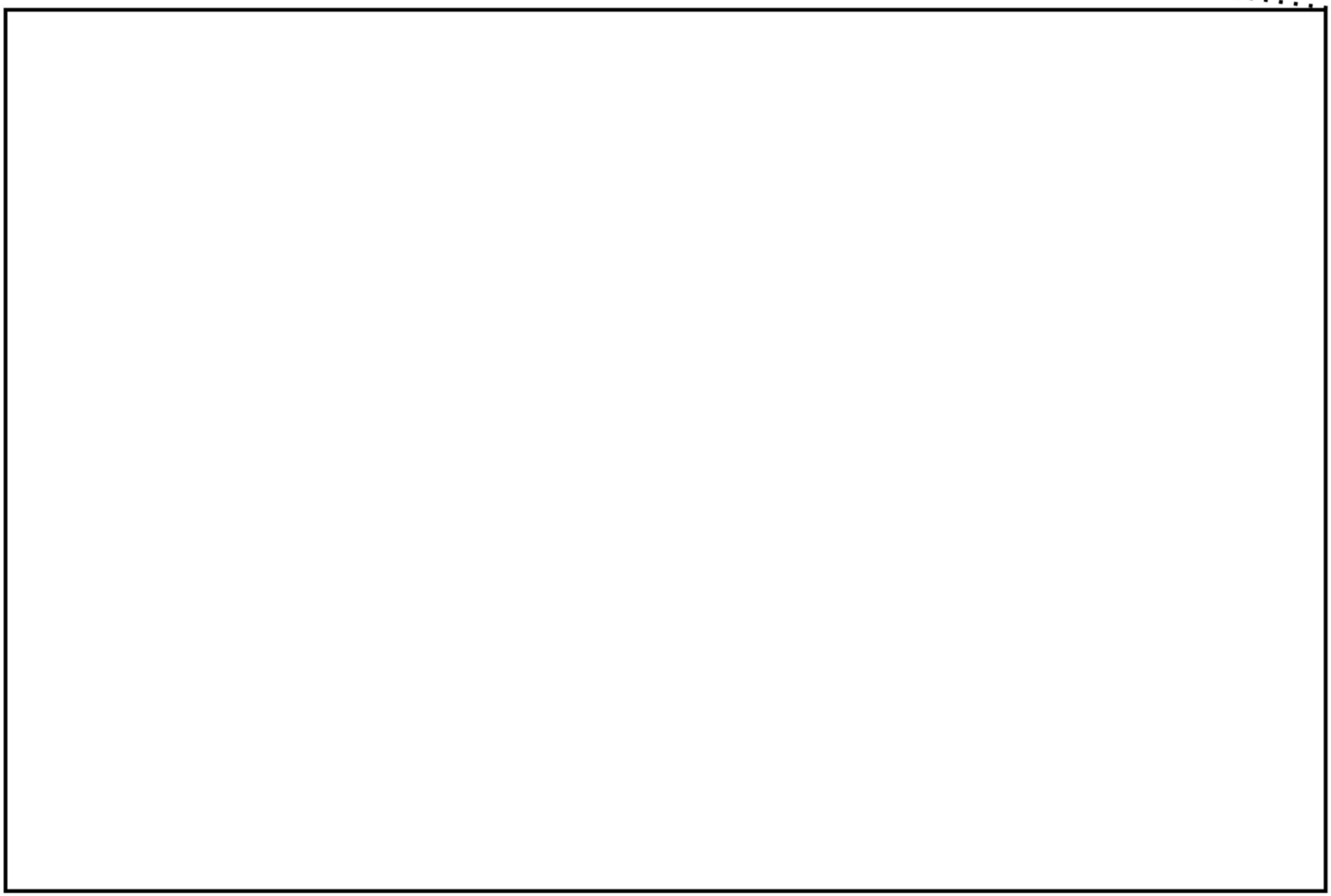
Release 2022-10
NSA 22005

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

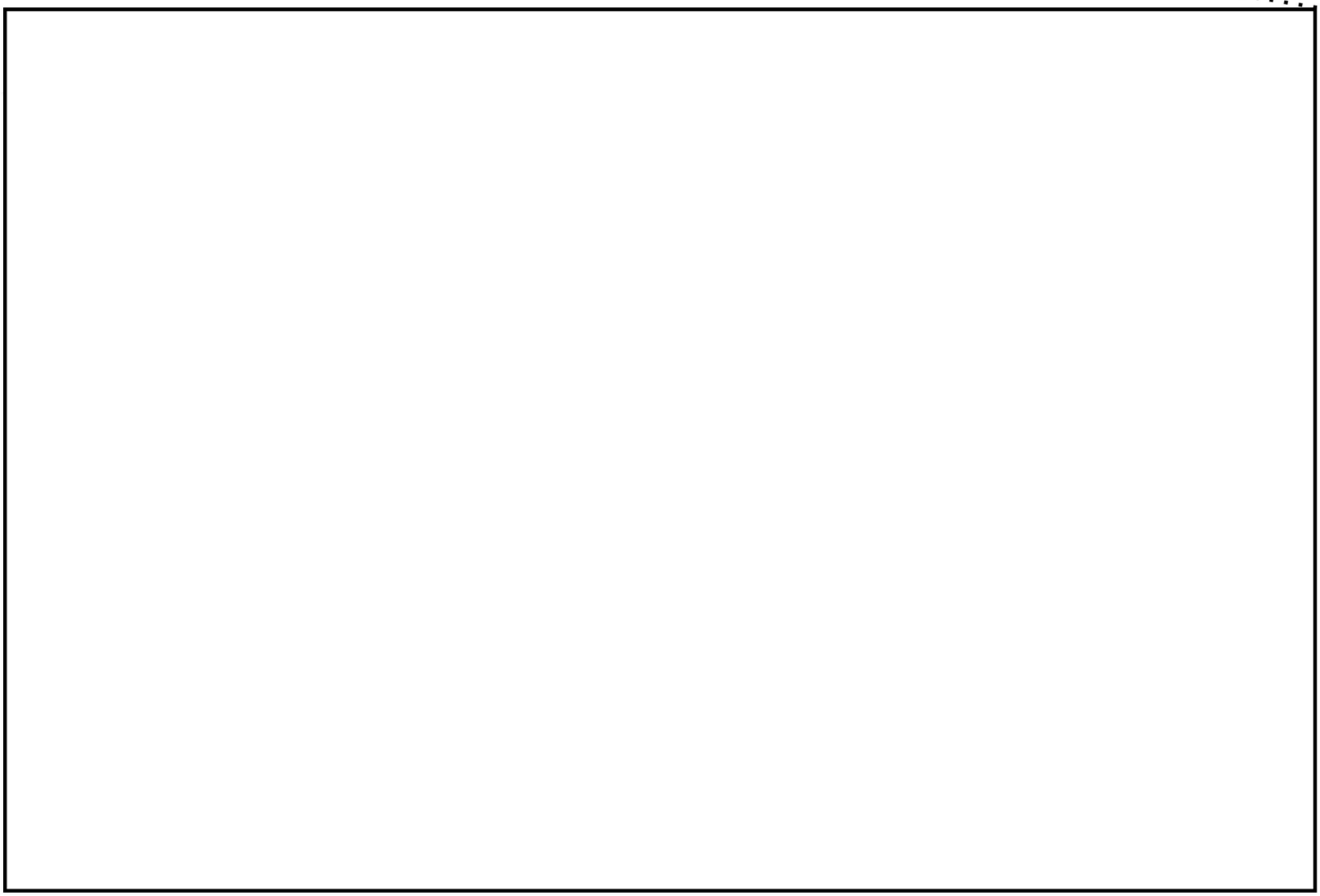


Release 2022-10
