NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

20 November 2015

IV-14-0036

Alleged Misuse of SIGINT Incident

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

I. (U) SUMMARY

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

~~(TS//REL~~) On 4 November 2013, the NSA/CSS Office of Inspector General (OIG) received information that in July 2013 [redacted] a former [redacted] contractor employee working in the NSA/CSS National Threat Operations Center (NTOC), [redacted] had been involved in a misuse of signals intelligence (SIGINT) incident. Specifically, [redacted] allegedly [redacted]

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

(U//~~FOUO~~) In addition to obtaining sworn testimony from [redacted] we conducted interviews with his former [redacted] Task Order Manager, former Contracting Officer's Representative (COR), and former NTOC coworker. We also obtained pertinent records from Oversight and Compliance [redacted]

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

~~(TS//SI//REL~~) The OIG found that in the course of his analytic duties, [redacted]

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

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused information obtained from SIGINT collection, [redacted] without appropriate authorization, without following established procedures, and in violation of his signed user agreement. By doing so, he violated Executive Order 12333, DoD 5240.1-R, USSID SP0018, and USSID DA3655.[1]

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

[1] (U//~~FOUO~~) [redacted] may have also violated [redacted] The Office of General Counsel reported this potential violation to the Department of Justice (DOJ), National Security Division, on [redacted] The DOJ did not respond to the referral. Additionally the OIG reported this potential violation to the United States Attorney's Office (USAO) for the District of Maryland on [redacted] This report does not analyze the potential criminal violation.

(b) (6)

(U//~~FOUO~~) The OIG will notify [redacted] of the results of this investigation. A summary of the findings will be forwarded to [redacted] and the Associate Directorate for Security and Counterintelligence (ADS&CI).

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

II. (U) INTRODUCTION

(U) Background

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

(b) (6)

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

~~(TS//REL)~~ was an contractor employee, assigned to the NTOC as a cyber intelligence analyst between On 8 July 2013, through his analytic work,

~~(U//FOUO)~~ On 9 July 2013, removed from his position as an NTOC analyst. He remained an employee, assigned to an unclassified building, until approximately September 2013 when his employment was terminated. After leaving gained employment with as a contractor intelligence analyst at the He maintained this employment for approximately six months before beginning civilian employment with the Department of Homeland Security (DHS) as the

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

~~(U//FOUO)~~ The information was referred to the OIG Investigations Division on 4 November 2013 by the OIG Intelligence Oversight Division who received the information from NTOC through the Quarterly Report form for compliance with E.O. 12333 and related directives.

(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
- USSID DA3655 – Computer Network Exploitation Data Acquisition Operations and Activities

III. (U) FINDINGS

*(U//~~FOUO~~) **ALLEGATION:** Did [redacted] misuse information obtained from SIGINT collection?*

(U//~~FOUO~~) *CONCLUSION: Substantiated.* *The preponderance of the evidence supports the conclusion that [redacted] misused information obtained from SIGINT collection, [redacted] without appropriate authorization, without following established procedures, and in violation of his signed user agreement. By doing so, he violated Executive Order 12333, DoD 5240.1-R, USSID SP0018, and USSID DA3655.*

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

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

(U) Documentary Evidence

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

(U//~~FOUO~~) This report summarized the incident that occurred on 8 July 2013:

> ~~(TS//SI//REL)~~ [redacted] .Overhearing of this activity at shift change (8 July), the analyst was informed this was a query violation."

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

(U//~~FOUO~~) The full incident report is attached in Appendix B.

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

(U//~~FOUO~~) [redacted] training record revealed prior to 8 July 2013 he took numerous courses regarding SIGINT authorities including:

-OVSC1100 Overview of Signals Intelligence Authorities (30 March 2013)
-OVSC1000 Intelligence Oversight Training (5 December 2012)
-OVSC1800 USSID Legal Compliance and Minimization Procedures (11 October 2012)
-OIAC1180 Annual IA Awareness Training (4 September 2012)

(U//~~FOUO~~) [redacted] training record is attached in Appendix C.

(U) [redacted] **User Acknowledgement**

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

~~(S//REL)~~ The [redacted] User Acknowledgement states:

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

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

[redacted]

(U//~~FOUO~~) [redacted] digitally signed this acknowledgement on 30 May 2013. The full [redacted] User Acknowledgement is located in Appendix D.

