

POLITICS

File Says N.S.A. Found Way to Replace Email Program

By **CHARLIE SAVAGE** NOV. 19, 2015



The National Security Agency headquarters at Fort Meade, Maryland in 2010.

Credit Saul Loeb/Agence France-Presse — Getty Images

WASHINGTON — When the National Security Agency’s bulk collection of records about **Americans’** emails came to light in 2013, the government conceded the **program’s** existence but said it had shut down the effort in December 2011 for “**operational** and resource **reasons.**”

While that particular secret program stopped, newly disclosed documents show that the N.S.A. had found a way to create a functional

equivalent. The shift has permitted the agency to continue analyzing social links revealed by **Americans'** email patterns, but without collecting the data in bulk from American telecommunications companies — and with less oversight by the Foreign Intelligence Surveillance Court.

The disclosure comes as a sister program that collects **Americans'** phone records in bulk is set to end this month. Under a law enacted in June, known as the U.S.A. Freedom Act, the program will be replaced with a system in which the N.S.A. can still gain access to the data to hunt for associates of terrorism suspects, but the bulk logs will stay in the hands of phone companies.

The newly disclosed information about the email records program is contained in a report by the **N.S.A.'s** inspector general that was obtained by The New York Times through a lawsuit under the Freedom of Information Act. One passage lists four reasons that the N.S.A. decided to end the email program and purge previously collected data. Three were redacted, but the fourth was uncensored. It said that “**other** authorities can satisfy certain foreign intelligence **requirements**” that the bulk email records program “**had** been designed to **meet**.”

The report explained that there were two other legal ways to get such data. One was the collection of bulk data that had been gathered in other countries, where the **N.S.A.'s** activities are largely not subject to regulation by the Foreign Intelligence Surveillance Act and oversight by the intelligence court. Because of the way the Internet operates, domestic data is often found on fiber optic cables abroad.

The N.S.A. had long barred analysts from using **Americans'** data that had been swept up abroad, but in November 2010 it changed that rule, documents leaked by Edward J. Snowden have shown. The

inspector general report cited that change to the **N.S.A.’s** internal procedures.

The other replacement source for the data was collection under the FISA Amendments Act of 2008, which permits warrantless surveillance on domestic soil that targets specific noncitizens abroad, including their new or stored emails to or from Americans.

“**Thus,**” the report said, these two sources “**assist** in the identification of terrorists communicating with individuals in the United States, which addresses one of the original reasons for **establishing**” the bulk email records program.

Timothy Edgar, a privacy official in the Office of the Director of National Intelligence in both the George W. Bush and Obama administrations who now teaches at Brown University, said the explanation filled an important gap in the still-emerging history of post-Sept. 11, 2001, surveillance.

“The document makes it clear that N.S.A. is able to get all the Internet metadata it needs through foreign **collection,**” he said. “**The** change it made to its procedures in 2010 allowed it to exploit metadata involving Americans. Once that change was made, it was no longer worth the effort to collect Internet metadata inside the United States, in part because doing so requires N.S.A. to deal **with**” restrictions by the intelligence court.

Observers have previously suggested that the **N.S.A.’s** November 2010 rules change on the use of **Americans’** data gathered abroad might be connected to the December 2011 end of the bulk email records program. Marcy Wheeler of the national security blog Emptywheel, for example, has argued that this was probably what happened.

And officials, who spoke on the condition of anonymity to discuss

sensitive collection programs, have said the rules change and the FISA Amendments Act helped make the email records program less valuable relative to its expense and trouble. The newly disclosed documents amount to official confirmation.

The N.S.A. and the Office of the Director of National Intelligence did not respond to a request for comment.

After the Sept. 11 attacks, Mr. Bush secretly authorized the N.S.A. to conduct surveillance and data-collection activities without obeying the Foreign Intelligence Surveillance Act, in a program called Stellarwind.

The email records component caused many internal headaches. In 2004, the Justice Department questioned its legality, contributing to a confrontation in the hospital room of Attorney General John Ashcroft and the threat of a mass resignation.

Mr. Bush then halted the program until the intelligence court began issuing secret orders authorizing it.

The court limited the categories of data that the N.S.A. was permitted to collect and restricted how it could gain access to the data. After violations of those limits were revealed in 2009, the N.S.A. suspended the program until mid-2010, only to end it the next year.

Follow the New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on November 20, 2015, on page A4 of the New York edition with the headline: File Says N.S.A. Found Way to Replace Email Program .

US

NSA Declassifies Inspector General Reports About Defunct Bulk E-mail Metadata Program

By **CHARLIE SAVAGE** NOV. 19, 2015

In response to a [Freedom of Information Act lawsuit](#) by The New York Times, the National Security Agency has released these documents. They largely consist of inspector general reports related to the **NSA's defunct bulk e-mail records collection program**. The program began as part of the Bush administration's response to the Sept. 11, 2001, terrorist attacks. In the spring of 2004, its legality was a central part of a famous incident in which Bush officials confronted each other in the hospital room of Attorney General John Ashcroft. That July, the Justice Department persuaded the Foreign Intelligence Surveillance Court to begin issuing orders authorizing the bulk records collection under a disputed interpretation of a provision of the Foreign Intelligence Surveillance Act permitting the installation of pen register/trap & trace devices, which collect metadata — information showing who contacted whom and when, but not the content of what they said. The NSA shuttered the program in December 2011. Its existence came to light in the summer of 2013 as part of the leaks by the former intelligence contractor Edward J. Snowden. [RELATED ARTICLE](#)

See following pages.



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*86 Chambers Street
New York, New York 10007*

November 10, 2015

By Electronic Mail

David E. McCraw, Esq.
Jeremy A. Kutner, Esq.
The New York Times Company
620 Eighth Avenue
New York, NY 10018
E-mail: mccrad@nytimes.com
jeremy.kutner@nytimes.com

Re: *The New York Times Co. and Charlie Savage v. National Security Agency*,
15 Civ. 2383 (KBF)

Dear David and Jeremy:

This Office represents the National Security Agency (“NSA”), the defendant in the above-referenced matter. Pursuant to the Scheduling Order, dated May 15, 2015, NSA has completed its review and processing of the attached documents. NSA is releasing 10 documents with redactions. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1) and (b)(3). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

Please let me know if you have any questions.

Sincerely,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: /s/ Andrew E. Krause
ANDREW E. KRAUSE
Assistant United States Attorney
Telephone: (212) 637-2769
Facsimile: (212) 637-2786
E-mail: andrew.krause@usdoj.gov

Attachments



~~TOP SECRET//COMINT//REL TO USA, FVEY~~
 NATIONAL SECURITY AGENCY
 CENTRAL SECURITY SERVICE
 FORT GEORGE G. MEADE, MARYLAND 20755-6000

November 30, 2009

The Honorable Silvestre Reyes
 Chairman, Permanent Select
 Committee on Intelligence
 United States House of Representatives
 H-405, The Capitol
 Washington, DC 20515

Dear Representative Reyes:

(U//FOUO) The Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA) authorizes the NSA Inspector General to assess the Agency's compliance with procedures for targeting certain persons outside the United States, other than United States persons. Except as otherwise stated, I have no reason to believe that any intelligence activities of the National Security Agency during the period 1 September 2008 through 31 August 2009 were unlawful.

(U//FOUO) My office reviews the collection, processing, and reporting of data at least quarterly. Incidents involving compliance with procedures for targeting certain persons outside the United States, other than United States persons, and incidents involving minimization of United States person information are reported to the OIG as they occur and quarterly. Each incident is evaluated against the targeting and minimization procedures set forth in the FAA and in NSA directives.

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

(S//SI//REL TO USA, FVEY) In compliance with the targeting and minimization procedures of §702 of the FAA, NSA/CSS disseminated [] intelligence reports between FAA implementation on 1 September 2008 and 31 August 2009. Of the [] disseminations, [] reports contained a reference to a United States person identity. Additionally, NSA released [] names of U.S. identities in response to [] customer requests.

(TS//SI//REL TO USA, FVEY) During this reporting period, [] valid foreign targets outside the United States at the time of tasking were later suspected or confirmed to be in the United States. []

(b)(1)

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

(TS//SI//REL TO USA, FVEY) We found and reported [] instances of §702 targeting or minimization mistakes to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight:

- [] target selectors had been tasked under an incorrect §702 certification category
- [] software malfunctions had caused unintended collection
- [] foreign intelligence targets had been incorrectly tasked for §702 collection []

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

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

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

- [] target w s later found to h ve U.S. citizenship
- There were [] delays in removing the t rget selectors from collection systems and
- [] dela s in purging unauthorized collection from NSA databases.

(U) Action was taken to correct the mist kes and processes were reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of U.S. person communications.

(U//FOUO) The Office of Inspector General continues to exercise oversight of Agency intelligence activities.

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


GEORGE ELLARD
Inspector General

Copy Furnished:
The Honorable Peter Hoekstra
Ranking Member, Permanent Select
Committee on Intelligence

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

~~TOP SECRET//COMINT//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ **Report on the Audit of NSA Controls to Comply
with the Foreign Intelligence Surveillance Court Order
Regarding Pen Register and Trap and Trace Devices**

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



DERIVED FROM: NSA/CSS Manual 1-52
DATED: 08 January 2007
DECLASSIFY ON: ~~20320108~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, and investigations and inspections. It's mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessment of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assesses whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, 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) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

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

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Advisory Report on the Audit of NSA Controls to
Comply with the Foreign Intelligence Surveillance Court Order Regarding Pen
Register and Trap and Trace Devices [REDACTED] ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This advisory report summarizes results of testing by the
Office of the Inspector General in support of the Audit of NSA Controls to Comply
with the Foreign Intelligence Surveillance Court Order Regarding Pen Register
and Trap and Trace Devices [REDACTED]

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

2. (U//~~FOUO~~) We determined that querying controls were adequate to
provide reasonable assurance of compliance with the terms of the Order. [REDACTED]

[REDACTED]

Based on our review, no management response is required for this report.

3. (U//~~FOUO~~) To discuss this report further, please contact [REDACTED]
on 963-0922(s) or by e-mail at [REDACTED]

4. (U) We appreciate the courtesy and cooperation extended to the audit
team throughout the review.

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

Handwritten signature of George Ellard in cursive script.

GEORGE ELLARD
Inspector General~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

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

[REDACTED]

(U//~~FOUO~~) DISTRIBUTION:

D●C (J. DeLong)

SID (T. Shea)

TD [REDACTED]

cc:

Director

●GC [REDACTED]

SV [REDACTED]

SV4 [REDACTED]

SV42 [REDACTED]

S12 [REDACTED]

S2 [REDACTED]

S21 [REDACTED]

S214 [REDACTED]

S332 [REDACTED]

T1 [REDACTED]

T12 [REDACTED]

T122 [REDACTED]

T1222 [REDACTED]

D4 IG POC [REDACTED]

●GC IG POC [REDACTED]

SID IG POC [REDACTED]

TD IG POC [REDACTED]

D●J NSD [REDACTED]

IG

(b)(6)

D/IG

D1 [REDACTED]

D11

D12

D13

D14

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

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

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

(U) EXECUTIVE SUMMARY(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ We conducted this review to determine whether the controls we tested as part of a [] yearlong review of NSA compliance with seven provisions of the Business Records Order were adequate to provide reasonable assurance of compliance with similar provisions of the Pen Register and Trap and Trace (PR/TT) Order. Of the [] queries made between [] the date when the Foreign Intelligence Surveillance Court signed [] and [] we found no errors or instances of non-compliance with the five provisions of the PR/TT Order related to querying that we tested. We therefore judged these controls to be adequate to provide reasonable assurance of compliance with the Order. []

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

~~(TS//SI//NF)~~ The Pen Register and Trap and Trace (PR/TT) Order

~~(TS//SI//NF)~~ The Foreign Intelligence Surveillance Court (FISC) granted NSA the authority to collect certain categories of metadata with the assistance of certain United States based telecommunications service providers and to analyze that metadata in support of investigations to protect against international terrorism. The PR/TT Order authorizes NSA to collect and analyze bulk metadata from providers within the United States.

~~(TS//SI//NF)~~ PR/TT metadata includes communication:

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

- ~~(TS//SI//NF)~~ addressing information (e.g., the "to," "from," "cc," and "bcc" fields) []

~~(TS//SI//NF)~~ The PR/TT Order prohibits collection of content of communications.

~~(TS//SI//NF)~~ The FISC renews the PR/TT Order approximately every 90 days. NSA, in consultation with the Department of Justice, did not seek an immediate renewal and allowed the PR/TT Order to expire in []

~~TOP SECRET//COMINT//NOFORN~~(b)(1)
(b)(3)-P.L. 86-36

~~TOP SECRET//COMINT//NOFORN~~(b)(1)
(b)(3)-P.L. 86-36

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

[redacted] because of concern the Agency could not comply with the order as written. [redacted] the FISC issued an Order substantially different from the previous versions in that, among other things, it redefined "facilities" [redacted] However, the provisions that limit the selectors on which NSA may query, as well as provisions to track and report on dissemination, remained essentially unchanged and are similar to those in the current Business Records (BR) Order, which authorizes the collection of bulk telephony metadata. The PR/TT Order includes a series of provisions to protect the privacy of United States persons (USPs) because the bulk metadata collected under the Order includes [redacted] [redacted] USP communications, the vast majority of which are unrelated to investigations to protect against international terrorism.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)**(U) This Review**

~~(TS//SI//NF)~~ We began this review in [redacted] but suspended it when NSA allowed the PR/TT Order to expire. We then conducted a yearlong *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004)* using a continuous auditing methodology to test monthly certain controls related to querying and dissemination. As part of that review, we evaluated the adequacy of controls to ensure compliance with seven requirements tested against *Standards of Internal Control in the Federal Government*. Because the requirements, controls, and processes used to query and to disseminate information are essentially the same under the PR/TT Order and the BR Order, we relied on the overall evaluation of controls conducted under ST-10-0004 and used the same test objectives and plans for both reviews. See Appendix A for details on the objective, scope, and methodology as well as a list of reports issued on our tests of BR controls.