NSA 22006

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)



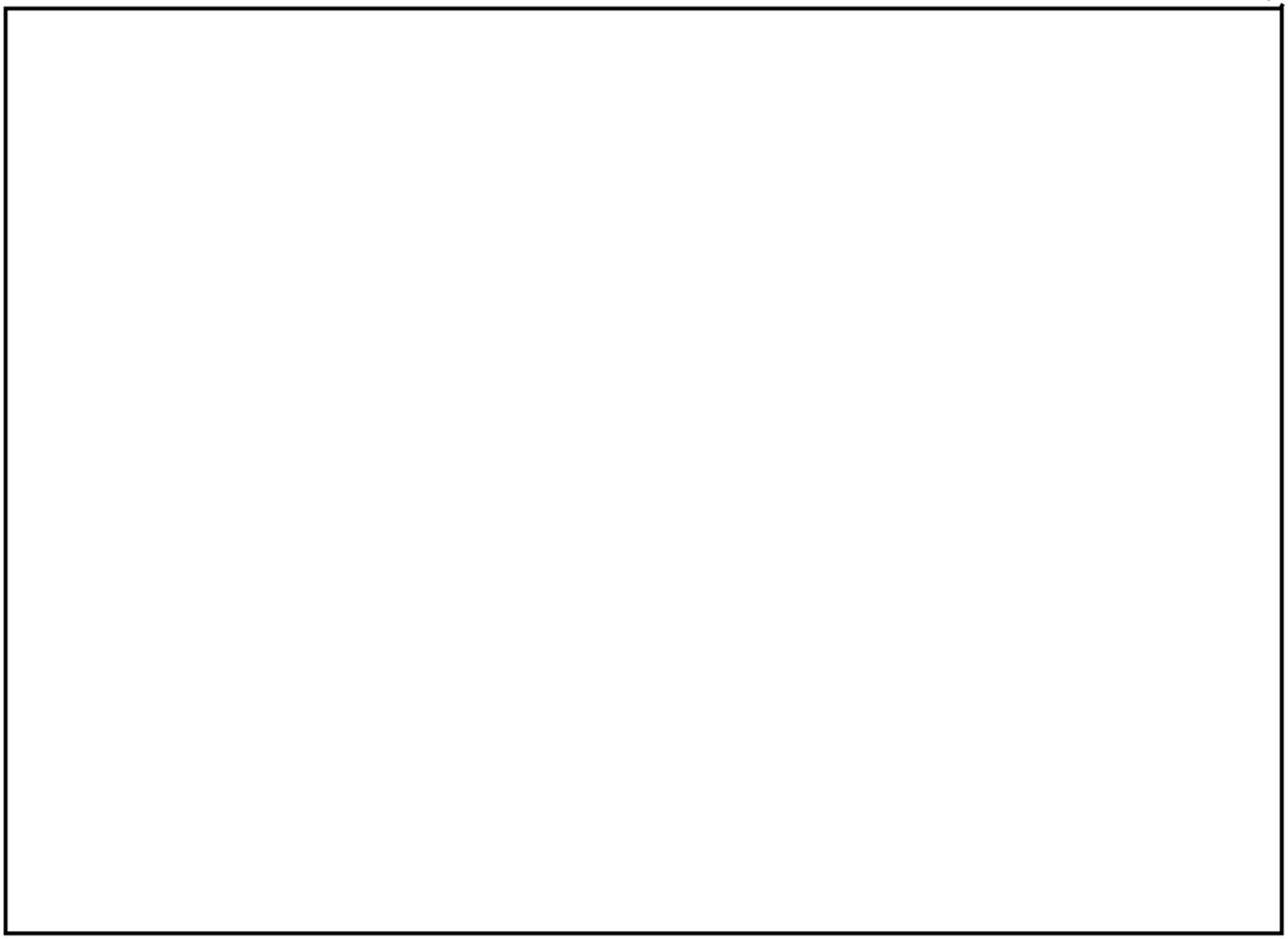
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)