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

(U) Testimonial Evidence

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

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

(U//~~FOUO~~) On 20 May 2014, [redacted] NSOC Contracts Oversight, was interviewed and provided the following sworn testimony.

~~(S//SI//REL)~~ [redacted] was the Contracting Officer's Representative (COR) for the [redacted] contract, on which [redacted] was previously assigned. She explained that while working for [redacted] in the NTOC, [redacted] conducted analysis on SIGINT traffic and wanted to "prove" that his analysis was correct. [redacted] was unable to provide any information regarding the [redacted] system. Although [redacted] never stated that he knew his actions were wrong, [redacted] explained that he was trying to "make a point" that his analysis was correct. [redacted] had received the proper training to work with SIGINT information and "he should have known" not to do what he did. "It was a stupid move."

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

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

(U//~~FOUO~~) [redacted] was unaware of how the incident was discovered; however, she explained that when it was discovered [redacted] SIGINT accesses were immediately revoked, he was removed from NSA access, and his employment with [redacted] was terminated.

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

(U//~~FOUO~~)

(U//~~FOUO~~) On 14 August 2014, was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) At the time of the incident, was an employee, working on a contract, supporting was employed as a security analyst, assigned to the NTOC On the day of the incident, received a phone call from at the time, who oversaw the analysts, and informed him of the matter. then talked to and directed him to complete all appropriate paperwork and report to the facility the next day. reported to the facility, as directed, where his SIGINT accesses were removed and he was sent to the maintained as an employee until approximately September 2013. At that time,

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

(U//~~FOUO~~) "he did misuse the system" and "should have known better." He had completed all the required training, had worked in the past and had experience in was told by an unrecalled coworker that actions were motivated by other coworkers stating that they did not believe he was a good analyst. Therefore, actions during this incident were conducted to prove that he was competent in his analytic skills.

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

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

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

(b) (6)

(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
(b) (6)

(U//~~FOUO~~)

(U//~~FOUO~~) On 3 March 2015, former contractor analyst assigned to the NTOC, was interviewed and provided the following sworn testimony:

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

(U//~~FOUO~~) was employed by and assigned to NTOC for approximately two and a half years, from early 2011 to summer 2013. During that time, he was employed as an analyst; Prior to this position, was employed by in another intelligence position for a few years where he also worked in the intelligence field.

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

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

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

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

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

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

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

~~(S//REL)~~ During the interview,

~~(TS//SI//REL)~~ denied malicious intent regarding the incident. Instead, he said his intent was

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

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

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

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

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

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

IV-14-0036

denied to prove he was a good analyst. In fact, believed he was one of the better analysts on the watch floor.

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

(U//~~FOUO~~) After the incident, was removed from the NSA contract on which he had been working. However, maintained his employment for a period of time. He was put on "overhead," meaning he was not placed on a specific contract, and was told to find another contract on which to work. "got the feeling" that, because of this incident, was not going to place him on another contract; therefore he left voluntarily and began working for another Government contracting company, While employed by worked as a for approximately six months as the He eventually left that position he began working as a civilian at the Department of Homeland Security (DHS). currently holds a civilian position with DHS as He informed the security officer at and his current employer about the incident by documenting it in general terms on his security forms. He also discussed the incident with his background investigator during his 2014 background investigation.

(b) (6)

(U//~~FOUO~~) Prior to his employment with spent in the field of intelligence He denied any other security incidents or violations, detected or undetected, at any other time in his career.

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

(U//~~FOUO~~)

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

(U//~~FOUO~~) On 14 April 2015 was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) was employed as a cyber security analyst in the NTOC from late 2009 to early 2011 had no recollection of Although he was unable to recall working with he was able to answer questions regarding his team's mission and protocol during his time as a contractor employee in the NTOC.

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

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

(U//~~FOUO~~) stated that the use of the website, was authorized. He further explained, "open source research is different from

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

(U) Analysis and Conclusions

~~(TS//SI//REL)~~ 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 United States Person (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 SP0018, Sections 3.1 & 4.1, the United States SIGINT System will not intentionally collect communications to, from, or about USPs.