~~(TS//SI//NF)~~ For this review, we tested NSA compliance with five provisions of the PR/TT Order related to querying for [redacted] [redacted] while an active Order was in place. Although the Order first became active in [redacted] after the Agency had allowed it to expire, the Agency did not resume collection and querying of PR/TT metadata until [redacted] (which closely mirrors its first renewal). [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-P.L. 86-36**(U) Test Results and Objectives Related to Querying**

~~(TS//SI//NF)~~ Of the [redacted] queries made during our test period, we found no errors or instances of non-compliance with the five provisions of the PR/TT Order related to querying that we tested.

~~(TS//SI//NF)~~ For the period reviewed, [redacted] issued from PR/TT metadata and appropriately reported in the 30-day renewal report. However, the dissemination did not contain PR/TT-derived USP information. With such [redacted] we did not formally test dissemination objectives.

(b)(1)
(b)(3)-P.L. 86-36~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

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

- ~~(TS//SI//NF)~~ Access: Were all queries to the PR/TT metadata made by authorized individuals (e.g., intelligence analysts and approved technical support personnel)?
- ~~(U//FOUO)~~ Reasonable Articulate Suspicion (RAS) Approval of Queried Selectors: Did all queries use RAS-approved seed selectors?
- ~~(U//FOUO)~~ Office of General Counsel (OGC) Review of USP Selectors: Did OGC verify that RAS determinations of all queried seed selectors associated with USPs had not been based solely on activities protected by the First Amendment to the Constitution?
- ~~(C//REL TO USA, FVEY)~~ Chaining: Were all queries chained to no more than two hops?
- ~~(U//FOUO)~~ Revalidation of Queried Selectors: Were all queried foreign and USP seed selectors revalidated within the Court's time frames—one year and 180 days, respectively—and approved by an authorized Homeland Mission Coordinator?

~~(TS//SI//NF)~~ These provisions limit access to the bulk metadata and the selectors that NSA is authorized to query. See Appendix B for details of test results.

(U) Test Results and Objectives Related to Dissemination

~~(TS//SI//NF)~~ The PR/TT Order also required that NSA track and report information shared outside the Agency. [REDACTED]

[REDACTED]

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

- ~~(TS//SI//NF)~~ 30-Day Reports: Did NSA accurately and completely report disseminations of PR/TT metadata outside NSA?
- ~~(TS//SI//NF)~~ Dissemination of Serialized SIGINT Reports with PR/TT Metadata: Was all information disseminated through serialized SIGINT reports approved by the Chief of Information Sharing Services (S12) or other authorized individuals?

(U) Conclusion

~~(TS//SI//NF)~~ Our tests of queries made under the PR/TT Order parallel the findings of our review of BR controls: querying controls are adequate to provide reasonable assurance of compliance with the provisions tested, but NSA management must ensure that controls remain effective. [REDACTED]

[REDACTED]

[REDACTED] we must rely on findings of our BR review that the largely manual process to disseminate is manageable given the small amount of information

~~TOP SECRET//COMINT//NOFORN~~

(b)(1)

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

~~TOP SECRET//COMINT//NOFORN~~

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

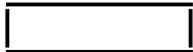


disseminated in 2010. We make no recommendations in this report because the implementation of recommendations in ST-10-0004L will be tracked by the Office of the Inspector General follow-up process.

~~TOP SECRET//COMINT//NOFORN~~

(U) APPENDIX A

(U) About the Audit



~~TOP SECRET//COMINT//NOFORN~~

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

(U) This page intentionally left blank.

~~TOP SECRET//COMINT//NOFORN~~

(U) ABOUT THE AUDIT

(U) Objectives

~~(TS//SI//NF)~~ The objective of this audit was to test whether controls to ensure that NSA compliance with key terms of the Pen Register and Trap and Trace (PR/TT) Order were operating effectively. Specifically, we tested NSA compliance with five provisions of the Order related to querying to assess the adequacy of controls. We tested these provisions because they were relatively stable, at risk for technical non-compliance or violation of privacy rights, and testable. For a requirement to be testable, compliance must be clearly objective and verifiable by supporting data. [REDACTED] (b)(3)-P.L. 86-36

(U) Scope and Methodology

~~(TS//SI//NF)~~ From January through February [REDACTED] we tested queries of PR/TT metadata made [REDACTED] during which NSA was operating under [REDACTED]

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

Outside of testing, we based our evaluation of controls on work conducted as part of the Business Records (BR) review (ST-10-0004).

~~(TS//SI//NF)~~ For querying, all selectors that were documented in [REDACTED] audit logs as having been queried were compared against access lists maintained by SV42 and reasonable articulable suspicion approvals and Office of General Counsel (OGC) reviews documented in [REDACTED] is NSA's corporate contact chaining system. It stores metadata from multiple sources, storing PR/TT metadata in a separate realm. [REDACTED] performs data quality, preparation, and sorting functions and summarizes contacts in the processed data. [REDACTED] is the selector tracking application used for PR/TT and BR querying. We also counted the number of hops chained for each selector as documented in [REDACTED] audit logs. We researched anomalies to make a final determination of compliance. (b)(1)
(b)(3)-P.L. 86-36

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

[REDACTED] We intended to verify that serialized Signals Intelligence (SIGINT) reports derived from PR/TT metadata, as documented in [REDACTED] were supported by dissemination authorizations and included in 30-Day Reports provided to the Foreign Intelligence Surveillance Court (FISC). [REDACTED] a management information system for SIGINT production, contains statistical information and customer feedback about serialized reports.

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

~~TOP SECRET//COMINT//NOFORN~~

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

~~(TS//SI//NF)~~ [redacted] We did not plan to test whether non-serialized reports were approved by the Chief, Information Sharing Services (SI2), or other authorized officials because approvals were documented in e-mails rather than formal dissemination authorizations. For the same reason, we did not plan to test whether 30-Day Reports accurately and completely disclosed non-serialized reports.

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

~~(TS//SI//NF)~~ During the *Audit on NSA Controls to Comply with Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004L)*, we met with individuals from OGC, the Office of the Director of Compliance, the SIGINT Directorate (SID), and the Technology Directorate, including the SID Office of Oversight and Compliance, Information Sharing Services, Homeland Security Analysis Center, SID Issues Support Staff, Analytic Capabilities,

[redacted] Information obtained from these meetings was used as a basis to conduct the PR/TT review.

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according to our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

(U) Prior OIG Coverage

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

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

~~(TS//SI//NF)~~ Supplemental Report to IG Report [redacted]

~~(TS//SI//NF)~~ *Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using PR/TT Devices* [redacted]

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

~~(TS//SI//NF)~~ Related OIG Coverage of the BR Order

~~(TS//SI//NF)~~ We issued the following reports as part of our *Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004)*. These reports provide details on the processes and controls in place to ensure compliance with the BR and PR/TT Orders.

- ~~(TS//SI//NF)~~ *Advisory Report on the Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004)*, 12 May 2010

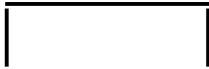
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

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

- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - January to March 2010 Test Results (ST-10-0004A), 1 June 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records April 2010 Test Results (ST-10-0004B), 10 June 2010
- ~~(TS//SI//NF)~~ Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - Control Weaknesses (ST-10-0004C), 29 September 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records May 2010 Test Results (ST-10-0004D), 30 June 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - June 2010 Test Results (ST-10-0004E), 20 July 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - July 2010 Test Results (ST-10-0004F), 18 August 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - August 2010 Test Results (ST-10-0004G), 28 September 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - September 2010 Test Results (ST-10-0004H), 28 October 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - October 2010 Test Results (ST-10-0004I), 1 December 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - November 2010 Test Results (ST-10-0004J), 20 December 2010
- ~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records - December 2010 Test Results (ST-10-0004K), 12 January 2011
- ~~(TS//SI//NF)~~ Draft Audit Report on NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (ST-10-0004L), 15 March 2011

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

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

(U) This page intentionally left blank.

~~TOP SECRET//COMINT//NOFORN~~

(U) APPENDIX B

(U) Test Results



~~TOP SECRET//COMINT//NOFORN~~

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

(U) This page intentionally left blank.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

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

(U) TEST RESULTS (b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ We judged NSA controls as adequate to provide reasonable assurance of compliance with the five provisions of the Foreign Intelligence Surveillance Court (FISC) Order regarding Pen Register and Trap and Trace Devices (PR/TT) related to querying that we tested. Test results show that NSA complied with these provisions for the test period [REDACTED]

[REDACTED] The ratings are defined on the last page of this report.

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

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

Area	Test Results	Test Errors	Compliance	Assessment of Controls
1. Access	Authorized individuals made all [REDACTED] queries of PR/TT metadata.	0	Compliant	Adequate
2. Reasonable articulable suspicion (RAS) approval of queried selectors	Seed selectors of [REDACTED] queries of PR/TT metadata in [REDACTED] were documented as RAS approved in [REDACTED] at the time of the query. The remaining [REDACTED] did not use RAS-approved seed selectors but were made for data integrity and test purposes, as permitted by the Order.	0	Compliant	Adequate
3. Office of General Counsel (OGC) review of U.S. person (USP) selectors	All [REDACTED] USP seed selectors were reviewed by NSA OGC for First Amendment concerns prior to being used to query [REDACTED]. These reviews are documented in NSA's RAS identifier management system, [REDACTED].	0	Compliant	Adequate
4. Chaining	All [REDACTED] queries made for foreign intelligence purposes were chained to no more than two hops from a RAS-approved selector, as required. In [REDACTED] of those instances, although a third hop was attempted, the queries were terminated before results were returned and therefore were within the two-hop limit.	0	Compliant	Adequate
5. Approval and revalidation of queried selectors	The [REDACTED] seed selectors queried for foreign intelligence purposes were RAS approved by authorized Homeland Mission Coordinators within the Court's time frames. An additional [REDACTED] seed selectors were queried for data integrity or test purposes as permitted by the Order.	0	Compliant	Adequate
6. 30-Day Reports	[REDACTED]			
7. Dissemination of serialized SIGINT reports with PR/TT metadata				

(b)(1)
(b)(3)-P.L. 86-36~~(TS//SI//NF)~~~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~**(U) RATING SYSTEM**

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

~~(U//SI//NF)~~

Description	Rating
A rating of green indicates that no instances of non-compliance with the PR/TT Order were identified during testing. Any noted scope limitations were related to the application of the continuous auditing methodology, not known control weaknesses	Compliant
A rating of yellow indicates that although no instances of non-compliance were identified, control weaknesses prevented us from testing the entire universe, as explained in the scope limitations.	Compliant, with scope limitations
A rating of red indicates that one or more instances of non-compliance with the PR/TT Order were identified during testing.	Non-compliant

~~(U//SI//NF)~~~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT STELLARWIND//ORCON//NOFORN//MR~~OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

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

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using Pen Register and Trap and Trace Devices [REDACTED] ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes the results of our assessment of management controls to implement the FISC Order authorizing NSA to collect information using Pen Register and Trap and Trace Devices (PRIT). Because of extenuating circumstances, management was unable to provide complete responses to the draft report but indicated general concurrence with the recommendations. We will follow up on management's actions to implement the recommendations in 90 days.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, NSA/CSS Office of the Inspector General, actions on OIG audit recommendations are subject to monitoring and followup until completion. Consequently, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." The status report should provide sufficient information to show that corrective actions have been completed. If a planned action will not be completed by the original target completion date, please state the reason for the delay and give a revised target completion date. Status reports should be sent to [REDACTED] Assistant Inspector General, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

3. (U) (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [REDACTED] on 963-2988 or via e mail at [REDACTED]

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

Brian R. McAndrew
BRIAN R. MCANDREW
Acting Inspector General

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~MR~~

~~TOP SECRET//COMINT STELLARWIND//ORCON//NOFORN//MR~~

DISTRIBUTION:

DIR

D/DIR

GC

AGC(O)

SIGINT Director

SID Program Manager for CT Special Projects, S

Chief, SID O&C

SSG I

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

SID Deputy Director for Customer Relationships

SID Deputy Director for Analysis and Production

Chief, S2I

Chief, S2I5

SID Deputy Director for Data Acquisition

Chief, S332

~~(TS//SI//NF)~~ **ASSESSMENT OF MANAGEMENT
CONTROLS TO IMPLEMENT THE FISC ORDER
AUTHORIZING NSA TO COLLECT INFORMATION USING
PEN REGISTER AND TRAP AND TRACE DEVICES**

~~(TS//SI//STLW//NF/OC)~~ **Background:** On 14 July 2004, the Foreign Intelligence Surveillance Court (FISC) issued a court order (the Order) granting the NSA the authority to install and use pen registers and trap and trace (PRTT) devices to collect the addressing and routing information of internet-based communications.

The Order establishes strict procedures governing the collection and use of, as well as access to, the data. This report assesses the general adequacy of management controls to ensure that the Agency complies with the terms of the Order. The effectiveness of management controls will be addressed in a subsequent report.

(b) (1)

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

(b) (3) - 50 USC 3024(i)

SUMMARY

~~(TS//SI//STLW//NF/OC)~~ *The management controls designed by the Agency to govern the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order. Due to the risk associated with the processing of electronic communications metadata involving U.S. person information, additional controls are needed for processing and monitoring of queries made against PRTT data, documenting oversight activities, and providing annual refresher training on the terms of the Order.*

~~(S//SI)~~ Includes all e-mail communications

(b) (1)

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

~~(TS//SI//NF)~~ The current version of the Order

(U) Criteria

~~(TS//SI//STLW//NF//OC)~~ **The Order.** The Order in effect during the time period of our review was issued on [REDACTED] expired on [REDACTED]. It authorized the Agency to:

(b)(1)

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

- collect and retain electronic communications metadata using pen registers and trap and trace devices to protect against international terrorism, and

- process and disseminate this data [REDACTED]

(b) (1)

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

(b) (3) - 50 USC 3024(i)

~~(TS//SI//NF)~~ Since the first order was signed in July 2004, the FISC has issued subsequent orders every ninety days. Although the specific terms and requirements of each order sometimes changed, the core authority—to collect and retain electronic communications metadata in the United States using pen registers and trap and trace devices—remains. Appendix B summarizes the significant changes since the first Order was signed.

~~(TS//SI//STLW//OC//NF)~~ To protect U.S. privacy rights, the Order specifies terms and restrictions regarding the collection, processing, retention,³ dissemination, and data security of electronic communications metadata and U.S. person information obtained under the Order. To ensure compliance with these terms and restrictions, the Order also mandates Agency management to implement a series of procedures to control the collection of data and the access to and use of the archived data collected pursuant to the Order. These control procedures are clearly stated in the Order. Appendix C summarizes the key terms of the Order and the related mandated control procedures.