Release 2022-10
NSA 22008

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

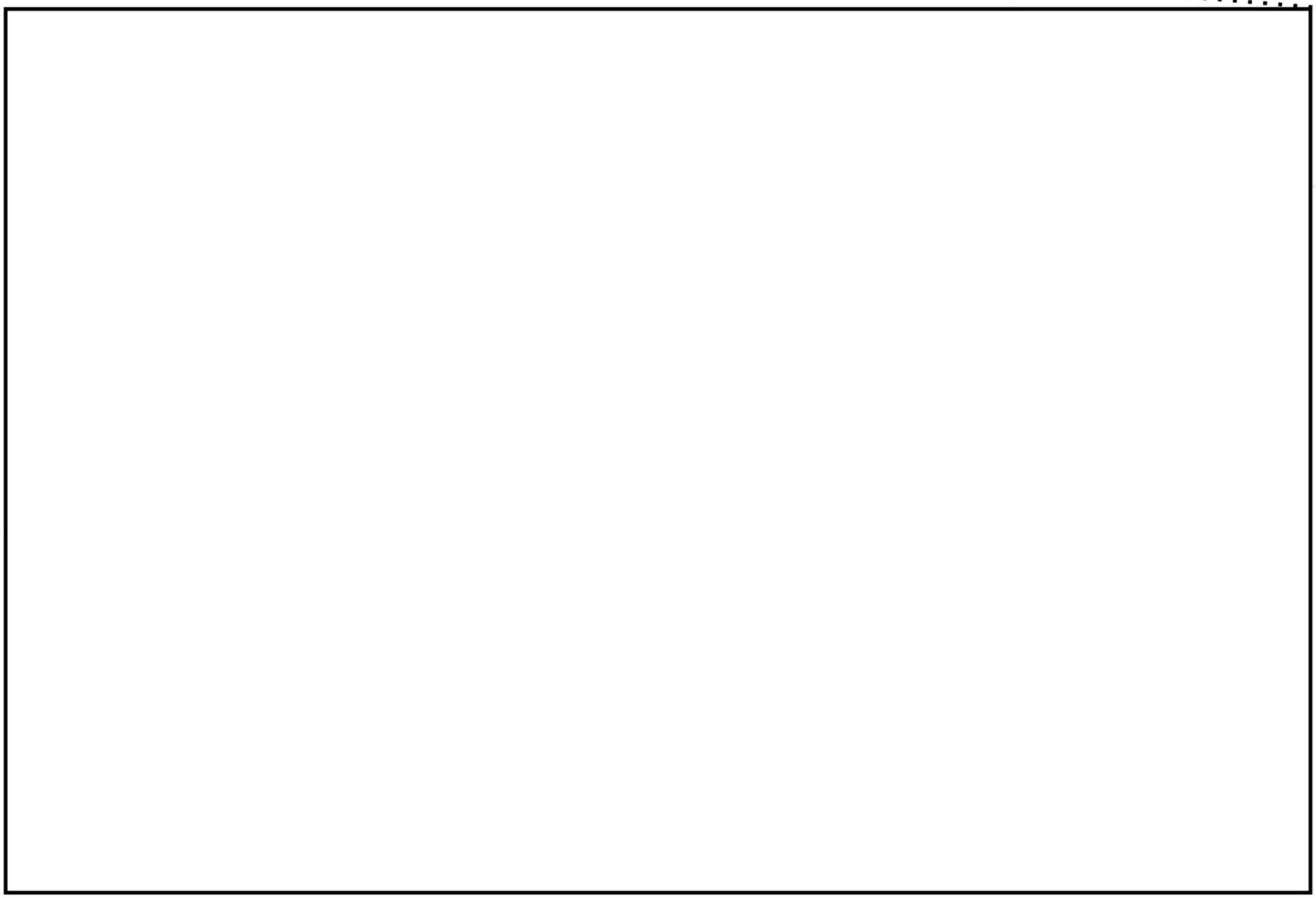
~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

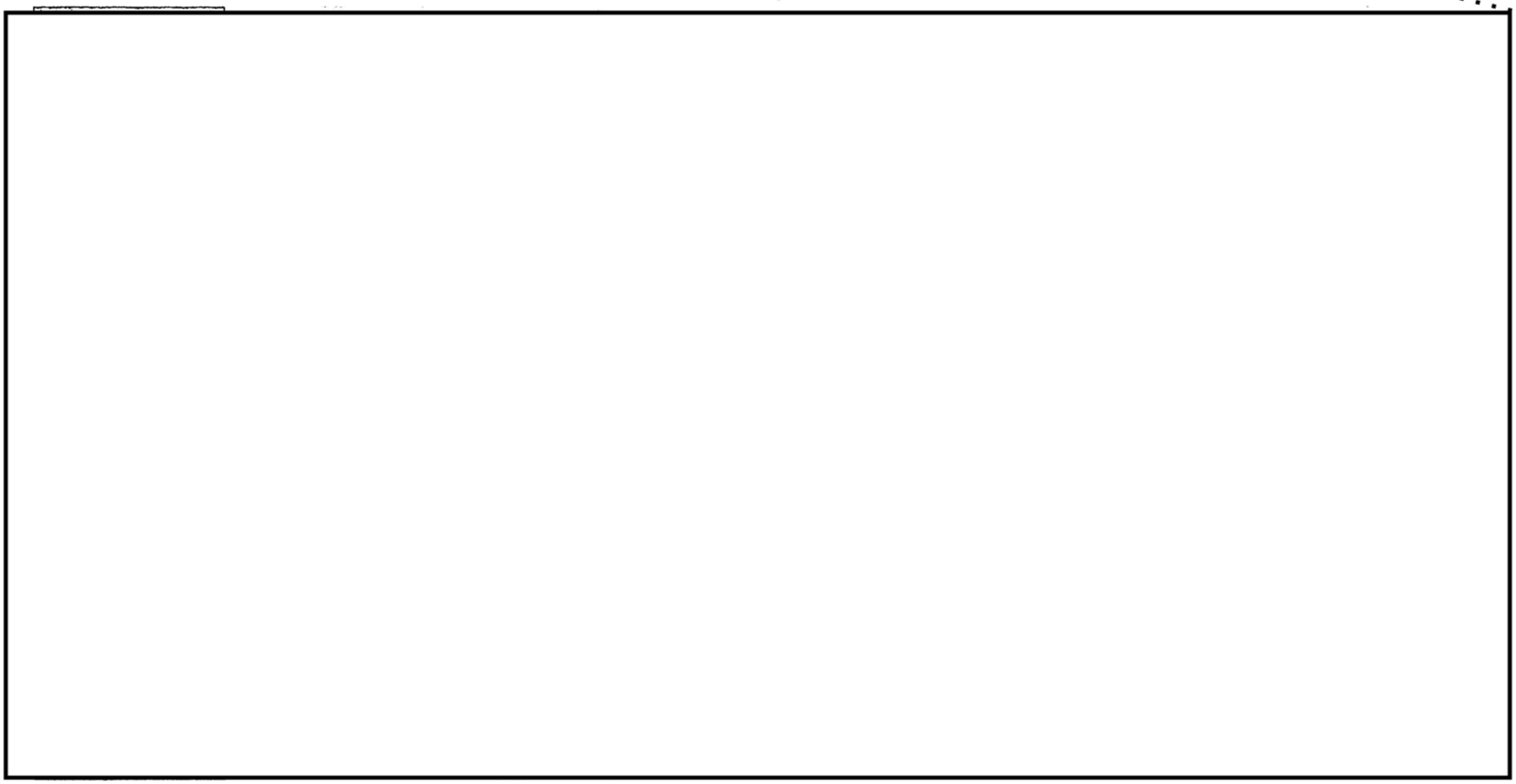
~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