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

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

~~(TS//SI//REL)~~ In the course of his analytic duties [redacted]

~~(TS//SI//REL)~~ At the time of the incident, [redacted] was a cyber intelligence analyst who had completed numerous NSA courses on applicable SIGINT regulations. Prior to his position with [redacted] in the intelligence field. Therefore, by virtue of his training and experience as an intelligence professional and cyber intelligence analyst, [redacted] should have been aware of the regulations [redacted]

(b) (6)

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

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

~~(S//REL)~~ [redacted] User Acknowledgement (Appendix D) on 30 May 2013. This document addresses several points that should have alerted [redacted]

~~(S//REL)~~ The [redacted] User Acknowledgement [redacted]

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

[redacted]

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

~~(TS//SI//REL)~~ According to USSID DA3655, Computer Network Exploitation (CNE) Data Acquisition Operations and Activities, Section 2 – Computer Network Exploitation Categories, [redacted]

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

[redacted]

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

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused information obtained from SIGINT collection, [redacted] without appropriate authorization, without following established procedures, and in violation of his signed user agreement. By doing so, he violated Executive Order 12333, DoD 5240.1-R, USSID SP0018, and USSID DA3655.

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

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

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

(U//~~FOUO~~) The tentative conclusions were sent to [redacted] via e-mail, on 27 October 2015. [redacted] acknowledged receipt of the tentative conclusions e-mail, but did not comment; therefore, the tentative conclusions became final.

V. (U) CONCLUSION

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

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

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] misused information obtained from SIGINT collection, [redacted] without appropriate authorization, without following established procedures, and in violation of his signed user agreement. By doing so, he violated Executive Order 12333, DoD 5240.1-R, USSID SP0018, and USSID DA3655.

V. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A summary of the investigative findings will be provided to [redacted] and [redacted]

[redacted]

Investigator

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

Concurred by:

[redacted]

Assistant Inspector General
for
Investigations

APPENDIX A

(U) Applicable Authorities

(U) Executive Order 12333, United States Intelligence Activities

Section 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…

In carrying out the responsibilities assigned in Section 1.1, the Secretary of Defense is authorized to use the following: (b) National Security Agency, whose responsibilities shall include: (3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence.

(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. Types of Information that may be collected about United States Persons:
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:
C2.3.1. Information Obtained With Consent. Information may be collected about a United States person who consents to such collection.
C2.3.2. Publicly Available Information. Information may be collected about a United States person if it is publicly available.
C2.3.3. Foreign Intelligence. Subject to the special limitation contained in section 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:
C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;
C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;
C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;
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
C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

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:
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.
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.

Procedure 14 – Employee Conduct, B.1. Employee Responsibilities

Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 and the 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, and applicable DoD directives.

(U) United States Signals Intelligence Directive (USSID) SP0018, Legal Compliance and U.S. Persons Minimization Procedures

(U) Section 3 – 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…

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

(U) Section 4 – Collection
4.1. ~~(S//SI//REL)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted]

a. (U) With the approval of the United States Foreign Intelligence Surveillance Court . . .
b. (U) With the approval of the Attorney General of the United States . . .
c. (U) With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and
d. (U) Emergency Situations.

(U) Section 9 – Definitions
9.18. (U) UNITED STATES PERSON:
a. (U) A citizen of the UNITED STATES,
b. (U) An alien lawfully admitted for permanent residence in the UNITED STATES,
c. (U) Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or
d. (U) CORPORATIONS incorporated in the UNITED STATES, including U.S. 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.

e. (U) The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) (U) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) (U) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON. . . .

