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

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

18 June 2014

IV-14-0011

Possible USSID 18 Violation

(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.

~~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.

I. (U) SUMMARY

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

~~(TS//SI//REL)~~ On 8 January 2013, [redacted] Intelligence Oversight Officer, [redacted] contacted the NSA/CSS Office of Inspector General (OIG) and stated that in October 2012, he conducted a test of the [redacted] using an overly broad search term which resulted in the retrieval of United States Person (USP) communications. [redacted] immediately reported the incident to his leadership and filed an incident report with Oversight and Compliance (SV).

(U//~~FOUO~~) In addition to obtaining sworn testimony from [redacted] we conducted an interview of his immediate supervisor at the time of the incident. We also obtained all pertinent records from SV.

~~(TS//SI//REL)~~ The preponderance of the evidence supports the conclusion that [redacted] violated EO12333, DoD 5240.1-R, and USSID SP0018 when he intentionally used a selection term, [redacted] which resulted in the retrieval of USP communications.

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

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

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

Classified By [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20390201~~

II. (U) BACKGROUND

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

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

(b) (6)

(U) Introduction

~~(TS//SI//REL)~~ entered on duty with the NSA in He began working on the in In January 2012, he was involved in an incident where USP information was inadvertently obtained After the incident, which was reported to SV,

~~(TS//SI//REL)~~ Despite being told otherwise, In October 2012, he an overly broad search term, in a query which resulted in the retrieval of USP information. He immediately filed an incident report and contacted his management.

(U) Applicable Authorities

(U) Below is a listing of citations. Refer to Appendix A for a full Table of Authorities.

- EO 12333 – United States Intelligence Activities
- DoD Directive 5240.1-R – Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons
- USSID SP0018 – Legal Compliance and U.S. Persons Minimization Procedures

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

III. (U) FINDINGS

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

(U//~~FOUO~~) ALLEGATION: Did [redacted] intentionally use a selection term that was reasonably likely to result in the interception of communications to or from a USP?

*(U//~~FOUO~~) **CONCLUSION:** Substantiated. The preponderance of the evidence supports the conclusion that [redacted] intentionally used a selection term that was reasonably likely to result in the interception of communications to or from a USP, in violation of EO 12333, Part 2.3, DoD 5240.1-R, Chapter 2, Procedures 2.3.1-2.3.4.2, Chapter 14, Procedure 14, C14.2.1,and USSID SP0018, §3.1,4.1, & 5.1(a).*

(U) Documentary Evidence

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

(U) **NSA/CSS Intelligence-Related Incident Report [redacted]**

~~(TS//SI//REL)~~ This incident report, completed by [redacted] summarizes the event that occurred on 17 October 2012 when [redacted] The entire incident report is located in Appendix B.

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

(U) [redacted] **Training Record**

(U//~~FOUO~~) [redacted] training record revealed that, prior to 17 October 2012, he took numerous courses regarding SIGINT authorities including:

[redacted]

(b) (6)

-OIAC1180 Annual IA Awareness Training (Most recent date of completion prior to the October 2012 incident: 4 September 2012)

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

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

(U) Testimonial Evidence

(U//~~FOUO~~)

(U//~~FOUO~~) On 15 March 2013, Intelligence Oversight Officer was interviewed by D14 Senior Investigator, as part of a separate investigation, and provided the following information.

(~~TS//SI//NF~~) After the January 2012 incident where USP communications were inadvertently obtained

(U//~~FOUO~~) On 23 and 24 October 2013, Intelligence Oversight Officer, was interviewed and provided the following sworn testimony.

(~~TS//SI//NF~~) In January 2012, was involved in an incident where USP information was inadvertently obtained This incident occurred

and an incident report was filed on 31 January 2012.

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

(~~TS//SI//REL~~) decided that

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

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

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

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

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

IV-14-0011

[redacted] resulted in USP information, [redacted] immediately filed and incident report [redacted], dated 17 October 2012.