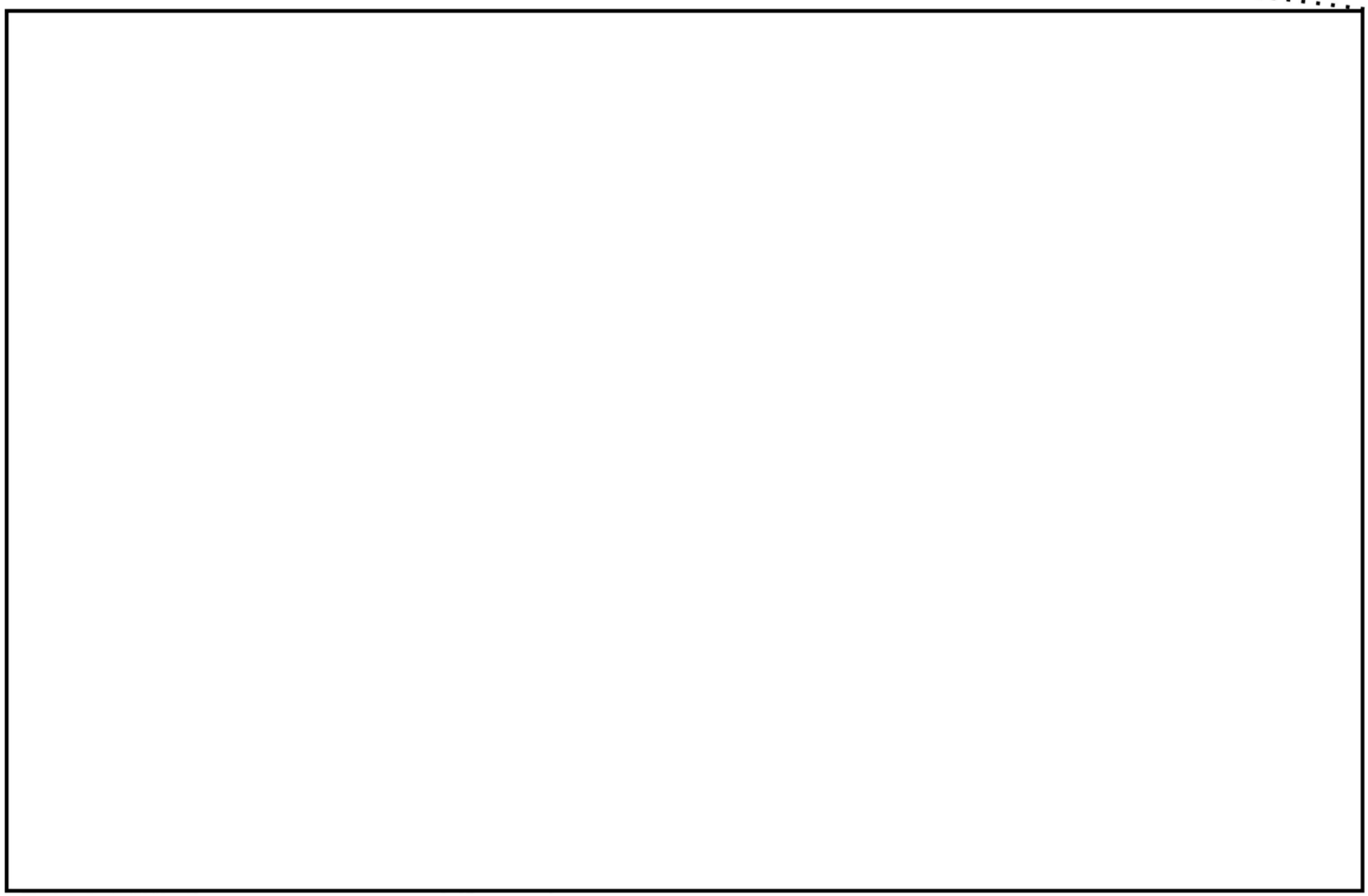
~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