(U//~~FOUO~~) United States Signals Intelligence Directive (USSID) DA3655, Computer Network Exploitation (CNE) Data Acquisition Operations and Activities

Section 2 – Computer Network Exploitation Categories

…2.7 (b) ~~(S//SI//REL)~~ [redacted]

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

Section 3 – Oversight and Policy

…3.2 ~~(S//SI//REL)~~ [redacted]

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

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

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

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

c. (U//~~FOUO~~)

d. (~~S//REL~~)

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

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

e. (U//~~FOUO~~) Management of the CNE mission requires orderly and thorough record keeping.

f. (U//~~FOUO~~)

APPENDIX B

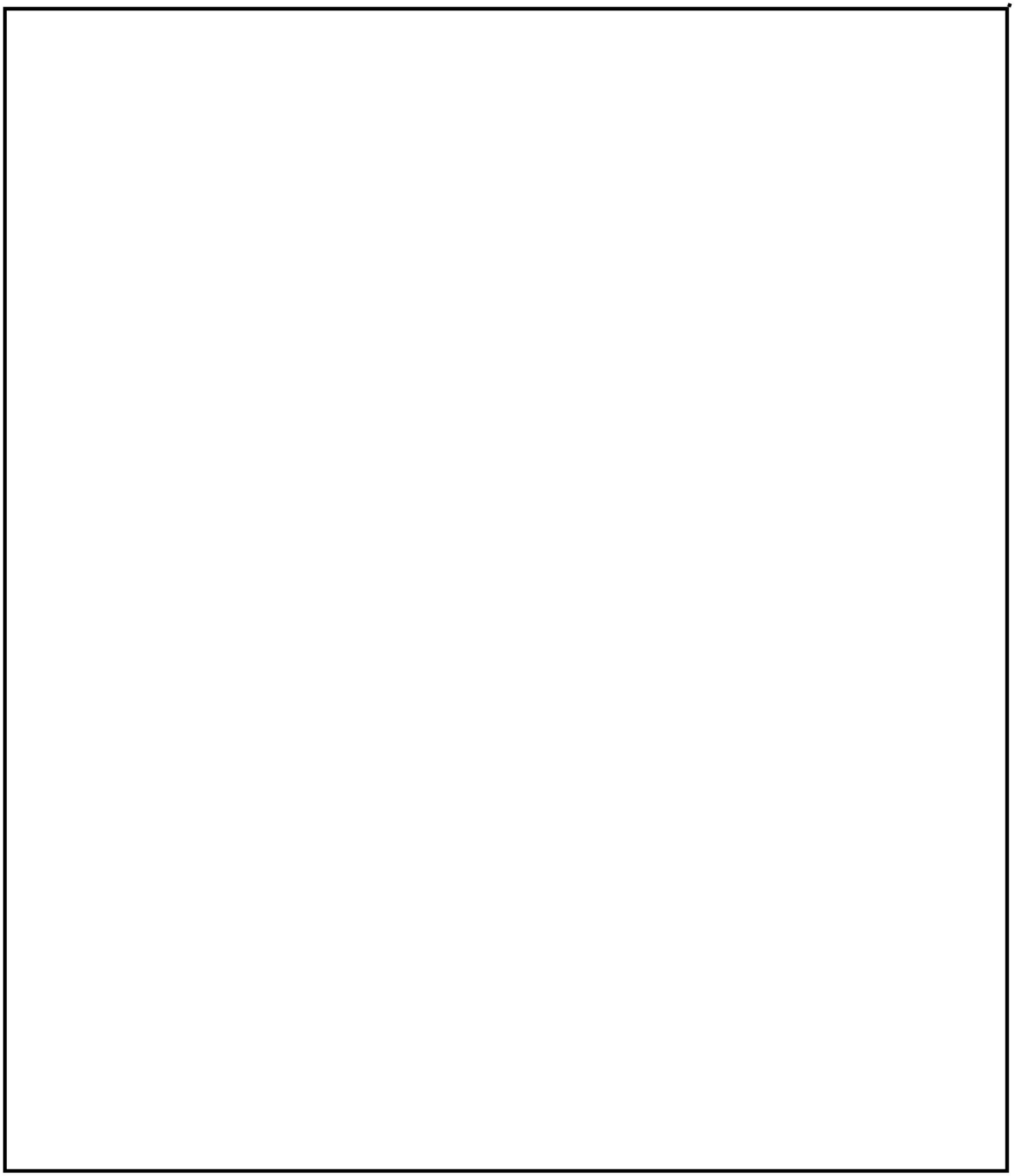
(U) Incident Report [redacted] . . . . . (b)(3)-P.L. 86-36

(U) NSA/CSS Intelligence-Related Incident Report

The minimum classification for this form is ~~SECRET//COMINT//REL TO USA, FVEY~~. The classification may be higher based on information input into the form. See the "Overall Incident Classification" field on page 1.