(U) Standards of Internal Control. Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations. The General Accounting Office's *Standards for Internal Control in the Federal Government*, November 1999 (the Standards), presents the standards that define the minimum level of quality acceptable for management control in government. NSA/CSS Policy 7-3, *Internal Control Program*, April 14, 2006, advises that evaluations of internal control should consider the requirements outlined by the Standards.

~~(TS//SI//NF)~~ We did not assess the controls over retention at this time as the Order allows data to be retained for 4½ years.

The Office of the Inspector General (OIG) uses the Standards as the basis against which management control is evaluated.

(U) Assessment Results

~~(TS//SI//NF)~~ Agency management implemented all of the control procedures specifically mandated by the Order. (See Appendix C.) Agency management also built on some of those mandated procedures to establish rigorous processes to ensure compliance with the overall terms of the Order. For example, [REDACTED]

[REDACTED]

[REDACTED] In addition, processes to document Shift Coordinator and Office of General Counsel (OGC) justifications and approvals demonstrate the Agency's diligence and rigor in assessing whether seed addresses meet the terms of the Order.

~~(TS//SI//NF)~~ In general, controls over collection, dissemination, and data security were adequate to ensure compliance with key terms of the Order. However, the following control weaknesses and needed improvements regarding processing and oversight exist:

- The authority to approve queries made against PRTT data should be separated from the capability to conduct queries.
- The SIGINT Directorate (SID) Office of Oversight and Compliance (O&C) monitoring of PRTT queries is ineffective.
- Improvements are needed to document OGC spot checks and monitoring of collection data, audit log functioning, and access lists.
- Agency management should provide annual advanced intelligence oversight training on the Order to comply with Agency and DoD policy.

(U//FOUO) Details of these issues are discussed below.

~~(TS//SI//NF)~~ The Authority to Approve Queries Made Against PRTT Data Should be Separated from the Capability to Conduct Queries

~~(TS//SI//NF)~~ Two Shift Coordinators in the CT Advanced Analysis Division (AAD) each have both the authority to approve the querying

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

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

[REDACTED] under the Order and the capability to conduct queries. *The Standards of Internal Control in the Federal Government* require that key duties and responsibilities be divided among different people to reduce the risk of error or fraud. In particular, responsibilities for authorizing transactions should be separate from processing and recording them. This lack of segregation of duties increases the risk that the Shift Coordinators will approve and query, either by error or intent, addresses that do not meet the terms of the Order.

Recommendation 1

~~(TS//SI)~~ Separate the authority to approve queries from the capability to conduct queries under the Order.

(ACTION: Chief, Counterterrorism Primary Production Center)

(U) Management Response

CONCUR. ~~(TS//SI//STLW/NF)~~ Though management concurred with the finding, it did not concur with the recommendation because Shift Coordinators occasionally need to query against PRTT data in emergency situations or during off hours. As an alternative control, management recommended that Shift Coordinators retain querying capability but that O&C routinely review their queries to ensure compliance with the Order.

Status: OPEN

Target Completion Date: [REDACTED]

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

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

~~(TS//SI//NF)~~ O&C Monitoring Does Not Provide Reasonable Assurance that PRTT Queries Comply with Key Terms of the Order

~~(TS//SI//NF)~~ In accordance with DIRNSA's declaration dated [REDACTED] 2004, which stated that O&C will periodically review the PRTT program, O&C personnel conducted periodic spot checks to verify that ad hoc queries made by analysts with access to PRTT data

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

were approved by a Shift Coordinator.² Although O&C monitoring of PRTT queries has the potential to be a strong and valuable compliance control, it is largely ineffective because SID management did not establish a comprehensive monitoring methodology designed for that purpose. Although there are no indications that violations have occurred, O&C monitoring does not provide reasonable assurance that PRTT queries comply with the following key terms of the Order:

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

- All queries made against PRTT data must meet the terms of the Order [redacted]
- Shift Coordinators must approve the foreign seed addresses of all queries made against PRTT data.
- OGC must approve U.S. seed addresses of queries made against PRTT data.
- Analysts may query to no more than two hops from the seed address.

(U) Monitoring is Essential to Effective Internal Control

~~(TS//SI//NF)~~ Monitoring is one of the five standards of internal control. Specifically, *The Standards of Internal Control in the Federal Government* states that monitoring includes regular management and supervisory activities, such as ongoing comparisons and reconciliations, to determine whether internal control is functioning properly. Effective monitoring makes management aware of inaccuracies, exceptions, or violations that could indicate internal control problems. Monitoring is the best means to verify compliance of PRTT queries because preventive controls are not practical.

~~(TS//SI//NF)~~ SID Management did not Establish a Comprehensive Monitoring Methodology

~~(TS//SI//NF)~~ O&C monitoring of PRTT queries is ineffective because SID management did not establish a comprehensive methodology to monitor compliance with four key terms of the Order. Developing a methodology requires identifying all the terms of the Order to be monitored, determining the most effective monitoring techniques, and identifying key data, format, and report requirements. Rather,

²~~(TS//SI//NF)~~ At the time of our review, O&C was transitioning to a new process to monitor PRTT queries and developing written procedures. Because O&C did not document spot check results or the procedures followed, we could not assess the overall adequacy of the monitoring conducted prior to our review. Our results are therefore based solely on the newly implemented process.

O&C personnel spot-checked PRIT queries based on the type and format of audit log data that was already available and on the concept of "superauditing" SIGINT queries. Superauditing consists of O&C personnel spot-checking SIGINT queries that have already been reviewed by an analyst's supervisor. As a result, SID management did not use effective monitoring techniques, did not have the data and reporting elements it needed to conduct effective monitoring, and based its monitoring on incomplete or inaccurate data.

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

~~(TS//SI//NF)~~ **Spot checks are insufficient to assess compliance with the Order.** To effectively monitor over [redacted] PRIT queries conducted per month, spot checks of [redacted] per 30-day period do not include enough data to draw reasonable conclusions on the Agency's overall compliance. Rather, monitoring techniques such as reconciliation or statistical sampling are more appropriate in that they either include a sufficient portion of the population, or take into account the risk that the sampled queries do not represent the entire population. [redacted]

Using spot checks as the only monitoring technique, O&C cannot provide reasonable assurance that the Agency complies with terms of the Order.

~~(TS//SI//NF)~~ O&C personnel acknowledged that "superauditing" is problematic in that PRIT queries, unlike SIGINT keyword queries, do not undergo front-line audits by supervisors. O&C personnel also agreed that reconciliation of PRIT queries to approved seed addresses is the preferred technique to monitor compliance with the Order and expressed frustration that audit log data could not be easily reconciled with records of approved seed addresses. At the time of our review, O&C was working with AAD to develop the report formats needed to conduct more effective monitoring.

~~(TS//SI//NF)~~ **Audit log reports do not consistently and accurately document originating seed addresses.** [redacted]

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

[redacted] Unmatched or missing seed addresses are not, in and of themselves, violations of the Order. Rather, because we do not know the seed addresses, we do not know whether a Shift Coordinator had approved them. Thus, O&C monitoring cannot provide reasonable assurance that [redacted] of the queries comply with two key terms of the Order. Specifically, because the audit logs

do not consistently and accurately document originating seed addresses, management cannot verify that:

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

- all queries made against PRIT data are traceable to seed addresses that meet the terms of the Order [redacted] and [redacted]
- a Shift Coordinator approved the originating seed addresses of all queries made against PRIT data.

~~(TS//SI//NF)~~ **Audit log reports are incomplete.** The audit log reports that ●&C spot-checks do not include all queries made against PRIT data. The reports include only the queries of analysts that the Program Management Office (PMO) lists as being approved for access to PRIT data. This data is incomplete because it does not include queries of excluded individuals—those that have the ability to query the PRIT data but are not on the PMO list or who are not analysts. For example, in one instance, the PMO list had not been updated to include two individuals who had just been granted access to PRIT data. Although the error was eventually caught and corrected by management, the audit log report was initially generated without including the two newly added individuals. Two systems administrators, who have the ability to query PRIT data, were also omitted from the audit log reports. Because all potential queries made against PRIT data are not included in the log reports, management cannot provide reasonable assurance of compliance with the Order.

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

~~(TS//SI//NF)~~ **Audit logs do not capture needed data.**⁵ Raw [redacted] audit logs comply with the terms of the Order by recording all queries made against PRIT data, including user login, IP address, date and time, and retrieval request. However, the audit logs do not capture critical data to verify compliance with two key terms of the Order. Specifically,

- ~~(TS//SI//NF)~~ Management cannot verify that OGC approved the originating U.S. seed addresses of queries made against PRIT data because the audit logs do not distinguish between U.S. and foreign addresses.
- ~~(TS//SI//NF)~~ Management cannot verify that analysts query to no more than two hops out because the audit logs

⁵~~(TS//SI//NF)~~ In response to a related recommendation in the OIG Report on the *Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court (FISC) Order: Telephony Business Records* (SI-06-0018), September 5, 2006, Agency management indicated that limited programming resources have prevented them from identifying and making changes to raw [redacted] audit logs that would facilitate periodic reconciliations. Action is contingent on the approval of a pending request to SID management to detail two computer programmers to the team.

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

do not track the number of hops from an originating seed address.

~~(TS//SI)~~ SID management did not identify the needed data, did not request changes be made to the audit logs to capture the data, and made no attempt to verify compliance with these two terms of the Order.

Recommendation 2

~~(TS//SI)~~ Restructure the raw [] audit logs to capture needed data, such as originating seed address, U.S. identifiers, number of hops, and PRTT identifiers.

(ACTION: [] with Chief, SID Oversight and Compliance)

(U) Management Response

CONCUR. ~~(TS//SI//STLW/NF)~~ The PMO and O&C concurred with the finding and recommendation. [] did not respond directly to the draft report, and no details were provided on its plans to implement the recommendation. Rather, O&C stated that it had provided its data requirements to the PMO. The Chief of the Advanced Analysis Division added that the database now distinguishes between U.S. and foreign addresses, so O&C can now monitor ●GC approval of U.S. seed addresses.

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

Status: **OPEN**

Target Completion Date: []

(U) OIG Comment

~~(U//FOUO)~~ Because we did not receive detailed plans from [] we cannot determine whether planned action meets the intent of the recommendation.

Recommendation 3

~~(TS//SI)~~ Establish, document, and implement procedures to monitor PRTT queries.

(ACTION: Chief, SID Oversight & Compliance)

(U) Management Response

CONCUR. ~~(TS//SI//STLW/NF)~~ O&C concurred with the finding and recommendation. Although it had developed a foundational document for monitoring PRTT queries, O&C emphasized that successful implementation depends on the completion of Recommendation 2.

Status: **OPEN**

Target Completion Date:

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

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

~~(TS//SI//NF)~~ Improvements Are Needed to Document Oversight Activities

~~(TS//SI//NF)~~ Documentation of certain oversight activities is not being maintained. In addition to specific controls, the Order mandates that the OGC conduct specific oversight activities: random spot checks of collected data, monitoring of the audit log function, and monitoring of individuals with access to PRTT data.

~~(TS//SI//NF)~~ OGC Does Not Document Mandated Spot Checks of Collection Data and Monitoring of the Audit Log Function

~~(TS//SI//NF)~~ As mandated by the Order, OGC periodically conducts random spot checks of the data collected and **(b)(1)** monitors the audit log function. OGC does not, however, document **(b)(3)-P.L. 86-36** the date, scope, or results of the reviews. The purpose of the spot **(b)(3)-50 USC 3024(i)** checks is to ensure that filters and other controls in place on the are functioning as described by the Order and that only court authorized data is retained. The purpose of monitoring the audit log function is to retain data needed to audit queries conducted under the Order. Currently, an OGC attorney

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

meets with the individuals responsible [redacted] and audit log functions and reviews samples of the data to determine compliance with the Order. The attorney stated that she would formally document the reviews only if there were violations or other discrepancies of note. To date, OGC has found no violations or discrepancies.

(U//~~FOUO~~) NSA/CSS Policy 7-3 requires management to document internal control systems and conduct internal control assessments. Documentation of internal control systems includes review documentation that shows the scope of review, the responsible official, the pertinent dates and facts, the key findings, and the recommended corrective actions.

~~(TS//SI//NF)~~ Without adequate documentation of court-ordered reviews, the Agency does not have readily available and verifiable evidence of its compliance with the Order.

Recommendation 4

~~(TS//SI)~~ Maintain documentation of spot checks of collection data and monitoring of audit logs functions to include:

- Date of the review,
- Time period reviewed,
- Source of the data (i.e. personnel assisting OGC), and
- Results and corrective actions, if needed.

(ACTION: NSA Office of the General Counsel)

(U) Management Response

CONCUR. ~~(TS//SI//STW/NF)~~ OGC concurred with the finding and recommendation and stated that it will begin documenting spot checks.

Status: **OPEN**

Target Completion Date: [redacted]

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

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

~~(TS//SI//NF)~~ **OGC Does Not Maintain Documentation of Data Access Monitoring Activities**

~~(TS//SI//NF)~~ Although the OGC is notified when the PMO has approved a request for PRTT data access, it does not maintain documentation that individuals being approved for access have obtained the required OGC briefing. The Order requires OGC to monitor the designation of individuals with access to the PRTT data. The *Standards for Internal Control in the Federal Government* states that "internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination." The lack of readily available documentation makes it difficult to effectively monitor who has access to PRTT data.

~~(TS//SI//NF)~~ Further, the *Standards for Internal Control in the Federal Government* defines monitoring to include comparisons and reconciliations. Periodically, Program management compares a list of system users with PRTT data access (system list) to a list of analysts approved by the PMO for access (PMO list). OGC conducts a similar review of the PMO list; however, there is no OGC-maintained list to compare against. Instead, the attorney conducting the review relies on memory to verify the accuracy and completeness of the list. Although the same attorney normally conducts all briefings and reviews the lists, during one review, the attorney did not recognize the name of one person on the PMO list. Upon further investigation, the attorney discovered that another operations attorney, who was properly cleared and familiar with the requirements of the order, had briefed the analyst. This was confirmed in the briefing attorney's calendar.

~~(TS//SI//NF)~~ When performing a review of individuals with access to the PRTT data, the OGC attorney is using the PMO list rather than the system list. Although only approved individuals should have access to the PRTT data, the system list shows which individuals are actually authorized in the system to query the data, including any analysts or other users who may not be approved by the PMO.