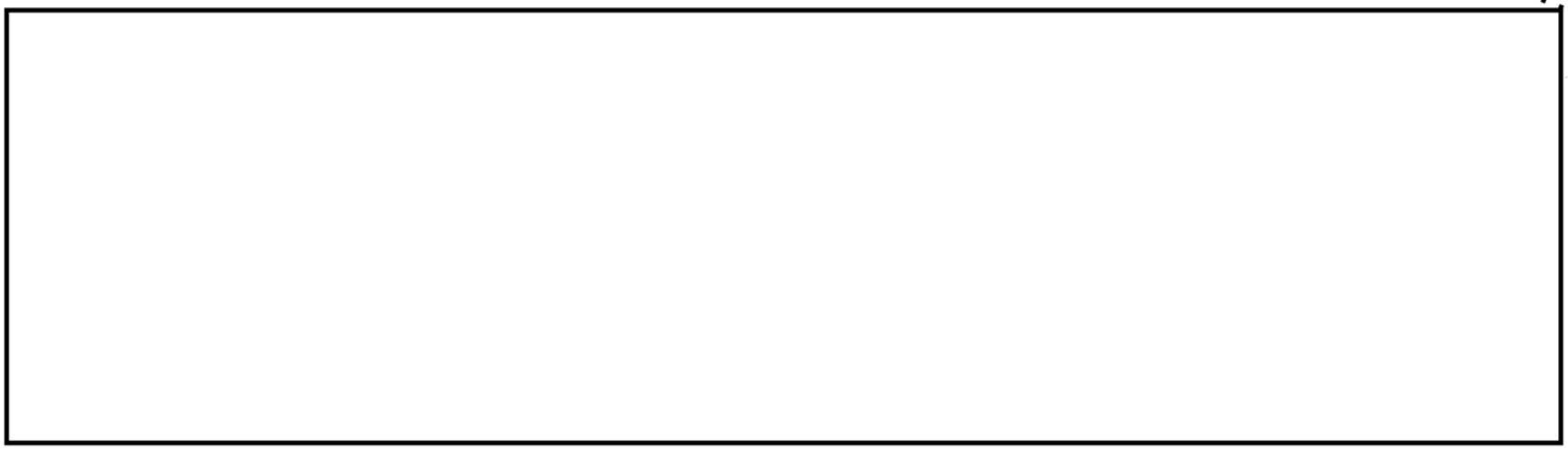
~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

~~TOP SECRET//SI//NOFORN~~



~~TOP SECRET//SI//NOFORN~~

APPENDIX N

[redacted] response to the OIG's tentative conclusion

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

Release 2022-10
NSA 22014

[redacted]

From: [redacted]
Sent: Friday, December 18, 2015 4:21 PM
To: [redacted]
Cc:
Subject: RE: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

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

Classification: ~~TOP SECRET//SI//NOFORN~~

I believe the conclusion is vague and misleading in parts. I never knowingly tasked a known USP [redacted] They were all, in the available context, unknowns which fit no known [redacted]

I take exception to this statement: ~~(S//SI//REL)~~ [redacted] resulted in [redacted] reasonably likely to result in the interception of communications to or from a USP [redacted]

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

At best the possibility was there, but not a probability which is how I interpret "reasonably likely."

~~(S//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

~~(TS//SI//NF)~~ [redacted]

Specific examples? What [redacted]

~~(TS//SI//NF)~~ [redacted] performed overly broad collection [redacted]

You have very specific data here. I've never seen it to comment on.

He stated that he [redacted]

Not possible. [redacted]

~~(TS//SI//NF)~~ [redacted]

Release 2022-10
NSA 22015

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

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

I am sure I know all of the witnesses as former colleagues for several years, and if they were so concerned they could have contacted me directly... before filing a formal complaint. As it was, when two of them did contact me, the grounds for hostile confrontation were well laid. As [redacted] said when I asked her who "we" were during the OGC meeting in July: [redacted] More than we have working some targets.

~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ Valid intelligence purpose? Yes, I believe so. The whole reason for starting this effort was to [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ This reminded me of a situation I had read about: [redacted]

That's enough; I'm just getting worked up and will ruin my holidays.

Good timing.

Release 2022-10
NSA 22016

==========

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

[redacted]

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

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

==========

From: [redacted]
Sent: Friday, December 18, 2015 3:42 PM
To: [redacted]
Cc: [redacted]
Subject: RE: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

Classification: ~~TOP SECRET//SI//NOFORN~~

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

[redacted]

(U//~~FOUO~~) I am personally unaware of any new allegations that have been filed against you.

(U//~~FOUO~~) At this time, I ask that you please confirm if you plan to provide any other information with regard to the tentative conclusion that I sent to you other than what you provided to me earlier this afternoon.

Thank you,

[redacted]

(U//~~FOUO~~) [redacted]
Senior Investigator
NSA/CSS OIG, Office of Investigations, D14
[redacted]

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

Release 2022-10
NSA 22017

From: [redacted]
Sent: Friday, December 18, 2015 3:35 PM
To: [redacted]
Cc: [redacted]
Subject: RE: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

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

Classification: ~~TOP SECRET//SI//NOFORN~~

[redacted]

(U) I'm going to add a little more:
Over the past few months my office chief asked me twice what I was doing regarding the "SIGDEV" effort.

- The first time I replied: nothing; it was shut down.
- He responded that he has a report that I "was at it again" (or words to that effect).
- I said: that's news to me; when and where is this happening?
  - There were no details.

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

(U) The second time was pretty much the same except I asked:

- OK, so if I *am* doing something, what of it?
- What is the problem?
  - No details.

~~(S//SI//REL)~~ [redacted]

(U) I never get any specifics to look into; just vague allegations. If something were going on recently, it could only be the result of old files not having been updated by more than a year (hard to imagine), or something else is going on (not hard to imagine; collection is a complex process). In any case, I'd like to understand what could possibly be the actual grounds for more allegations; what is triggering them… I'm assuming something was actually seen (Where? When?).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ Yesterday, for the first time in well over a year [redacted]

~~(S//SI//REL)~~ On the other hand, we have heard from [redacted]

(U) Having received your email today; [redacted] If someone else has a [redacted] fine… I will stay in this lane unless I am give written instructions to move out of it.

(U) That's my story.