The minimum classification for this form is ~~SECRET//COMINT//REL TO USA, FVEY~~. The classification may be higher based on information input into the form. See the "Overall Incident Classification" field on page 1.

The minimum classification for this form is ~~SECRET//COMINT//REL TO USA, FVEY~~. The classification may be higher based on information input into the form. See the "Overall Incident Classification" field on page 1.



The minimum classification for this form is ~~SECRET//COMINT//REL TO USA, FVEY~~. The classification may be higher based on information input into the form. See the "Overall Incident Classification" field on page 1.

APPENDIX C

Training Record

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

PERSONNEL PRIVILEGED

*** This document may be removed from NSA facilities, without a CAO review or prior approval, UNLESS a course that was ***
*** sponsored by another Intelligence Community Agency is listed. If a course from another Agency is listed, a request ***
*** for approval of the document should be submitted via email to DL DJ4_privacy with a copy of the training history attached.***

Name:
Learner ID:
Department:

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

(b) (6)

Course Designator	Start Date	End Date	Title	Hours	Score
OVSC1100	30-MAR-2013	30-MAR-2013	(U) OVERVIEW OF SIGNALS INTELLIGENCE AUTHORITIES	2	P
				1	P
OVSC1203	12-DEC-2012	04-JAN-2013	(U) FISA AMENDMENT ACT (FAA) SECTION 702	4	90
				1	P
CLAS1000	11-DEC-2012	11-DEC-2012	(U) ELEMENTS OF CLASSIFICATION AND MARKING	1	P
OVSC1000	05-DEC-2012	05-DEC-2012	(U) NSA/CSS INTELLIGENCE OVERSIGHT TRAINING	1	P
CLAS1700	05-DEC-2012	05-DEC-2012	(U) RECORDS MANAGEMENT ANNUAL AWARENESS TRAINING	1	P
OVSC1800	06-SEP-2012	11-OCT-2012	(U) LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES	2	100
				16	P
PRIV1001	04-SEP-2012	04-SEP-2012	(U) ANNUAL PRIVACY AWARENESS FOR EMPLOYEES	1	P
OIAC1180	04-SEP-2012	04-SEP-2012	(U) CYBER AWARENESS CHALLENGE	1	P
				1	P
				24	P
OVSC1100	02-APR-2012	02-APR-2012	(U) OVERVIEW OF SIGNALS INTELLIGENCE AUTHORITIES	2	P
				1	NE
OVSC1203	25-NOV-2011	07-DEC-2011	(U) FISA AMENDMENT ACT (FAA) SECTION 702	4	100
OVSC1800	17-NOV-2011	02-DEC-2011	(U) LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES	2	100
				1	P
OIAC11802011	08-OCT-2011	10-OCT-2011	(U) ANNUAL IA AWARENESS TRAINING	1	P
PRIV1001	02-SEP-2011	04-SEP-2011	(U) ANNUAL PRIVACY AWARENESS FOR EMPLOYEES	1	P
CLAS1000	02-SEP-2011	04-SEP-2011	(U) ELEMENTS OF CLASSIFICATION AND MARKING	1	P
OVSC1100	27-MAY-2011	29-MAY-2011	(U) OVERVIEW OF SIGNALS INTELLIGENCE AUTHORITIES	1	P
OPSE1301	20-MAR-2011	22-MAR-2011	(U) OPSEC FUNDAMENTALS	4	P
				2	P
PRIV1001	21-DEC-2010	23-DEC-2010	(U) ANNUAL PRIVACY AWARENESS FOR EMPLOYEES	1	P
OIAC11802010	21-DEC-2010	23-DEC-2010	(U) ANNUAL IA AWARENESS TRAINING	1	P
				1	100
OVSC1203	09-DEC-2010	20-DEC-2010	(U) FISA AMENDMENT ACT (FAA) SECTION 702	4	95
OVSC1100	02-JUN-2010	02-JUN-2010	(U) OVERVIEW OF INTELLIGENCE AUTHORITIES	4	100
OVSC1800	02-JUN-2010	07-DEC-2010	(U) LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES	2	96
				1	NE
				40	A
					NE
				120	A
				32	A
				1	NE
				24	NE
				8	NE