Recommendation 5

~~(TS//SI)~~ Maintain a list of individuals who have been briefed on the proper use of the PRTT data and periodically reconcile that list with both the system list and the PMO list.

(ACTION: NSA Office of the General Counsel)

(U) Management Response

CONCUR. ~~(TS//SI//STLW/NF)~~ OGC did not agree that reconciliation is needed to effectively monitor the designation of individuals with access to the PRIT data. It did, however, concur with the recommendation and agreed to a proposal made by the PMO to replicate the PMO list in the Lotus Notes Tracker Program, a program for which the OGC has restricted access, and automate a process to reconcile the lists weekly.

Status: **OPEN**

Target Completion Date:

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

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

~~(TS//SI//NF)~~ Annual Advanced Intelligence Oversight Training on the Order Is Needed to Comply with NSA Policy

~~(S//SI)~~ SID management does not provide annual refresher training on the terms of the Order to appropriate personnel. Such training constitutes advanced Intelligence Oversight training as defined by NSA/CSS Policy 1-23, *Procedures Governing NSA/CSS Activities that Affect U.S. Persons*, March 11, 2004. Specifically, NSA/CSS Policy 1-23 requires that the SIGINT Director:

(U) ... provide training to all employees (including contractors and integrators) in order to maintain a high degree of sensitivity to, and understanding of, the laws and authorities referenced in this Policy. Such training shall include both core and advanced intelligence oversight training and refresher training with appropriate testing. All employees shall receive core training, and those with exposure to U.S. person information shall receive appropriate advanced training. Training shall be required at least annually (or more often commensurate with the

level of exposure to U.S. person information by the employee).

~~(S//SI)~~ As mentioned, OGC briefs individuals on the terms of the Order when they are granted access to PRIT data. OGC also forwards, by e-mail, copies of newly issued orders to key personnel in [redacted] and AAD. The PMO, in turn, posts the Order on a website accessible to cleared personnel; however, because the e-mails do not include detailed explanations of changes made to the Order, they do not constitute advanced training. No additional refresher training on the Order is provided. As a result, the SIGINT Director does not comply with Agency policy and risks violations of the Order by individuals who do not fully understand the terms of the Order.

(b) (1)

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

Recommendation 6

~~(TS//SI)~~ Conduct annual advanced intelligence oversight refresher training to analysts and collectors on the terms of the Order as required by NSA/CSS Policy 1-23.

(ACTION: SIGINT Director)

(U) Management Response

CONCUR. ~~(TS//SI//STLW/NF)~~ O&C tentatively concurred with the finding and recommendation but had not yet formally coordinated with the SIGINT Director or OGC.

Status: **OPEN**

Target Completion Date: [redacted]

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

(U) OIG Comment

(U) Because management did not provide details, we cannot determine whether planned action meets the intent of the recommendation.

(U) Conclusion

~~(TS//SI//NF)~~ The authority for the Agency to obtain and query on bulk address and routing information on electronic communications is extraordinary. Activities conducted under the Order are thus extremely sensitive. The Agency must take this responsibility

seriously and show good faith in its execution. Much of the foundation for a strong control system is set up by the Order itself, in the form of mandated control procedures, and, in many ways, Agency management has made the controls even stronger. Our recommendations will address control weaknesses not covered by the Order or Agency management and will meet Federal standards for internal control and Agency regulations. Once the noted weaknesses are addressed, and additional controls are implemented, the management control system will provide reasonable assurance that the terms of the Order will not be violated.

APPENDIX A

(U) About the Audit

This page intentionally left blank

(U) ABOUT THE AUDIT

(U) Objectives

~~(TS//SI)~~ The overall objectives of this review were to:

- assess whether management controls are adequate to provide reasonable assurance that NSA complies with the terms of the PR/TT Order, and
- verify that control procedures mandated in the PR/TT Order are in place.

(U) Scope and Methodology

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

~~(U//FOUO)~~ The audit was conducted from [REDACTED]

~~(TS//SI)~~ We interviewed Agency personnel and reviewed documentation to satisfy the review objectives. We conducted limited testing of audit log data of PRTT queries to assess the effectiveness of controls.

~~(TS//SI)~~ As footnoted, we did not assess controls related to the retention of Internet metadata pursuant to the Order. As the Order authorizes NSA to retain data for up to 4½ years, such controls are not applicable at this time.

(U) OIG Investigation of Violations of PRTT Orders

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

~~(TS//SI)~~ On [REDACTED] the OIG issued a report of the findings from an investigation into violations of the PRTT Order, 14 July 2004 (PR/TT [REDACTED]). The OIG investigation began on [REDACTED] after the OGC notified the OIG that a violation occurred. The violation was first noticed on [REDACTED] and occurred as a result of [REDACTED]. The investigation determined the cause of the violation and the extent to which unauthorized collection occurred.

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

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

~~(TS//SI)~~ The OIG report of investigation does not make formal recommendations to management. Rather, the report summarizes key facts and evaluates responsibility for the violation. This review confirms that management has taken steps to prevent recurrence of the violation. In particular, management now continuously monitors [REDACTED] [REDACTED] that might result in violations. This review also

identified, however, two areas that were cited in the report of the investigation that still need improvement:

- Although O&C has become more involved in monitoring PRIT queries, additional action is needed to make the monitoring effective.
- While personnel are notified of changes in renewals of the PRIT Order and new orders are posted on a centralized website, refresher training is still needed to ensure that NSA personnel implement the Order correctly.

APPENDIX B

(U//~~FOUO~~) Summary of Changes to the PRTT Orders

This page intentionally left blank

**(U//FOUO) SUMMARY OF CHANGES TO
THE PRTT ORDERS**

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

Order Number	Effective Dates	Changes from Previous Order
(b)(1) (b)(3)-P.L. 86-36		Initial Order. Authorized NSA to collect and retain Internet metadata to protect against international terrorism, and to process and disseminate this data regarding [redacted] with certain restrictions. [redacted]
		<ul style="list-style-type: none"> • [redacted] • Increased the number of analysts allowed access to the metadata from 10 to 15. • Added OGC spot checks of the incoming data. • Added a 30-day reporting requirement.
		No changes
		Added reference to [redacted] Order that prohibits querying on STELLARWIND-derived "seeds."
		<ul style="list-style-type: none"> • [redacted] • Added requirement to discuss the nature of the data collected on [redacted] in the 30-day report.
		No changes (b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)
		No changes
		<ul style="list-style-type: none"> • [redacted] • Changed on-line retention period from 18 months to 4.5 years. There was no effect on the overall retention period. Data must be destroyed after 4.5 years.
		Added the stipulation that: "E-mail addresses that are currently the subject of FISC authorized electronic surveillance and/or physical search based on the FISC's finding of probable cause to believe that they are used by [redacted] shall be deemed approved for meta data querying without approval of an NSA official due to the FISC authorization" (page 12).
		<ul style="list-style-type: none"> • [redacted] • [redacted] • Increased the number of analysts allowed access to the metadata to from 15 to 20.

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

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

(U//FOUO) Primary Order is dated [redacted] however, all secondary orders are dated [redacted]

~~TOP SECRET//COMINT//STELLARWIND//ORCON//NOFORN//MR~~

This page intentionally left blank

APPENDIX C

(U//FOUO) Mandated Terms and Control Procedures

This page intentionally left blank

~~TOP SECRET//COMINT//STELLARWIND//ORCON//NOFORN//MR~~
 (U) PR/TT FISC Order (PR/TT [REDACTED])

(U) Terms and Mandated Control Procedures for NSA

Control Area I. Collection

(b) (1)

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

~~(TS//SI//ST//AW//NF)~~ I. Collection

(b)(1) (b)(3)-P.L. 86-36 Terms of the Order	Responsible Entity	Mandated Control Procedures
<p>A. The pen registers and trap and trace devices will be attached or applied to the following facilities: [REDACTED] (Pg 3-10, para 4 [REDACTED]) A detailed description of the data that should be included in each [REDACTED] is attached. (b) (1)</p> <p>The authority granted is within the United States. (Pg 12, Para (3)) (b) (3)-P.L. 86-36 (b) (3)-50 USC 3024 (a)</p>	PM/FOCI	<p>1. Every thirty (30) days during the authorized period of surveillance, NSA shall file with the Court a report that includes: (i) any changes in the description [REDACTED] and (ii) a description of the nature of the communications collected [REDACTED] and a statement of whether the filtering process is properly limiting acquisition to communications that are to or from authorized [REDACTED] (Pg 15 Para (5)(g))</p>
<p>B. Collection of the contents of such communications as defined by 18 U.S.C. §2510(5) is not authorized. (Pg 3-9, Para (1))</p> <p>Addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications, includes:</p> <ul style="list-style-type: none"> the "to," "from," "cc," and "bcc" fields for these communications <div data-bbox="122 737 723 982" style="border: 1px solid black; height: 100px; width: 100%;"></div>	<p>SSO</p> <p>PM/FOCI</p> <p>OGC</p>	<p>1. [REDACTED] electronic communications [REDACTED] process the electronic communications to extract and record only the routing and addressing information, but not the contents of the electronic communications [REDACTED] (Pg 3-10, Para 4 [REDACTED]) (b)(1) (b)(3)-P.L. 86-36</p> <p>2. In addition, should the United States seek renewal of the authorities requested herein, at that time it will file a report that includes: (i) detailed information regarding any new facilities proposed to be added to such authority; and (ii) any changes in the proposed means of collection [REDACTED] the pen register and/or trap and trace devices. (Pg 15 Para (5)(g))</p> <p>3. At least twice during the 90 day authorized period of surveillance, OGC will conduct random spot checks [REDACTED] to ensure that the collection is functioning as authorized by the Court. Such spot checks shall include an examination of a sample of the data. (Pg 16, Para (5)(d)(3))</p>

~~(TS//SI//ST//AW//NF)~~

~~TOP SECRET//COMINT//STELLARWIND//ORCON//NOFORN//MR~~

~~(SUSPENSIVE)~~ 1. Collection (continued)

Terms of the Order	Responsible Entity	Mandated Control Procedures
<p>C. Installation and use of pen registers and trap and trace devices as requested in the Government's application is authorized for a period of ninety days from the date of this Order, unless otherwise ordered by the Court. (Pp. 14, Para. (D)). This authorization [redacted]</p>	<p>PMD</p>	<p>None</p>

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

(b)(3)-P.L. 86-36 Control Area II: Processing

~~(CONFIDENTIAL)~~ II. Processing

Terms of the Order	Responsible Entity	Mandated Control Procedures
<p>A. Such queries shall be performed only on the basis of a particular known [redacted] after the NSA has concluded, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are facts giving rise to a reasonable articulable suspicion that such account or address is associated with [redacted]</p> <p>[redacted]</p> <p>Provide], however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. (Pg. 14, Para. (5)(c))</p>	<p>PMO</p> <p>OGC</p> <p>OGC</p> <p>PMO/OGC</p>	<p>1. The NSA shall ensure that the mechanism for accessing such information will automatically generate a log of auditing information for each occasion when the information is accessed. Its include the accessing user's login ID address, date and time, and retrieval request. (Pg. 13, Para. (5)(b))</p> <p>2. OGC shall monitor the functioning of the system after logging of auditing information required by [the order]. (Pg. 15, Para. (5)(d)(ii))</p> <p>3. OGC shall ensure that analysts with the ability to access such information receive appropriate training and guidance regarding the querying standard set out in [the order], as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information. (Pg. 15, Para. (5)(d)(i))</p> <p>4. Every thirty (30) days during the authorized period of surveillance, NSA shall file with the court a report that includes: (i) the discussion of queries that have been made since the prior report to the Court and the NSA's application of the standard set out in paragraph (a) above to those queries. (Pg. 15, Para. (5)(g))</p>
<p>(b) (1)</p> <p>(b) (3) - P.L. 86-36</p> <p>(b) (3) - 50 USC 3024(i)</p>		

4.1.3.4 This order, PR 14 is the first one that includes

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

~~(TS//SI//STELW//NF)~~ II. Processing (continued)

Terms of the Order	Responsible Entity	Mandated Control Procedures
<p>A (continued)</p> <p>(b) (1) (b) (3)-P.L. 86-36 (b) (3)-50 USC 3024(i)</p>	<p>OGC</p> <p>PMO</p>	<p>5. OGC shall, to ensure appropriate consideration of any First Amendment issues, review and approve proposed queries of metadata [redacted] based on seed accounts used by U.S. persons. (Pg. 16, Para. (b)(1)(i)). It shall be memorandum to NSA's Office of General Counsel; 6. review the legal adequacy for the bases of such queries, including the First Amendment provision set out in paragraph c, above (Pg. 16, Footnote 13)</p> <p>6. Queries shall only be conducted with the approval of one of the following NSA officials: the Signals Intelligence Directorate Program Manager for Counterterrorism Special Projects; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or a Counterterrorism Advanced Analysis Unit Coordinator in the Analysis and Production Directorate of the Signals Intelligence Directorate. (Pg. 16, Para. (5)(c))</p>
<p>B. Such information shall be accessed only through queries using the contact chaining [redacted] methods described at page 13 of the Court's July 14, 2004 Opinion and Order in Docket No. PR-11 [redacted] (Pg. 14, Para. (5)(c))</p>	<p>AAD</p>	<p>7. None</p>

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

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

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

~~(TS//SI//STELW//NF)~~ Contact chaining. NSA will use computer algorithms to identify within the archive metadata all [redacted] accounts that have been in contact with the seed account, as well as all accounts that have been in contact within the first tier of accounts that had direct contact with the seed account. [redacted] (Pg. 43, Para. (1) of the Court's July 14, 2004 Opinion and Order in Docket No. PR-11 [redacted])

³ (TS//SI//NF)

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

~~(TS//SI//STLAW//NF)~~ II. Processing (continued)

Terms of the Order

- C. Further, all meta data queries shall be performed in accordance with this Court's [redacted] Orders in Docket Numbers [redacted] (Pg. 14, Para. (5)(c)).
- NSA shall not query the meta data collected under the authorities granted in the above referenced dockets (hereinafter "FISA meta data") on the basis of any "seed" [redacted] that has been validated using information obtained from SW collection. Paragraph 12 of the [redacted] Order prohibited NSA from using SW information to validate any seed [redacted] such prohibition remains in effect. (Pg. 1, Para. (1) of [redacted]).
 - In addition, NSA is hereby prohibited from accessing FISA meta data in any manner [redacted] based on seed [redacted] [redacted] previously validated through use of SW information. (Pg. 2, Para. (1) of [redacted]).
 - NSA is still authorized to query FISA meta data on the basis of seed [redacted] validated without the use of SW information including, but not limited to, [redacted] [redacted] (Pg. 2, Para. (1) of [redacted]).
 - The government is directed to advise the Court immediately of any instance where, contrary to this understanding, information from FISA meta data was included in an application to this Court (other than in the above-referenced dockets). For any such instance, the government shall advise whether the FISA meta data was obtained from a query based on a seed [redacted] that was validated through the use of SW information. (Pg. 1, Para. (3) of [redacted]).