==========

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

[redacted]

Release 2022-10
NSA 22018

[redacted]

[redacted]

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

==========

From: [redacted]
Sent: Friday, December 18, 2015 2:39 PM
To: [redacted]
Cc: [redacted]
Subject: RE: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

Classification: ~~TOP SECRET//SI//NOFORN~~

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]

The next step in the OIG's process is to give full consideration to the comments you provided. We will also include a copy of your response in our report of investigation. Please confirm if you plan to provide any other information other than what you have provided in your email, below. If so, I will keep the case open until 8 January 2016 (unless you require additional time). If no, I will proceed with finalizing the report and closing the case.

Thank you,

[redacted]

(U//~~FOUO~~) [redacted]
Senior Investigator
NSA/CSS OIG, Office of Investigations, D14
[redacted]

From: [redacted]
Sent: Friday, December 18, 2015 2:08 PM
To: [redacted]
Cc: [redacted]
Subject: RE: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

Classification: ~~TOP SECRET//SI//NOFORN~~

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

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

Release 2022-10
NSA 22019

[redacted]

I want to put this behind me as soon as possible.

All I will say is that it's a little short on specifics regarding where (in the collection environment) violations were found. You also fail to mention that the analysts contacted me with their concerns only weeks after they'd filed their complaints against me… some colleagues, eh?

Thank you for your efforts and HAGO,

So what's next?

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

==========

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

[redacted]

[redacted]

[redacted]

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

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

==========

From: [redacted]
Sent: Friday, December 18, 2015 1:45 PM
To: [redacted]
Cc: [redacted]
Subject: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

Classification: ~~TOP SECRET//SI//NOFORN~~

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]

Release 2022-10
NSA 22020

(U//~~FOUO~~) This is to notify you of the tentative conclusion that the Office of the Inspector General (OIG) reached in our investigation regarding an allegation that you misused the SIGINT system. Please see the attached document for our analysis and tentative conclusion.

(U//~~FOUO~~) In accordance with the investigative process, you now have the opportunity to comment on the tentative conclusion and/or offer additional information before we close our investigation. You are not required to respond with regard to our tentative conclusion. If you choose not to respond, please simply acknowledge receipt of this notification. However, if you choose to respond, please do so in writing by 1700 hours, 8 January 2016. Any comments and/or additional information you provide will be given full consideration in reaching our final conclusion. If you require additional time or have any questions, please let me know.

(U//~~FOUO~~) [redacted]
Senior Investigator
NSA/CSS OIG, Office of Investigations, D14
[redacted]

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 200130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 200130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

Classified By: [redacted]
Derived From: NSA/CSSM 1-52

Release 2022-10
NSA 22021

Dated: 20130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 200130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

---

[1] (U//~~FOUO~~) EO 12333, §1.7(c) states that NSA shall conduct its SIGINT activities "for foreign intelligence and counterintelligence purposes to support national and departmental missions."

Release 2022-10
NSA 22022

[redacted]

From: [redacted]
Sent: Monday, December 21, 2015 12:28 PM
To: [redacted]
Cc:
Subject: RE: (U) IV-13-0077 Notification of Investigative Tentative Conclusion
Attachments: IV-13-0077 OIG Tentative Conclusion 20151218 (3)-reply..docx

Classification: ~~TOP SECRET//SI//NOFORN~~

[redacted]

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

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

Final comments attached in red in text.

HAGO,

==========

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

[redacted]

[redacted]

[redacted]

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

==========

From: [redacted]
Sent: Friday, December 18, 2015 1:45 PM
To: [redacted]
Cc: [redacted]
Subject: (U) IV-13-0077 Notification of Investigative Tentative Conclusion

Classification: ~~TOP SECRET//SI//NOFORN~~

Release 2022-10
NSA 22023

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

[redacted]

(U//~~FOUO~~) This is to notify you of the tentative conclusion that the Office of the Inspector General (OIG) reached in our investigation regarding an allegation that you misused the SIGINT system. Please see the attached document for our analysis and tentative conclusion.

(U//~~FOUO~~) In accordance with the investigative process, you now have the opportunity to comment on the tentative conclusion and/or offer additional information before we close our investigation. You are not required to respond with regard to our tentative conclusion. If you choose not to respond, please simply acknowledge receipt of this notification. However, if you choose to respond, please do so in writing by 1700 hours, 8 January 2016. Any comments and/or additional information you provide will be given full consideration in reaching our final conclusion. If you require additional time or have any questions, please let me know.

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

(U//~~FOUO~~) [redacted]
Senior Investigator
NSA/CSS OIG, Office of Investigations, D14
[redacted]

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

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 200130930
Declassify On: 20401201

Classification: ~~TOP SECRET//SI//NOFORN~~

Release 2022-10
NSA 22024

(U//~~FOUO~~) ANALYSIS AND TENTATIVE CONCLUSION OF OIG INVESTIGATION IV-13-0077 – [redacted]

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

(U) **DoD 5240.1-R** implements DoD Directive 5240.01 and EO 12333, Section 2.3. This regulation contains the Attorney General-approved procedures for all DoD IC components and has a classified annex that governs SIGINT activities.[1] The Classified Annex to DoD 5240.1-R states that communications of or concerning USPs may be intercepted intentionally or selected deliberately only under certain specific circumstances. The Classified Annex requires the Director of NSA (DIRNSA), or his designee, to issue directives and instructions implementing the procedures found in the Classified Annex. USSID SP0018 is the Agency directive that implements the classified annex.[2]

(U//~~FOUO~~) **NSA/CSS Policy 1-23**, paragraph 1, states that NSA/CSS shall collect, process, retain, and disseminate information about USPs only as prescribed in DoD Directive 5240.1, DoD 5240.1-R and its Classified Annex, and the Foreign Intelligence Surveillance Act (FISA). Paragraph 3 states that the SIGINT mission of the NSA/CSS is to collect, process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions. Paragraph 3 also states that NSA/CSS shall intentionally collect only foreign communications and shall not intentionally collect U.S. person communications without proper legal authorization.