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

~~(TS//SI//NF)~~ [redacted] asserted that he did not intentionally search for USP information, [redacted]

(U//~~FOUO~~) [redacted] (b) (3)-P.L. 86-36

(U//~~FOUO~~) On 4 February 2014, [redacted] was interviewed and provided the following sworn information.

~~(TS//SI//NF)~~ [redacted] was [redacted] supervisor in October 2012 when the incident occurred. [redacted] had become increasingly frustrated with the lack of audit controls in the [redacted] added that [redacted] was a very good analyst and a solid performer and that his intent when conducting the query was not malicious.

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

(U) Analysis and Conclusions

~~(TS//SI//NF)~~ According to Executive Order 12333 Part 2.3, elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with established procedures. DoD Directive 5240.1-R, Chapter 2, Procedure 2, C2.3.4.2 states that information that identifies a USP, may only be collected under certain circumstances. Additionally, Chapter 14, Procedure 14, C14.2.1 states, "employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333…and this Regulation." According to USSID SPOO18, §3.1 & 4.1, the United States SIGINT System will not intentionally collect communications to, from, or about USPs. Further, §5.1 (a) states, "No selection term that is reasonably likely to result in the interception of communications to or from a [USP]…may be used unless there is a reason to believe that foreign intelligence will be obtained from the use of such a selection

term." [redacted] is, and was at the time of the incident, an Intelligence Oversight Officer (IOO) who has completed numerous courses on the applicable regulations. The SV website describes IOO's as the "SIGINT compliance experts in the extended enterprise who help ensure NSA operates compliantly within its SIGINT Authorities." Therefore, by virtue of his training and experience as a SIGINT compliance expert, [redacted] was aware of the regulations and the prohibitions regarding using overly broad search terms and conducting queries that would reasonably be likely to result in USP communication.

~~(TS//SI//NF)~~ In his first account of the incident, documented on the incident report [redacted]

[redacted] testimony that his intention was to show that the database was in compliance with regulations and did not contain USP information is not reasonable.

(U//~~FOUO~~) Although [redacted] made attempts to report what he believed to be a non-compliant SIGINT system to the proper authorities, the fact that he disagreed with their conclusions does not justify using an overbroad search term, in violation of policy, to prove them wrong. The preponderance of the evidence supports the conclusion that [redacted] intentionally used a selection term that was reasonably likely to result in the interception of communications to or from a USP, in violation of EO1233 Part 2.3, DoD 5240.1-R, Chapter 2, Procedures 2.3.1-2.3.4.2, Chapter 14, Procedure 14, C14.2.1, and USSID SPOO18, §3.1, 4.1, & 5.1(a).

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

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

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

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

(U//~~FOUO~~) [redacted] responded to the tentative conclusions with the following statement:

~~(TS//SI//NF)~~ After reading these conclusions I am concerned that a significant contributory factor has not been cited. [redacted]

~~(TS//SI//NF)~~ To help illustrate my point, I would ask the following two questions: [redacted]

~~(TS//SI//NF)~~ At the time of the incident, nobody could answer those two questions. [redacted]

(U//~~FOUO~~) Auditing is defined under USSID SPOO19 as, *"The process USSS elements and overseers use to review queries made against unevaluated, unminimized (raw) SIGINT data or repositories to ensure that the queries are compliant with U.S. laws and procedures that govern SIGINT activities. The types of auditing are:*

- *(U//~~FOUO~~)* ***Active Auditing:*** *The review of queries against raw SIGINT data or repositories that offer a significant risk of violating the privacy rights of U.S. persons (also known as post-query review). Any system, tool, database, or process which enables*

a user to conduct alpha-numeric searches against raw SIGINT content is actively audited. This function is performed by the elements of a SIGINT mission;

- *(U//~~FOUO~~) **Passive Logging (also known as Passive Auditing)**: The baseline auditing requirement imposed on raw SIGINT data and repositories to record information concerning their use. Passive logging tracks a user's queries of raw SIGINT on a given system and may include a variety of information ranging from simple sign-in, sign-out times to the specific details of mouse clicks on a screen. The logs are not actively reviewed but are stored for potential compliance review at the discretion of SV. This function is performed by the system;*
- *(U//~~FOUO~~) **Spot Checking:** Process of auditing a portion or sampling of the queries executed within specific raw SIGINT data or repositories that have been approved for this type of auditing. This function is performed by the elements of a SIGINT mission; and*
- *(U//~~FOUO~~) **Super Auditing:** The independent review of activities conducted against raw SIGINT systems, tools, or databases. This function is performed by SV."*

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

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

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

~~(TS//SI//NF)~~ As the conclusions cite, I was a trained and experience [sic] SIGINT compliance expert. This fact contributed to the incident.