Responsible Entity

A-AD

PMAC/CI

Mandated Control Procedures

1. None

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

2. The government was ordered to submit a description of procedures for processing applications and advising the court of instances where FISA meta data was included in an application to the Court. (Pg. 3, Para. (3) of [redacted]).
3. Before implementing any change to those procedures, the government will submit a written explanation of the new procedures and how they will adequately ensure adherence to the objectives described at pages 1-5 of the [redacted] letter. (Pg. 1, Para. (4) of [redacted]).

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

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

~~TOP SECRET//COMINT//STELLARWIND//ORCON//NOFORN//MR~~~~(TS//SI//STLW//NF)~~ II. Processing (continued)

Terms of the Order	Responsible Entity	Mandated Control Procedures
<p>D. E-mail addresses that are currently the subject of FISC authorized electronic surveillance and/or physical search based on the FISC's finding of probable cause to believe that they are used by [REDACTED] including those used by U.S. persons, shall be deemed approved for meta data querying without approval of an NSA official due to the FISC authorization. (P) 15, Para (5)(c)</p>	<p>AAD</p> <p>(b) (1) (b) (3) - P.L. 86-36 (b) (3) - 50 USC 3024(i)</p>	<p>None</p>

~~(TS//SI//STLW//NF)~~**Control Area III: Dissemination**~~(TS//SI//STLW//NF)~~

Terms of the Order	Responsible Entity	Mandated Control Procedures
<p>A. The NSA shall apply the Attorney General approved guidelines in United States Signals Intelligence Directive 18 (Attachment D) to the application in Docket No. PR 11 [REDACTED] to minimize information concerning U.S. persons obtained from the patch users and trap and trace devices authorized hereto. (P) 16, Para (5)(c)</p>	<p>AAD & ORC</p>	<p>Prior to disseminating any U.S. person information outside of the NSA, the Chief of Information Systems Services in the NSA's Signals Intelligence Directorate shall determine that the information is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance. (P) 16, Para (5)(e)</p>

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

~~(TS//SI//STLW//NF)~~~~TOP SECRET//COMINT//STELLARWIND//ORCON//NOFORN//MR~~

Control Area IV: Retention

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

Terms of the Order	Responsible Entity	Mandated Control Procedures
A. Information obtained from the authorized pen registers and trap and trace devices shall be available online for querying, as described in the Order, for four and one half years. Metadata shall be destroyed no later than four and one half years after its initial collection. (Pg. 17, Para (S)(4))	<input type="checkbox"/> & Technical Support	1. None

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

Control Area V: Data Security (b) (3) - P.L. 86-36

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

Terms of the Order	Responsible Entity	Mandated Control Procedures
A. The NSA shall store such information in a manner that ensures that it will not be commingled with other data. (Pg. 15 Para (S)(a))	OGC	1. OGC shall monitor the designation of individuals with access to such information under the order. (Pg. 15, Para (S)(d)(ii))
B. The ability to retrieve information derived from the pen register and trap and trace devices shall be limited to twenty ⁹ specially cleared analysts and to specially cleared administrators. (Pg. 14 Para (S)(b))	<input type="checkbox"/> & Technical Support	2. None

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

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

⁹ Retention was not part of this review.
¹⁰ PR/TE ☐ increased the number of people with PR/TE data access to 20.



~~SECRET//NOFORN~~
NATIONAL SECURITY AGENCY

FORT GEORGE G. MEADE, MARYLAND 20755-6000

19 December 2012

The Honorable Saxby Chambliss
Vice Chairman, Select Committee
on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Vice Chairman:

(U//~~FOUO~~) Section 702 (1) (2) of the FISA Amendments Act of 2008 (FAA) authorizes the National Security Agency/Central Security Service (NSA/CSS) Office of the Inspector General (OIG) to assess the Agency's compliance with procedures for targeting certain persons, other than U.S. persons (USPs), outside the United States. My office reviews the collection, processing, and reporting of data at least quarterly. Incidents involving compliance with procedures for targeting certain persons, other than USPs, outside the United States and incidents involving minimization of USP information are reported to the OIG as they occur and quarterly. Each incident is evaluated against the targeting and minimization procedures set forth in the FAA and in NSA/CSS directives. This report covers 1 September 2011 through 31 August 2012.

(U//~~FOUO~~) The OIG completed the Special Study: Assessment of Management Controls Over FAA §702. This study examined the design of these management controls; future studies will test the identified controls.

(b)(1)

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

(S//NF) In compliance with the targeting and minimization procedures of §702 of the FAA, [redacted] intelligence reports were disseminated by NSA/CSS [redacted] based on SIGINT derived from FAA §702 authorized collection.¹ Of the [redacted] disseminated reports, [redacted] contained one or more references to U.S. persons.² This number includes references to a United States electronic communications service provider as part of the

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

¹ (U//~~FOUO~~) These reports were based in whole or in part on information acquired pursuant to FAA §702(a).

² (U//~~FOUO~~) [redacted] the references to U.S.-person identities may have resulted from collection pursuant to FAA §702 or from other authorized Signals Intelligence activity conducted by NSA that was reported in conjunction with information acquired under FAA §702.

(S//NF) The Central Intelligence Agency (CIA) does not conduct acquisitions under FAA §702. However, it receives unminimized communications from NSA and FBI and disseminates information based on that information.

(b)(1)

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

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

communications identifier used by targets of this acquisition and other non-U.S. persons with whom they communicate. A communicant using email account targetA@USprovider.com was included here as a report referencing a U.S.-person identity. In February 2012, NSA stopped counting such communications identifiers as U.S. person identifiers if the user is a non-U.S. person. As a result, the number of intelligence reports containing one or more references to U.S. persons is significantly lower this year than last.³

~~(S//NF)~~ In addition, NSA/CSS released [] USP identities in response to customer requests for USP identities not referred to by name or title in the original reporting.⁴ (b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ During this reporting period, [] foreign targets reasonably believed to be located outside the United States at the time of tasking were later suspected or confirmed to be in the United States. In each instance, NSA/CSS targeted selectors that at the time of targeting were reasonably believed to be outside the United States but were later found to be []
the United States. []

(U//~~FOUO~~) Compliance incidents occurred under such circumstances as:

- (U//~~FOUO~~) Tasking under an incorrect certification,
- ~~(S//NF)~~ Errors in entry of the selector for tasking,
- (U//~~FOUO~~) Insufficient foreignness support,
- (U//~~FOUO~~) Dissemination errors,
- (U//~~FOUO~~) Poor construction of database queries, and
- (U//~~FOUO~~) USP status discovered post-tasking.

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

(U) Action has been taken to correct mistakes, and internal management processes have been reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of USP communications.

(U//~~FOUO~~) This is the fourth year for which the OIG has assessed for the Congress the Agency's compliance with FAA §702. To ensure consistency between the DIRNSA report and the OIG report, the OIG and SID worked together to achieve a common understanding of the

³ ~~(S//NF)~~ For the previous reporting period, NSA reported that [] intelligence reports contained one or more references to U.S. persons, including references to U.S. electronic communications providers as part of a communications identifier. (b)(1)
(b)(3)-P.L. 86-36

⁴ ~~(S//NF)~~ For the previous reporting period, NSA reported that there were [] identities disseminated in response to requests for identities not referred to by name or title in the original reporting. [] reports by the NSA/CSS Threat Operation Center account for [] of the increase. Approximately [] of these disseminated United States person identities were proper names of real persons or their titles; []

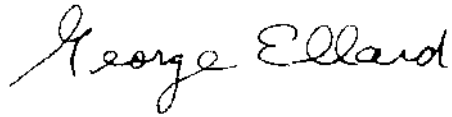
~~SECRET//NOFORN~~

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

~~SECRET//NOFORN~~

reporting requirements and have agreed on a methodology for accumulating and analyzing compliance statistics.

(U) The OIG continues to exercise oversight of Agency intelligence activities.

A handwritten signature in cursive script that reads "George Ellard".

GEORGE ELLARD
Inspector General

Copy Furnished:
The Honorable Dianne Feinstein
Chairman, Select Committee
on Intelligence

~~SECRET//NOFORN~~

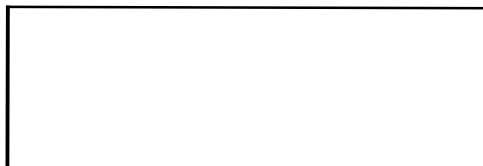
~~TOP SECRET//SI//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Report on the Special Study of NSA's
Purge of Pen Register and Trap and Trace Bulk
Metadata



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

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

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

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by statute and the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, and investigations and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as 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 assess whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests and complaints, at the behest of management, because of irregularities that surface during inspections and audits, or on the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

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

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

**OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE**

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

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Report on the Special Study of NSA's Purge of Pen Register and Trap and Trace Bulk Metadata [REDACTED] — ACTION (b)(3)-P.L. 86-36
MEMORANDUM

1. ~~(TS//SI//NF)~~ This advisory report summarizes the results of the review by the Office of the Inspector General of NSA's Purge of Pen Register and Trap and Trace Bulk Metadata [REDACTED].

2. ~~(TS//SI//NF)~~ On the basis of our observations and review of procedures and documentation, we determined with reasonable assurance that the Agency destroyed Pen Register and Trap and Trace (PR/TT) bulk metadata from its declared systems, databases, and tape and system backups disclosed to us before the PR/TT authority expired on 9 December 2011. Based on our review, no management response is required for this report.

3. (U) We appreciate the courtesy and cooperation extended to our staff throughout the review. For additional information, please contact Mr. [REDACTED] on 963-0922(s) or via e-mail at [REDACTED]

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

A handwritten signature in cursive script that reads "George Ellard".

George Ellard
Inspector General

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

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

(U) DISTRIBUTION:

DIRNSA

SID (T. Shea)

TD [REDACTED]

cc: EXDIR (F. Fleisch)

COS (D. Bonanni)

DOC (J. DeLong)

D4 [REDACTED]

OGC [REDACTED]

ST [REDACTED]

SV [REDACTED]

SV4 [REDACTED]

SV42 [REDACTED]

S3 [REDACTED]

S31323 [REDACTED]

S3531 [REDACTED]

TE [REDACTED]

TE6 [REDACTED]

TV [REDACTED]

TI [REDACTED]

T12 [REDACTED]

T121 [REDACTED]

T122 [REDACTED]

T1222 [REDACTED]

D4 IG POC [REDACTED]

OGC IG POC [REDACTED]

SID IG POC [REDACTED]

TD IG POC [REDACTED]

DL d-comply-tasker

DL SIDIGLIAISON

DL TD_REGISTRY

DOJ NSD [REDACTED]

(b)(6)

IG

D/IG

D1 [REDACTED]

D11

D12

D13

D14

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

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

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

NSA/CSS Office of the Inspector General ADVISORY REPORT

~~(TS//SI//NF)~~ SPECIAL STUDY OF THE AGENCY'S PURGE OF PEN REGISTER AND TRAP AND TRACE BULK METADATA

(U) Overview

~~(TS//SI//NF)~~ This report summarizes our special study of the Agency's processes to destroy Pen Register and Trap and Trace (PR/TT) bulk metadata from its declared systems, databases, and backups before the authority expired on 9 December 2011. On the basis of our observations and review of procedures and documentation, we conclude with reasonable assurance that the Agency destroyed PR/TT bulk metadata in the systems, databases, and backups disclosed to us.

(U) Background

(b)(1)

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

~~(TS//SI//NF)~~ Between July 2004 [redacted] to the expiration of the PR/TT authority on 9 December 2011, the National Security Agency (NSA), with the assistance of certain U.S. telecommunications service providers, collected, processed, and analyzed metadata from Internet communications to obtain foreign intelligence information about the international terrorist activities [redacted]

This activity occurred under a PR/TT authority (renewable every 90 days) granted by the Foreign Intelligence Surveillance Court (FISC).

(b)(1)

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

(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ In early 2011, the Signals Intelligence Directorate (SID) conducted an examination of the NSA PR/TT program to assess its value as a source of foreign intelligence information. That examination revealed that the PR/TT program was not producing valuable foreign intelligence information after the program had been reinitiated [redacted]

(b)(1)

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

~~(TS//SI//NF)~~ On [redacted] 2011, SID requested that the Director, NSA (DIRNSA) terminate the PR/TT program. SID recommended that NSA not renew the PR/TT authority and destroy all bulk metadata collected pursuant to the PR/TT authority. SID identified several limitations that contributed to the program's inability to meet expectations.


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

(b)(1)

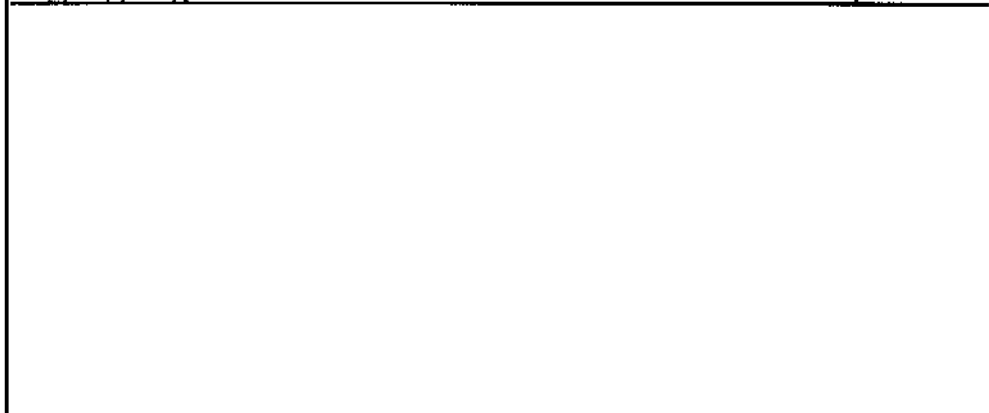
(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)


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

~~TOP SECRET//SI//NOFORN~~2. ~~(TS//SI//NF)~~ 

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




3. ~~(TS//SI//NF)~~ **Other authorities can satisfy certain foreign intelligence requirements that the PR/TT program was designed to meet.** The Supplemental Procedures Governing Communications Metadata Analysis (SPCMA), which SID implemented widely in late 2010, allows NSA to call-chain from, to, or through U.S. person selectors in Signals Intelligence collection obtained under a number of authorities. In addition, notwithstanding restrictions stemming from the FISC's recent concerns regarding upstream collection, FAA §702 has emerged as another critical source for collection of Internet communications of foreign terrorists. Thus, SPCMA and FAA §702 assist in the identification of terrorists communicating with individuals within the United States, which addresses one of the original reasons for establishing the PR/TT program in 2004.