(U//~~FOUO~~) **USSID SP0018** § 3.1 also states that it is the policy of the U.S. SIGINT System (USSS) to target or collect only foreign communications and the USSS will not intentionally collect communications of or about USPs or persons or entities in the United States, except as set forth in USSID SP0018.[3]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(S//SI//REL)~~ **USSID SP0018** § 4.1 states that communications known to be to, from, or about a USP, [redacted], will not be intentionally intercepted, or selected through the use of a selection term, except in certain specified instances with the approval of the Foreign Intelligence Surveillance Court (FISC), the Attorney General, or DIRNSA. USSID SP0018 § 4.1(c)(5) also states that voice and facsimile communications with one communicant in the United States may be targeted for collection only with the prior approval of DIRNSA (when the approval of the Attorney General or the FISC is not required[4]) if technical devices (e.g., [redacted]) are employed that limit acquisition by

---

[1] (U) DoD 5240.1-R and its Classified Annex were approved by the Attorney General prior to the creation of the Director of National Intelligence and the requirement for consultation with the Director of National Intelligence.

[2] (U//~~FOUO~~) USSID SP0018 incorporates the requirements of all the higher level authorities listed above; so compliance with USSID SP0018 generally ensures compliance with those higher level authorities. A violation of USSID SP0018, however, does not necessarily result in a violation of a higher level authority. In cases of noncompliance with USSID SP0018, the misconduct must also be examined against the requirements of the higher level authorities to determine whether additional violations have occurred.

[3] (U) In accordance with USSID SP0018, section 9.18.e., a person known to be currently in the United States will be treated as a USP unless that person is reasonably identified as a non-USP or circumstances give rise to a reasonable belief that such person is not a USP. A person known to be outside the United States, or whose location is not known, will not be treated as a USP unless such person is reasonably identified as such or circumstances give rise to a reasonable belief that such person is a USP.

[4] (U) FISA requires FISC authorization for the acquisition of the contents of wire communications to or from a person in the United States, without consent, if such acquisition occurs in the United States. 50 U.S.C. 1801(f)(2).

Release 2022-10
NSA 22025

the NSA to communications when the target is a non-USP outside the United States [redacted][5]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI)~~ **USSID DA3511** states that the [redacted]

[redacted]

~~(S//SI//REL)~~ Accordingly, SIGINT collection is permissible only if it is reasonably designed not to intentionally target communications of or about USPs, or persons in the United States, unless targeting a specific USP or person in the United States pursuant to the prior approval of the FISC, Attorney General, or DIRNSA.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ [redacted]

[redacted]

~~(S//SI//REL)~~ [redacted] activities violated these restrictions. [redacted]

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

his activities did in fact target and collect such communications.

(U) Not true. Any collection of USPs was incidental.

~~(S//SI//REL)~~ [redacted] told the OIG that he started his own project in 2012. [redacted]

[redacted]

~~(S//SI//REL)~~ [redacted]

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

[5] ~~(S//SI//REL)~~ The Classified Annex has similar provisions in § 4.A.1. Thus, a violation of § 4 of USSID SP0018 would also result in a violation of the Classified Annex, DoD 5240.1-R, DoDD 5240.01, NSA/CSS Policy 1-23, and EO 12333.

[6] ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(S//SI//REL)~~ Not exactly correct. [redacted]

[redacted]

[redacted]

~~(S//SI//REL)~~ As I stated in interviews and recapped in an earlier email, the results were that the [redacted]

~~(S//SI//REL)~~ [redacted] Well-established procedures exist to request and document exceptions to these safeguards when validated foreign intelligence needs necessitate the targeting and collection of U.S. selectors.

~~(TS//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(S//SI//REL)~~ I repeat, I never knowingly, intentionally tasked USP [redacted]

~~(S//SI//REL)~~ [redacted] resulted in [redacted] reasonably likely to result in the interception of communications to or from a USP [redacted]

~~(S//SI//REL)~~ Stating that something is reasonably likely is not proof it actually happened and [redacted] was never the intent.

~~(S//SI//REL)~~ [redacted]

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

Release 2022-10
NSA 22027

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

~~(S//SI//REL)~~

- ~~(TS//SI//NF)~~

~~(S//SI//REL)~~ This I really need to see to be able to put any context on it. Right now I see this as only an unsubstantiated statement.

- ~~(TS//SI//NF)~~

(U) Undoubtably? Based on what?

~~(TS//SI//NF)~~ Although told the OIG that he was completely sure that he had never the evidence shows that he did.

(U) Ditto.

He told the OIG in an email that he was going to

(U) Absolutely. Taken out of context they were

Further, during his testimony

(U) Not accurate. The comments were entered into

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~(TS//SI//NF)~~

~~(S//SI//REL)~~ IMO this is a stretch.

Release 2022-10
NSA 22028

[redacted]

~~(S//SI//REL)~~ I do recall somebody contacting me about a potential problem [redacted]

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) Ditto

[redacted]

~~(S//SI//REL)~~ I totally do not recall an instance like this. [redacted]

[redacted]

~~(S//SI//REL)~~ T[redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted] contends that his activity was compliant and he did not task U.S. selectors or collect USP [redacted]

~~(S//SI//REL)~~ I still do. USP [redacted] were never knowingly, intentionally subjected to study.

We disagree. [redacted]

[redacted]

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

~~(S//SI//REL)~~ The request would have been [redacted]

[redacted]

~~(S//SI//REL)~~ Furthermore, because [redacted] did not report and cease the non-compliant activity combined with the above described activities, he violated USSID SP0019 §3.6 which states:

> ...every individual must comply with applicable laws, statutes, directive, and regulations by: reporting any non-compliant activity to management, an IOO, SV, and OIG; taking measures to reduce the risk of non-compliant activity and to prevent future non-compliant

Release 2022-10
NSA 22029

activity; and exercising due diligence to remain compliant, i.e., make every reasonable attempt to adhere to the rules and standards.