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

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

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

IV-14-0011

[redacted] Again, this incident was self reported [redacted]

~~(TS//SI//NF)~~ Any conclusions of this incident that do not outline the contributory facts [redacted] in my opinion, are reckless. In the current culture, [redacted]

(U//~~FOUO~~) The information provided does not change the conclusion that [redacted] intentionally used a selection term that was reasonably likely to result in the interception of communications to or from a USP. However, due to his concern [redacted] D14 will forward a summary of his concerns to D11 for their review, possible coordination with SV, and any follow up action deemed appropriate.

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

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

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

V. (U) CONCLUSION

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] intentionally used a selection term that was reasonably likely to result in the interception of communications to or from a USP, in violation of EO12333 Part 2.3, DoD 5240.1-R, Chapter 2, Procedures 2.3.1-2.3.4.2, Chapter 14, Procedure 14, C14.2.1, and USSID SP0018, §3.1, 4.1, & 5.1(a).

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

V.(U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A copy of this report of investigation will be provided to Employee Relations for information and any action deemed appropriate. Also, a summary of the findings will be forwarded to the Associate Directorate for Security and Counterintelligence (ADS&CI).

[redacted]
Investigator

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

Concurred by:

[redacted]
Assistant Inspector General
for
Investigations

blank page

APPENDIX A

(U) Applicable Authorities

(U) EXECUTIVE ORDER 12333, UNITED STATES INTELLIGENCE ACTIVITIES,

(U) Part 2.3 Collection of information

(U) 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:

(a) Information that is publicly available or collected with the consent of the person concerned;

(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;

(c) Information obtained in the course of a lawful foreign 30 intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

(U) In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with

procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

(U) DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons

(U) Chapter 2, Procedure 2. Collection of Information about United States Persons, C2.3. (U) Types of Information that may be collected about United States Persons:
(U) Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:
(U) C2.3.1. Information Obtained With Consent. Information may be collected about a United States person who consents to such collection.
(U) C2.3.2. Publicly Available Information. Information may be collected about a United States person if it is publicly available.
(U) C2.3.3. Foreign Intelligence. Subject to the special limitation contained in section (U) C2.5., below, information may be collected about a United States person if the information constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are:
(U) C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;
(U) C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;
(U) C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;
(U) C2.3.3.4. Persons who are reasonably believed to be prisoners of war; missing in action; or are the targets, the hostages, or victims of international terrorist organizations; or
(U) C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.
(U) C2.3.4. Counterintelligence. Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:
(U) C2.3.4.1. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.
(U) C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

(U) Chapter 14, Procedure 14 – Employee Conduct, C14.2.1. Employee Responsibilities:
(U) Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation. In conducting such activities,

employees shall not exceed the authorities granted the employing DoD intelligence components by law; Executive Order, including E.O. 12333 (reference (a)), and applicable DoD directives.

(U) United States Signals Intelligence Directive (USSID) SPOO18, Legal Compliance and U.S. Persons Minimization Procedures

(U) Policy and the USSS Foreign Communications Mission

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…

(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…

(U) Selection Terms

5.1 Use of Selection Terms During Processing…

…a. ~~(S//SI//REL)~~ No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. Person (wherever located). [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION term…

(b) (1)

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

APPENDIX B

(U) Incident Report

The minimum classification for this form is . The classification may be higher based on information input into the form. See the "Overall Incident Classification" field on page 1.

(U) NSA/CSS Intelligence-Related Incident Report

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

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

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

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