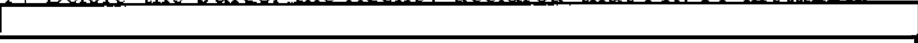
4. ~~(TS//SI//NF)~~ 

(U) DIRNSA's Decision

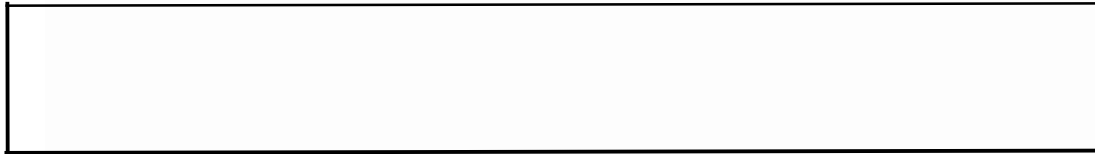
(b)(1)
 (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ On  2011, DIRNSA approved SID's request to allow the PR/TT Order to expire and to destroy all collected bulk metadata from the PR/TT program before the authority expired on 9 December 2011.

~~(TS//SI//NF)~~ NSA Systems and Repositories that Stored PR/TT Metadata

~~(TS//SI//NF)~~ Before the purge, the Agency declared that PR/TT metadata was stored 

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

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

1. ~~(TS//SI//NF)~~ [redacted] is the Agency's corporate database that ~~(b)(3)-P.L. 86-36~~ accepts metadata [redacted] into separate partitions, including PR/TT FISA. [redacted] contained the contact chain summaries and transaction records for PR/TT.

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

- ~~(TS//SI//NF)~~ [redacted] stored the contact chain summaries that document Internet communications between two persons. A contact chain summary shows that a person communicated with another person, their first and last contact dates, and the total number of communications between them.

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

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

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

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

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

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

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

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

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

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

~~TOP SECRET//SI//NOFORN~~~~(TS//SI//NF)~~ **Review of NSA's PR/TT Bulk Metadata Purge**

~~(TS//SI//NF)~~ The PR/TT metadata purge was performed from [] (b)(3)-P.L. 86-36 through 9 December 2011. On 2 December and 7 December 2011, the OIG independently observed the Agency's purge processes to destroy PR/TT bulk metadata from its declared systems, databases, and backups (as disclosed by TD). It is important to note that we lack the necessary system accesses and technical resources to search NSA's networks to independently verify that only the disclosed repositories stored PR/TT metadata. As a result, we completed our special study through observation and review of procedures and system documentation for the disclosed repositories only.

~~(TS//SI//NF)~~ During our study, we observed the Knowledge Services' [] Team (T1222) and T121 personnel perform system commands to purge PR/TT metadata from Agency systems and databases. At our request, TD personnel provided us with system documentation before and after the purge commands had been performed. This documentation showed that the file systems and tables that stored PR/TT metadata had been deleted from Agency systems and databases. We also observed T1222 submit the backup tapes for secure destruction and obtained copies of receipts signed by destruction personnel.

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

~~(TS//SI//NF)~~ However, S3 had completed its purge before we had the opportunity to observe. As a result, we were able to review the [] purge procedures only for reasonableness; we were not able to do the before and after comparisons that we did for the TD systems and databases disclosed to us. S3 did provide system documentation that showed PR/TT metadata files no longer resided in temporary memory of the [] system and confirmed that PR/TT dataflows had been terminated and all other purge procedures had been completed for [] systems according to plan. Refer to Table 1 for the six areas reviewed.

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

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

(U) Table 1. Special Study Results

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

Review Area	Org.	OIG Review Method	Procedures Adequately Performed?
Tape, disk, and system backup destruction practices	T1222	Observed T1222 submit backup tapes for secure destruction. Obtained copies of receipts signed by destruction personnel. Reviewed procedures and observed T1222 perform commands to purge [redacted] Obtained system documentation that showed that the file system had been deleted.	(b)(1) (b)(3)-P.L. 86-36 Yes
[redacted]	T1222	Reviewed procedures and observed T1222 perform commands to purge [redacted] [redacted] Obtained system documentation that showed that tables had been deleted.	Yes
[redacted]	T1222	Reviewed procedures and observed T1222 perform commands to purge [redacted] for [redacted] Obtained system documentation that showed that file systems had been deleted.	Yes
[redacted]	T1222	Reviewed procedures and observed T1222 perform commands to purge [redacted] [redacted] Obtained system documentation that showed that file systems had been deleted.	Yes
[redacted]	T121	Reviewed procedures and observed T121 perform commands to purge PR/TT metadata from directories and tables. Obtained system documentation that showed that directories, files, and tables had been purged of PR/TT metadata [redacted]	Yes
[redacted] Systems	S3	[redacted] purge procedures were reviewed only for reasonableness. S3 had completed its purge before we had the opportunity to observe. S3 subsequently provided system documentation that showed that PR/TT metadata files no longer resided in temporary memory of [redacted] and confirmed that PR/TT dataflows had been terminated and all other purge procedures had been completed according to plan.	Yes

~~(TS//SI//NF)~~**(U) Conclusion**

~~(TS//SI//NF)~~ On the basis of our observations and review of procedures and documentation, we conclude with reasonable assurance that the Agency destroyed PR/TT bulk metadata from its declared systems, databases, and tape and system backups disclosed to us before the PR/TT authority expired on 9 December 2011.

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

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

(U) This page intentionally left blank.

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

(U) APPENDIX

(U) T1222, T121, and S3 Purge Procedures

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~~~(TS//SI//NF)~~ Table A1. PR/TT Bulk Metadata Purge Procedures

(b)(1)

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

(TS//SI//NF)	
Dates	Procedure
	<p>[redacted] (S3) terminated [redacted] PR/TT dataflows, purged metadata, and powered down equipment.</p> <p>[redacted] query services [redacted] were deleted to prevent analysts from accessing PR/TT chain [redacted] data stored in [redacted]</p>
12/2/11	<p>Phase 1 – T1222's purge procedures to destroy PR/TT metadata collected [redacted]</p> <p>[redacted]</p> <ul style="list-style-type: none"> • [redacted] • [redacted] • [redacted] • [redacted] • [redacted] • [redacted] • [redacted]
12/7/11	<p>Phase 2 – T1222's purge procedures to destroy PR/TT metadata collected [redacted]</p> <p>[redacted]</p> <ul style="list-style-type: none"> • [redacted] • [redacted] • [redacted] • [redacted] • [redacted] • [redacted] • [redacted]
12/7/11	<p>T121's purge procedures to delete sample PR/TT metadata from the [redacted] system:</p> <ul style="list-style-type: none"> • [redacted] • [redacted] • [redacted] • [redacted] • [redacted] • [redacted]
12/9/11	[redacted]
<p>Note: Before the purge, the Agency had only PR/TT metadata [redacted]</p> <p>* PR/TT metadata obtained before [redacted] had not been saved to the [redacted]. As a result, no action was needed by T1222 for the [redacted] during the Phase 1 purge.</p> <p>† The entire [redacted] was deleted during the Phase 1 purge. As a result, no action was needed by T1222 [redacted] during the Phase 2 purge.</p> <p>‡ [redacted]</p> <p>§ [redacted]</p>	

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

(b)(1)

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

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

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

(U) This page intentionally left blank.

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

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

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

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

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



~~SECRET//REL TO USA, FVEY~~
 NATIONAL SECURITY AGENCY
 CENTRAL SECURITY SERVICE
 FORT GEORGE G. MEADE, MARYLAND 20755-6001

30 December 2011

The Honorable Michael J. Rogers
 Chairman, Permanent Select
 Committee on Intelligence
 United States House of Representatives
 Capitol Visitor Center HVC-304
 U.S. Capitol Building
 Washington, DC 20515-6415

Dear Representative Rogers:

(U//~~FOUO~~) The FISA Amendments Act of 2008 (FAA) authorizes the National Security Agency/Central Security Service (NSA/CSS) Office of the Inspector General (OIG) to assess the Agency's compliance with procedures for targeting certain persons, other than U.S. persons (USPs) outside the United States. My office reviews the collection, processing, and reporting of data at least quarterly. Incidents involving compliance with procedures for targeting certain persons, other than USPs, outside the United States and incidents involving minimization of USP information are reported to the OIG as they occur and quarterly. Each incident is evaluated against the targeting and minimization procedures set forth in the FAA and in NSA/CSS directives. This report covers 1 September 2010 through 31 August 2011.

(S//~~REL TO USA, FVEY~~) In compliance with the targeting and minimization procedures of §702 of the FAA, NSA/CSS disseminated intelligence reports based on SIGINT derived from FAA §702 authorized collection. Of the [] disseminated reports, [] contained a reference to a USP. In addition, NSA/CSS released [] USP identities in response to customer requests, some of which were not unique.

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

(S//~~REL TO USA, FVEY~~) During this reporting period, [] valid foreign targets who were reasonably believed to be located outside the United States at the time of tasking were later suspected or confirmed to be in the United States. In each instance, NSA/CSS targeted selectors that at the time of targeting were confirmed to be outside the United States but were later []

[]
 []
 [] Compliance incidents occurred under such circumstances

as:

- (U//~~FOUO~~) Delays in implementing minimization procedures and purging unauthorized collection.
- (U//~~FOUO~~) Analyst misunderstanding of the authority.
- (U//~~FOUO~~) Poor construction of database queries, and

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

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

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

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

- (U//~~FOUO~~) System errors.

(U) Action has been taken to correct mistakes, and internal management processes have been reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of USP communications.

(U//~~FOUO~~) This is the third year for which the OIG has assessed for the Congress the Agency's compliance with FAA §702. After the OIG filed its report for the year ending 31 August 2010, discrepancies were identified between the data provided to the OIG by the Signals Intelligence Directorate (SID) and similar information contained in a draft Agency Report of Annual Review Pursuant to Section 702(l) of the Foreign Intelligence Surveillance Act prepared by the NSA Office of General Counsel (OGC). It was determined that different methodologies had been used to provide the information. The statistics were compiled differently for the number of reports disseminated based on FAA §702 collection and for the number of USPs referenced in reporting. There were no differences in reporting for the number of USP identities released in response to customer requests.

(U//~~FOUO~~) The following table contains data for all three years of reporting using a consistent methodology. When reconstructing the data, we discovered that we were unable to confirm exactly how -- of several possible legitimate counting methods -- the numbers provided to us on USPs referenced in reporting for 2009 and 2010 had been compiled. For the current year and retrospectively for 2009 and 2010, the table reflects the total number of USP identities referenced in reports derived from FAA §702 collection, regardless of the number of times an individual identity was released or the number of USP identities per report. In addition, the 2010 data initially provided to us on the number of reports disseminated excluded reports produced by Signals Intelligence organizations outside NSA's headquarters complex [REDACTED]. [REDACTED] That number has been adjusted.

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

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

Report	Reports Disseminated Based on FAA §702 Collection	USPs Referenced in Reporting
September 2008 – August 2009	[REDACTED]	[REDACTED] (b)(1)
September 2009 – August 2010	[REDACTED]	[REDACTED] (b)(3)-P.L. 86-36
September 2010 – August 2011	[REDACTED]	[REDACTED]

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

(U//~~FOUO~~) To ensure consistency of reporting for the year ending 31 August 2011 and for future years, the OIG, OGC, and SID worked together to achieve a common understanding of the reporting requirements for the two reports and have agreed on a methodology for accumulating and analyzing the compliance statistics. The process has been standardized to ensure continued accuracy and is being documented for future reporting. The table above presents the reportable figures agreed on by the OIG and OGC for all three years for which reports have been required.

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

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

(U) The OIG continues to exercise oversight of Agency intelligence activities.

A handwritten signature in cursive script that reads "George Ellard".

GEORGE ELLARD
Inspector General

Copy Furnished:

The Honorable C.A. Ruppertsberger
Ranking Member, Permanent Select
Committee on Intelligence

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

~~SECRET//SI//NOFORN~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL
9800 Savage Road
OPS 2B, Suite 6247
Ft. George Meade, MD 20755-6247



20 December 2013

The Honorable Saxby Chambliss
Vice Chairman, Select Committee
on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Vice Chairman:

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

(U) Section 702 (l) (2) of the FISA Amendments Act of 2008 (FAA) authorizes the National Security Agency/Central Security Service (NSA/CSS) Office of the Inspector General (OIG) to assess the Agency's compliance with procedures for targeting non-U.S. persons outside the United States. My Office reviews incidents involving compliance with procedures for targeting non-U.S. persons outside the United States and incidents involving minimization of U.S. person information as they are reported to the OIG and quarterly. Each incident is evaluated against the targeting and minimization procedures adopted by the Director of National Intelligence and the Attorney General and approved by the Foreign Intelligence Surveillance Court. This letter covers the 12-month period ending 31 August 2013.

~~(S//SI//NF)~~ During that period, the OIG completed two reports on implementation of FAA §702. The first was an assessment of management controls over FAA §702, which examined the design of the management controls that ensure compliance with FAA §702 and the targeting and minimization procedures associated with the 2011 Certifications. Future studies will test the identified controls. The second report [REDACTED]

~~(S//NF)~~ In compliance with the targeting and minimization procedures of FAA §702, [REDACTED] intelligence reports were disseminated by NSA/CSS [REDACTED] based on SIGINT derived from FAA §702 authorized collection.¹ Of the [REDACTED] disseminated reports, [REDACTED] contained one or more references to USPs.² During the previous reporting period, NSA stopped counting references to U.S. service providers contained in an e-mail address as a USP reference if the e-mail address was used by a non-USP. For example, a reference in a disseminated report that target A communicated using e-mail account targetA@USprovider.com is no

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

¹ (U) These reports were based in whole or in part on information acquired pursuant to FAA §702(a).