(U//~~FOUO~~) Section 4.8 of USSID SP0019 defines reportable activity and non-compliant activity as including mishandling of U.S. persons information and queries against raw SIGINT data that are inadvertently, intentionally, or carelessly likely to target or retrieve United States or Second Party communications. Section 4.10 states that, when non-compliant activities are detected, the activity that caused the non-compliant situation must be stopped immediately and the situation closely monitored to verify that the problem has been resolved.

(U) The activity was stopped when someone with the authority to say so spoke up.

(U//~~FOUO~~)

~~(S//SI//NF)~~ Signals Intelligence Directorate

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(S//SI//REL)~~ were reasonably likely to result in the interception of communications of or about

taskings, therefore, violated

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) We've discussed this.

(U//~~FOUO~~) Foreign Intelligence Purpose

[7] (U)
[8] ~~(S//NF)~~

Release 2022-10
NSA 22030

~~(S//SI//REL)~~ Many witnesses questioned whether [redacted] had a valid foreign intelligence purpose for his activities.[9] Some witnesses were willing to accept that NSA had a foreign intelligence purpose [redacted] however, they were unsure whether [redacted] activities complied with laws and regulations because they had difficulty understanding his complex and technical work. Other witnesses agreed that [redacted]

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

~~(S//SI//REL)~~ [redacted]

(U//~~FOUO~~) The OIG concludes that determining whether [redacted] had a valid foreign intelligence purpose for each of his activities is unnecessary because, even assuming that he did, he failed to comply with the authorities that apply to SIGINT activities that target and collect USP [redacted]

~~(TS//SI//REL)~~ [redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

[redacted]

(U) Quite simply I did not know who to coordinate with or that it would be necessary.

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

(U//~~FOUO~~) Although in hindsight [redacted] actions seem egregious, they must be considered in context of the conflicting guidance he was given. At various times, [redacted] was told by different supervisors, oversight officials, and attorneys that his activities were acceptable but was told by others to immediately stop. Many officials involved in trying to determine what

[9] (U//~~FOUO~~) EO 12333, §1.7(c) states that NSA shall conduct its SIGINT activities "for foreign intelligence and counterintelligence purposes to support national and departmental missions."
[10] (U//~~FOUO~~) USSID4000 was superseded by SID Implementing Directive, Annex F, *Governance of the Signals Intelligence Mission*, 25 February 2013.

Release 2022-10
NSA 22031

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

was doing and whether he had violated policies or regulations relied on explanations or on other officials involved in the matter because they did not fully understand the technical details of project.

~~(S//REL)~~ The OIG found that, even if was truly unaware that he had tasked and collected USP and whether or not his management or officials responsible for intelligence oversight directed to stop his project due to non-compliant activity, acted with reckless disregard of the regulations, policies, and procedures that govern the use of the SIGINT system when he started his project and continued to work on it.

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

~~(S//SI//REL)~~ Until told to stop by someone with the authority to do so.

~~(TS//SI//REL)~~ is an experienced analyst who has worked for more than He touts himself as the longest-serving in the Intelligence Community. acknowledged to the OIG that he had been proceeding with his project in a "kind of [by the] seat of the pants" mode and that his project was somewhat dangerous and unknown territory. He said that he had not trained anyone else on the techniques of his project because he did not want anyone to end up in trouble, if it was determined that the project was not appropriate. acknowledged that he needed guidance He also told the OIG that his project may not be worth documenting except "as a bad choice of judgment."

(b) (6)

~~(TS//SI//REL)~~ Based on his technical knowledge, experience, and self-awareness that his project was, at minimum, questionable, was careless and exercised poor judgment when he started his project without having his project officially and completely vetted through his management chain and the Agency offices responsible for oversight of such activities, such as SV and OGC.

(U) Well now I know better. I also have NO intention of getting involved in this again. Period.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//REL)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (6)

~~(S//SI//REL)~~ No one "exploited" anything intentionally.

~~(TS//SI//REL)~~ Although contends that his activity was compliant and he did not task U.S. selectors or collect USP the OIG found that had tasked and collected on USP an analyst with extensive experience in and trained on the use of and rules pertaining to the SIGINT system, knew or should have known that his taskings resulted in or were likely to result

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

in the interception of communications to or from USPs [redacted] without the requisite prior approvals.

~~(S//SI//REL)~~ [redacted]

~~(TS//SI//REL)~~ **TENTATIVE CONCLUSION**: Substantiated. [redacted] His activities resulted in, or were reasonably likely to result in, the unauthorized collection of communications to or from USPs or persons in the United States, or both. The preponderance of the evidence supports the conclusion that, by doing so, [redacted] violated the classified annex of DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, NSA/CSS Policy 1-23, and United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and U.S. Minimization Procedures*.

~~(S//SI//REL)~~ IMO not substantiated: there are no facts here that identify any USP numbers [redacted]

~~(TS//SI//REL)~~ In addition, [redacted] violated the United States Signals Intelligence Directive (USSID) SP0019, *NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy,* when he carelessly performed activities likely to target and retrieve United States Person [redacted] communications. [redacted] also violated USSID DA3511, *Data Acquisition Directorate and Data Flow Management*, when he [redacted]

~~(S//SI//REL)~~ Also not substantiated. [redacted]

~~(TS//SI//REL)~~ Finally, the preponderance of the evidence supports the conclusion that [redacted] violated [redacted] and USSID SP0019 when he [redacted] effected collection that resulted or was reasonably likely to result in the unauthorized collection of communications to or from [redacted][12]

~~(S//SI//REL)~~ I repeat, no [redacted] were knowingly or intentionally targeted. I am not sure how these Conclusions are supposed to read, but I found this heavy on conclusion based apparently on hearsay with no real examples to back up the most damning statements.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

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

[11] (U//~~FOUO~~) The overarching authorities [redacted] violated are Executive Order (EO) 12333, *United States Intelligence Activities*, and Department of Defense (DoD) Directive 5240.01, *DoD Intelligence Activities*.

[12] (U) [redacted]

Release 2022-10
NSA 22033