* Indicates Embedded Course

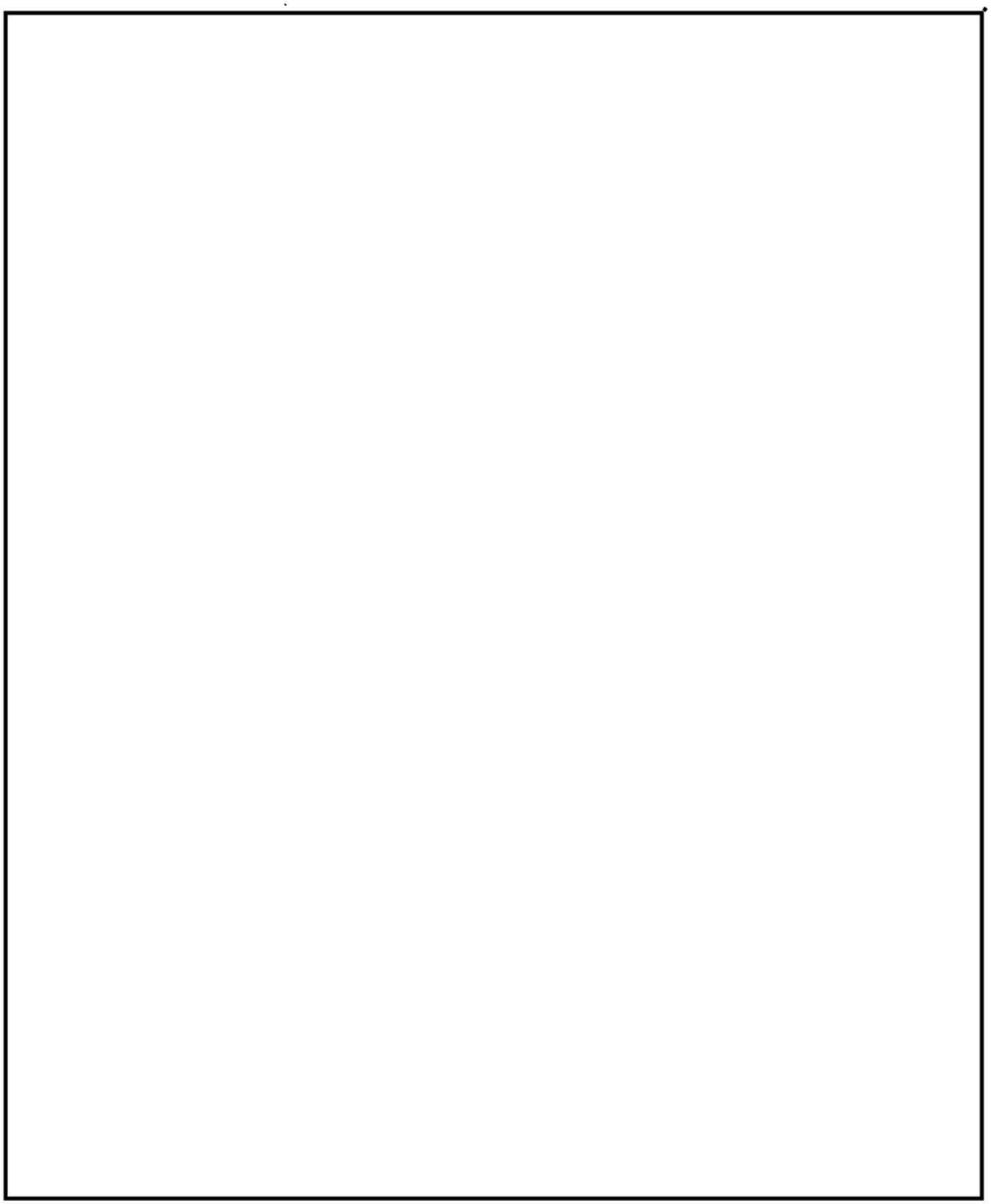
(b)(3)-P.L. 86-36

APPENDIX D

[redacted] User Acknowledgement

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

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~



Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: 20291123

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL~~