² (U) [REDACTED]

[REDACTED] the references to USP identities might have resulted from collection pursuant to FAA §702 or from other authorized SIGINT activity conducted by NSA that was reported in conjunction with information acquired under FAA §702.

~~(S//NF)~~ The Central Intelligence Agency (CIA) does not conduct acquisitions under FAA §702. However, it receives unminimized communications from NSA and FBI and disseminates information based on those communications. [REDACTED]

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

~~SECRET//SI//NOFORN~~

~~SECRET//SI//NOFORN~~

longer included as a report referencing a USP identity, if target A is a non-USP. Because this change was in effect for the entirety of the current reporting period, the total number of NSA intelligence reports counted for this report as containing one or more references to USPs is significantly lower than last year.²

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

(U//FOUO) NSA/CSS released [] USP identities in response to customer requests for USP identities not referred to by name or title in the original reporting.³ The majority of these requests were received from elements of the United States Intelligence Community or federal law enforcement agencies. (b) (1)

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

(S//NF) During this reporting period, NSA determined that, on [] occasions, selectors belonging to non-USPs reasonably believed to be located outside the United States at the time of tasking were later suspected or confirmed to be []

(S//SI//NF) [] DoJ filed a preliminary notice of compliance incident with the FISC that advised the Court that []

(U) As reported in the OIG's quarterly report to the President's Intelligence Oversight Board on NSA activities, compliance incidents occurred under such circumstances as:

- (U) Tasked selector not meeting the requirements of the certification
- (U) System errors resulting in improper storage or access
- (U) Delayed detasking of targets identified as USPs or traveling in the United States
- (U) Dissemination errors
- (U) Poor construction of database queries and
- (U) USP status discovered post-tasking. (b)(1)

(b) (1)

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

(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

(b) (3)-50 USC 3024(i)

(S//NF) For the previous reporting period, NSA reported that [] intelligence reports contained one or more references to USPs, including references to U.S. electronic communications providers as part of a communications identifier.

⁴ (S//NF) For the previous reporting period, NSA reported that [] identities were disseminated in response to requests for identities not referred to by name or title in the original reporting. For the current reporting period, fewer than a quarter of these disseminated USP identities were proper names of individuals or their titles. []

(U//FOUO)

~~SECRET//SI//NOFORN~~

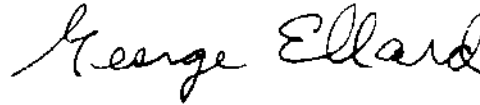
(b) (3)-P.L. 86-36

~~SECRET//SI//NOFORN~~

(U) Action has been taken to correct mistakes, and management processes have been reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of USP communications.

(U) This is the fifth year for which the OIG has reviewed the Agency's compliance with FAA §702 for the Congress. To ensure consistency between DIRNSA's report of the annual review conducted in accordance with FAA §702 (1) (3) and this OIG report, the OIG and the Signals Intelligence Directorate worked together to achieve a common understanding of the reporting requirements and have agreed on a methodology for accumulating and analyzing compliance statistics.

(U) The OIG continues to exercise oversight of Agency intelligence activities.



DR. GEORGE ELLARD
Inspector General

Copy Furnished:
The Honorable Dianne Feinstein
Chairman, Select Committee
on Intelligence

~~SECRET//SI//NOFORN~~



~~TOP SECRET//COMINT//REL TO USA, FVEY~~
 NATIONAL SECURITY AGENCY
 CENTRAL SECURITY SERVICE
 FORT GEORGE G. MEADE, MARYLAND 20755-6000

19 November 2010

The Honorable Silvestre Reyes
 Chairman, Permanent Select
 Committee on Intelligence
 United States House of Representatives
 H-405, The Capitol
 Washington, DC 20515

Dear Representative Reyes:

(U//FOUO) The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA) authorizes the National Security Agency/Central Security Service (NSA/CSS) Office of the Inspector General (OIG) to assess the Agency's compliance with procedures for targeting certain persons outside the United States, other than U.S. persons. My office reviews the collection, processing, and reporting of data at least quarterly. Incidents involving compliance with procedures for targeting certain persons outside the United States, other than U.S. persons, and incidents involving minimization of U.S. person information are reported to the OIG as they occur and quarterly. Each incident is evaluated against the targeting and minimization procedures set forth in the FAA and in NSA/CSS directives. This report covers the period 1 September 2009 through 31 August 2010.

~~(S//SI//REL TO USA, FVEY)~~ In compliance with the targeting and minimization procedures of §702 of the FAA, NSA/CSS disseminated [] intelligence reports based on FAA 702 authority. Of the [] disseminations, [] reports contained a reference to a U.S. person identity. In addition, NSA/CSS released [] U.S. identities in response to [] customer requests. The total of [] is an aggregate of FAA-derived identities because NSA/CSS's tracking system did not discriminate between FAA sections until 26 November 2009.

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

~~(TS//SI//REL TO USA, FVEY)~~ During this reporting period, [] valid foreign targets reasonably believed to be located outside the United States at the time of tasking were later suspected or confirmed to be in the United States. In many instances, NSA/CSS targeted selectors that at the time of targeting were confirmed to be outside the United States but were later []

[] In some cases, compliance incidents occurred under circumstances such as:

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

Derived From: NSA/CSS Classification Guide 2-48
 Dated: 20090804
 Declassify On: ~~20351130~~

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

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

- (U//~~FOUO~~) Target selectors were tasked under an incorrect §702 certification category.
- (U//~~FOUO~~) Targets were tasked before §702 certification was approved.
- (U//~~FOUO~~) Software malfunctions caused unintended collection.
- (U//~~FOUO~~) Database queries were poorly constructed.
- (U//~~FOUO~~) There were delays in implementing minimization procedures and in purging unauthorized collection.

(U) Action was taken to correct any mistakes, and processes were reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of U.S. person communications.

(U//~~FOUO~~) The OIG continues to exercise oversight of Agency intelligence activities.


GEORGE ELLARD
Inspector General

Copy Furnished:
The Honorable Peter Hoekstra
Ranking Member, Permanent Select
Committee on Intelligence

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



OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

7 April 2008
IG-10919-08

TO: DISTRIBUTION

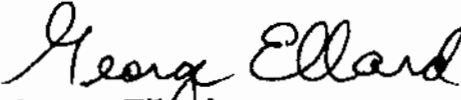
SUBJECT: (U) Report on the Assessment of Management Controls to Implement the Protect America Act of 2007 (ST-08-0001)—ACTION MEMORANDUM

1. (U) This report summarizes our Assessment of Management Controls to Implement the Protect America Act of 2007 (ST-08-0001) and incorporates management's response to the draft report.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, NSA/CSS *Office of the Inspector General*, actions on OIG recommendations are subject to monitoring and follow-up until completion. Therefore, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." If you propose that a recommendation be considered closed, please provide sufficient information to show that actions have been taken to correct the deficiency. If a planned action will not be completed by the original target completion date, please state the reason for the delay and provide a revised target completion date. Status reports should be sent to [redacted] Assistant Inspector General for Follow-up, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. For additional information, please contact [redacted] on 963-2988 or via e-mail at [redacted]

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


George Ellard
Inspector General

Approved for Release by NSA on 11-10-2015. FOIA Case #80120 (litigation)

DISTRIBUTION:

DIR

D/DIR

GC

D/GC(O)

Signals Intelligence Director

Chief, SID/PPAS

Chief, SV

SID/POC IG Liaison SV

Chief, S2

Chief, S3

Chief, S33

Chief, S332

cc:

IG

D12

D13

D14

(U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(S//SI)~~ NSA has implemented procedures to comply with the provisions of the Protect America Act of 2007 (PAA), which modified the Foreign Intelligence Surveillance Act (FISA) and was signed into law on 5 August 2007. To protect the privacy rights of U.S. persons, the new legislation required NSA to implement and follow procedures established by the Director, NSA (DIRNSA) to ensure its adherence to three requirements: that targets are located overseas, that the foreign intelligence purpose is significant, and that personnel follow applicable minimization procedures. In general, management controls to comply with PAA requirements are adequate. Specific controls to determine that targets are located overseas are especially strong.

~~(S//SI)~~ Made necessary by the technology changes that have occurred since the FISA was drafted in 1978, "FISA modernization" was intended to restore the effectiveness of the Act by eliminating the requirement for NSA to obtain court orders for monitoring the communications of persons physically located outside of the United States. Although the PAA expired in February 2008, NSA collection permitted under its provisions will continue for up to another year.

(U) HIGHLIGHTS

(U) The Office of the Inspector General assessed procedures established by DIRNSA to ensure compliance with the three PAA requirements. Management concurred with the recommendations.

- (U) NSA immediately implemented DIRNSA-directed procedures on compliance with the PAA. Management controls to determine that targets are located overseas are particularly strong.
- ~~(S//SI) NSA PAA~~ PAA tasking needs additional controls. Though current controls provide reasonable assurance of compliance with the PAA, additional controls are needed to verify that only authorized selectors are on collection and that information acquired through the use of selectors is related to the expected foreign intelligence targets.
- (U) More rigorous controls will increase the reliability of [] for PAA compliance. While existing [] are excellent preventive and detective controls, current methodologies are not rigorous enough to draw valid conclusions about the entire population.

(U) This page intentionally left blank.

(U) TABLE OF CONTENTS

(U) EXECUTIVE SUMMARY	I
(U) TABLE OF CONTENTS	III
I. (U) BACKGROUND.....	1
II. (U) FINDING	3
III. (U) SUMMARY OF RECOMMENDATIONS.....	11
(U) ACRONYMS AND ABBREVIATIONS.....	13

APPENDIX A – (U) About the Review

APPENDIX B – (U) Assessment of Management Controls

APPENDIX C - (U) Full Text of Management Comments

(U) This page intentionally left blank.

I. (U) BACKGROUND

(U) The Protect America Act of 2007

~~(S//SI//REL TO USA, FVEY)~~ On 5 August 2007, the President signed into law the Protect America Act (PAA) of 2007. The PAA, which expired on 16 February 2008, amended the Foreign Intelligence Surveillance Act (FISA) of 1978. Specifically, the PAA authorized the Attorney General (AG) and Director of National Intelligence (DNI) to approve, without a court order, the collection of foreign intelligence information from facilities located inside the United States concerning persons reasonably believed to be located outside the United States, subject to certain criteria. As of 31 March 2008, NSA had approximately [] Internet selectors and [] telephony selectors on PAA-authorized collection. From the passage of the PAA through 31 March 2008, NSA had issued [] reports that included PAA-derived intelligence.

(U) Requirements of the PAA

(U) The objective of our review was to assess the adequacy of management controls to implement and ensure compliance with three requirements of the PAA related to NSA operations:

- ~~(S//SI)~~ **Foreignness.**¹ Selectors on PAA collection must concern "persons reasonably believed to be located outside of the United States."
- ~~(S//SI)~~ **Foreign Intelligence Purpose.** A significant purpose of the collection is to obtain foreign intelligence information.
- (U) **Minimization Procedures.** NSA personnel must follow appropriate minimization procedures.

~~(S//SI//REL TO USA, FVEY)~~ At the time of our review, the AG and DNI issued [] separate certifications that authorize NSA to acquire foreign intelligence information of certain targets:

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

¹ (U) NSA's reasonable belief that a target is located outside of the United States based on one or more pre-determined factors.

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



(U) These certifications were based on representations made by the Director of NSA (DIRNSA) in affidavits that detail the management controls and procedures that NSA will follow.

(U) Standards of Internal Control

(U) We assessed management controls against the General Accounting Office's *Standards for Internal Control in the Federal Government*, November 1999, which presents the five standards that define the minimum level of quality acceptable for management control in government—Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring.

(U) Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations. NSA/CSS Policy 7-3, *Internal Control Program*, advises that evaluations of internal control should consider the requirements outlined by the Standards. The Office of the Inspector General (OIG) uses the Standards as the basis against which management control is evaluated.

II. (U) FINDING

~~(S//SI)~~ Since the PAA was passed in August 2007, Agency management has made progress in implementing the PAA and establishing management controls that are crucial to ensuring compliance with the PAA. NSA implemented all the procedures delineated by DIRNSA in the affidavits to the certifications. The controls implemented to verify that selectors tasked under the PAA for targets located outside of the United States are particularly strong. Nevertheless work remains to implement additional controls to:

- ~~(S//SI)~~ Verify [] that authorized selectors, and only those selectors, are on collection.
- ~~(S//SI)~~ Verify that analysts routinely review intercepted data and confirm that information acquired is related to the expected foreign intelligence targets.
- (U) Improve the validity and reliability of various [] of PAA compliance by Agency management. (b)(3)-P.L. 86-36
- (U) Improve target analysts' understanding of the PAA.

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

(U) Assessment details are included in Appendix B.

(U) NSA Immediately Implemented DIRNSA-directed procedures on compliance with the PAA

(U) Within weeks of the PAA enactment, NSA implemented the procedures that DIRNSA delineated in the affidavits and built on those procedures to establish rigorous processes to ensure compliance with the three requirements of the PAA. Management controls to determine and document foreignness were particularly strong. Controls covering foreign intelligence purpose and compliance with minimization procedures were also adequate.

(U) Some examples of NSA's accomplishments to date are:

- (U//~~FOUO~~) The PAA Implementation Team was established to coordinate all aspects of PAA implementation. Components of the team include internal and external communications, collection and data flows, mission operations, and policy and oversight.

- ~~(S//SI//REL TO USA, FVEY)~~ Telephony and Internet selector tasking systems were updated to allow analysts to document the foreignness determination. Also, controls were programmed into tasking systems to ensure that required information is documented and tasking is appropriate to AG/DNI certification targets.
- (U//~~FOUO~~) Within weeks of PAA passage, Signals Intelligence Directorate (SID) Oversight & Compliance (O&C) office, with the Office of General Counsel (OGC) and the Associate Directorate for Education and Training, had developed interim training that included a briefing by an OGC attorney and a competency test. On January 9, 2008, O&C deployed new and improved training.
- (U//~~FOUO~~) Agency management developed and published standard operating procedures, including procedures for training and raw traffic access, tasking, and incident reporting that will ensure consistent application of the PAA.
- (U//~~FOUO~~) A PAA web site was established to provide the NSA workforce with consistent, reliable, and timely information. From a single location, target analysts can read communications from NSA leadership, access certification-related documents, and view PAA-related standard operating procedures (SOPs).
- (U//~~FOUO~~) The PAA Procedures and Analytic Support (PPAS) team runs various processes to ensure compliance with the PAA. Specifically, PPAS personnel conduct [] foreignness checks of current targeting and notify target analysts of potential changes to a target's status. They also perform various [] of taskings for compliance with other PAA requirements and guide target analysts through the targeting and tasking processes.

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

(U) PAA tasking needs additional controls

~~(S//SI)~~ Although NSA implemented a series of controls to provide reasonable assurance that target analysts task only authorized selectors—selectors that meet the foreignness and foreign intelligence purpose requirements—additional controls are needed to verify that only authorized selectors are on collection and that tasked selectors are producing foreign intelligence of the expected targets.

~~(S//SI)~~ Controls are needed to verify [redacted] that authorized selectors, and only those selectors, are on collection.

~~(S//SI//REL TO USA, FVEY)~~ With the telephony tasking system, and to some extent the Internet selector tasking system, [redacted] a risk of discrepancies [redacted]

[redacted] Ultimately, discrepancies might result in violations of over-collection—selectors that are on collection that should not be—and incidents of under-collection—selectors that are not on collection but should be. Periodic reconciliation of NSA and provider records is critical to identify and resolve discrepancies and minimize violations and incidents.

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

~~(S//SI)~~ At the time of our review, NSA had not fully reconciled Agency [redacted] tasked selectors. Although Collection Managers prepared draft reconciliation procedures, the procedures were manual. [redacted]

~~(S//SI)~~ Implement [redacted] process that routinely reconciles PAA-tasked selectors with the providers.

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

(ACTION: S3/Chief, S332)

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

(U) Management Response

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

Status: OPEN
Target Completion Date: 15 May 2008

(U) OIG Comment

(U) Planned and ongoing actions meet the intent of the recommendation.

~~(S//SI)~~ **Controls are needed to validate that target analysts routinely confirm that information acquired through the use of selectors is related to the expected foreign intelligence targets.**

~~(S//SI)~~ PAA Standard Operating Procedures #2-07, Analyst Checklist, obligates target analysts to periodically "review intercepted data and confirm that the tasked selector is producing foreign intelligence from the expected target (which is authorized under the Certification)." A supplementary SOP on the analysts' obligation to review was in draft. Additional controls are needed to monitor compliance with this requirement to ensure that unintended persons are not mistakenly targeted.

~~(S//SI)~~ **Implement controls to verify that target analysts routinely review intercepted data and confirm that information acquired through the use of selectors is related to the expected foreign intelligence targets.**

(ACTION: Chief, S2 with O&C)

~~(U//FOUO)~~ In December 2007, Analysis and Production personnel said they are considering an automated report that will determine whether target analysts query, and therefore review, communications in the collection databases. Although such a report is technically feasible, its usefulness as a management control remains uncertain.

(U) Management Response

CONCUR. ~~(S//SI)~~ The Deputy Director for Analysis and Production (DDAP) is working with O&C to establish formal controls to verify that target analysts routinely review both telephony and internet-based collection. The system currently being devised will

Status: **OPEN**

Target Completion Date: **30 June 2008**

(b) (1)

P.L. 86-36

(b) (3)-50 USC 3024(i)

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

(U) More rigorous methodologies will improve the reliability of NSA spot checks

(U//~~FOUO~~) As shown in Appendix B, NSA is conducting, or plans to conduct, [] that are important to ensure compliance with the requirements of the PAA. Specifically,

- ~~(S//SI)~~ The PPAS team is conducting [] of foreignness determinations (with limited checks of foreign intelligence purpose) of selectors tasked under the PAA.
- ~~(S//SI)~~ The SID O&C reviews selectors pulled for AG/DNI reviews and is working on plans to conduct [] of targeting decisions that will complement AG/DNI reviews without being redundant.
- (U//~~FOUO~~) O&C conducts [] supraaudit reviews of queries in raw traffic databases to ensure compliance with the appropriate certification and minimization procedures.
- (U//~~FOUO~~) O&C conducts [] reviews of all reports generated by PAA collection to ensure adherence to NSA policy and standard minimization procedures.

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

(U) While such checks are excellent preventive and ~~detective~~ controls, neither organization had documented its [] procedures or considered using quality assurance and statistical sampling techniques that would strengthen the reliability of the results. In particular, neither organization had documented formal methodologies that specified the universe, population, sample size, and means of selecting items for review. The bases for sample sizes were unstructured and sample item selections were judgmental rather than truly random.² Sampling results were therefore not rigorous enough to draw valid conclusions about the entire population.

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

(U) Integration of statistical sampling or quality assurance techniques into existing and planned methodologies will not only increase the validity and usefulness of the [] but will likely decrease the frequency, time, and effort needed to conduct them. In short, well-planned methodologies will improve the reliability and efficiency of these important controls.

²(U) For a sample to represent a population, all items should have an equal probability of selection. Only samples that are truly random (e.g., by using a random number table to select items) are representative of the population. Samples based on haphazard or judgmental methods may be biased and are unlikely to be representative of the population.

~~(U//FOUO)~~ Develop and document rigorous methodologies for conducting [] of PAA compliance.

(ACTION: Chief, O&C and Chief, PPAS)

~~(U//FOUO)~~ In January 2008, the Chief, O&C stated that both O&C and PPAS are working on more rigorous methodologies.

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

(U) Management Response

CONCUR. ~~(S//SI//REL)~~ Management stated that O&C is documenting methodologies and procedures for conducting [] [] The management response did not include planned corrective actions for PPAS []

Status: **OPEN**

Target Completion Date: **2 May 2008**

(U) OIG Comment

(U) Planned action meets the intent of the recommendation for O&C. Planned action for PPAS remains unresolved.

(U) Target analysts need greater understanding of the PAA

~~(U//FOUO)~~ As shown in Appendix B, NSA has made significant progress in implementing a critical management control—training and awareness. Agency-wide e-mails, workforce presentations, a PAA-dedicated web site, and interim training are used to communicate with the NSA workforce. Improved training will further highlight aspects of the PAA authority most relevant to target analysts. However, two additional improvements are needed to provide target analysts the tools and guidance they need to implement the PAA.

(U) Working Aid or Quick Reference on NSA Authorities

~~(U//FOUO)~~ Given the increasingly complex and dynamic web of authorities under which NSA operates, target analysts are at risk of misunderstanding the PAA authorities. Although existing training and awareness provides details on the PAA, analysts might still be confused about how it differs from other NSA authorities. A working aid or quick reference that compares the basic elements and requirements of NSA's various authorities, with links to the authorities themselves, will help analysts navigate through the many documents and legalese and reduce the risk of violations.

Such guidelines and working aids should be available to employees at all times.

(U//FOUO) Publish and maintain a working aid that compares key requirements for SIGINT collection, processing, retention, and dissemination authorized by E.O. 12333 with requirements of other significant additional authorities, for example the PAA and FISA. In the working aid, provide links to the authorizing documents.

(ACTION: O&C with OGC)

(U//FOUO) The Chief, O&C, stated that planning has begun to develop a course that will include an overview and explanation of NSA's authorities, when to use them, what needs to be done to acquire them, and what the handling and minimization procedures are for each. If a working aid becomes an element of such training, we recommend that it be made available to the workforce as soon as possible rather than be tied exclusively to the training course.

(U) Management Response

CONCUR. **(U//FOUO)** Management stated that O&C levied a requirement for the Associate Directorate for Education and Training to develop an overview course of NSA's surveillance authorities. Course development is well underway and includes a requirement for a job aid.

Status: **OPEN**

Target Completion Date: **25 April 2008**

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

(U) Communicating PAA-related Guidance **(b)(1)**

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

~~**(S//SI)**~~ Not surprisingly, certain overarching questions on how to apply and comply with the PAA surfaced during our review. For example, target analysts expressed their uncertainty on querving and purging communications of targets [redacted] the United States. However, no mechanism was in place to keep the analysts informed of what to do while O&C consulted with OGC and developed the needed guidance. For example, by the end of our review, OGC had issued guidance in an e-mail to O&C, who subsequently decided that PPAS, rather than the target analysts, would purge collection for PAA incidents; but, existing procedures

were not updated to reflect this change. As NSA personnel continue to apply the PAA, more questions and uncertainties will inevitably emerge. To minimize confusion, a process is needed to vet, communicate, and post PAA guidance as a reference until it can be incorporated into more formal policy or SOPs, if needed.

(U//FOUO) Implement a process to vet, communicate, and post PAA guidance until it can be incorporated into policy or SOPs.

(ACTION: O&C)

(U) Management Response

CONCUR. (U//FOUO) Management stated that O&C would work with the OIG, OGC, SID Policy and the PAA Legal/Policy/Oversight Team to document the process for vetting, communicating, and posting PAA guidance.

Status: **OPEN**

Target Completion Date: **2 May 2008**

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

(U) Conclusion

(U) Within a short time, NSA has made considerable progress in setting up the needed training, policies, processes, procedures, systems, and oversight to ensure compliance with the PAA. Our recommendations strengthen the planned or implemented management controls, and NSA has already taken steps to address many of our concerns. As Congress continues to debate a long-term solution to the collection gaps that exist in FISA, the controls that NSA has in place set a solid foundation that will accommodate any law that supersedes the PAA.

(U) For this review, we did not conduct a full range of compliance and substantive testing needed to draw conclusions on the efficacy of management controls. We plan to complete such testing in a follow-on review.

III. (U) SUMMARY OF RECOMMENDATIONS

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

(U) Recommendation 1

~~(S//SI)~~ Implement [] process that routinely reconciles PAA-tasked selectors []

(U) Action: SID/S332

(b) (1)

(U) Status: OPEN

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

(b) (3) - 50 USC 3024(i)

(U) Target Completion Date: 15 May 2008

(U) Recommendation 2

~~(S//SI)~~ Implement controls to verify that target analysts routinely review intercepted data and confirm that information acquired through the use of selectors is related to the expected foreign intelligence targets.

(U) Action: SID/S2

(U) Status: OPEN

(U) Target Completion Date: 30 June 2008

(U) Recommendation 3

~~(U//FOUO)~~ Develop and document rigorous methodologies for conducting [] of PAA compliance.

(U) Action: SID/O&C and PPAS

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

(U) Status: OPEN

(U) Target Completion Date: 2 May 2008

(U) Recommendation 4

~~(U//FOUO)~~ Publish and maintain a working aid that compares key requirements for SIGINT collection, processing, retention, and dissemination authorized by E.O. 12333 with requirements of other significant additional authorities, for example the PAA and FISA. In the working aid, provide links to the authorizing documents.

(U) Action: SID/O&C with D/OGC

(U) Status: OPEN

(U) Target Completion Date: 25 April 2008

(U) Recommendation 5

(U//FOUO) Implement a process to vet, communicate, and post PAA guidance until it can be incorporated into policy or SOPs.

(U) Action: SID/O&C

(U) Status: OPEN

(U) Target Completion Date: 2 May 2008

(U) ACRONYMS AND ABBREVIATIONS

AG	(U) Attorney General
DIRNSA	(U) Director, National Security Agency
DNI	(U) Director of National Intelligence
FISA	(U) Foreign Intelligence Surveillance Act
O&C	(U) Oversight & Compliance
OIG	(U) Office of the Inspector General
PAA	(U) Protect America Act
PPAS	(U) PAA Procedures and Analytic Support
OGC	(U) Office of General Counsel
SID	(U) Signals Intelligence Directorate

(U) This page intentionally left blank.

(U) APPENDIX A

(U) About the Review

(U) This page intentionally left blank

(U) ABOUT THE REVIEW

(U) Objectives

(U) The objective of this review was to assess whether management controls are adequate to provide reasonable assurance that NSA complies with the terms of the PAA. In particular, our review assessed the adequacy of controls on the three PAA requirements:

- ~~(S//SI)~~ **Foreignness.** Selectors on PAA collection must concern "persons reasonably believed to be located outside of the United States."
- ~~(S//SI)~~ **Foreign Intelligence Purpose.** A significant purpose of the collection is to obtain foreign intelligence information.
- (U) **Minimization Procedures.** NSA personnel must follow appropriate minimization procedures.

(U) Scope and Methodology

(U) The review was conducted from September 14, 2007 to November 30, 2007.

(U) We interviewed Agency personnel and reviewed documentation to satisfy the review objectives.

(U) We did not conduct a full range of compliance or substantive testing that would allow us to draw conclusions on the efficacy of management controls. Our assessment was limited to the overall adequacy of management controls.

(U) This review was conducted in accordance with generally accepted government auditing standards, as set forth by the Comptroller General of the United States and implemented by the audit manuals of the DoD and NSA/CSS Inspectors General.

(U) Prior Coverage

(U) The OIG has conducted no prior coverage of NSA's implementation of the PAA.

(U) This page intentionally left blank

(U) APPENDIX B

(U) Assessment of Management Controls

(U) This page intentionally left blank

~~TOP SECRET//COMINT//NOFORN~~

ST-08-0001

(U) ASSESSMENT OF MANAGEMENT CONTROLS

(U) Many of the internal control requirements were established by the Affidavit of DIRNSA submitted for each Certification, Exhibit A to the Affidavit, and Exhibit B to the Affidavit. Exhibit A is common to each of the three AG/DNI certifications issued at the time of the review and establishes the procedures used to determine the foreignness of a target. Exhibit B for each affidavit contains the minimization procedures to be used for information collected under the related Certification. These procedures are unique to each Certification. In addition to the control requirements established by the affidavits and exhibits, the Standards for Internal Control in the Federal Government provides a general framework of controls that should be incorporated into daily operations.

	Control Objective	Source	Description	Assessment		
				Good	Adequate	Needs Improvement
Foreignness	(U//FOUO) [redacted]	(U) Exhibit A	(U//FOUO) According to the Analyst Checklist, a tasking analyst must review tasking submitted by a target analyst for a second-level review of foreignness. If the target analyst and tasking analyst are the same person, a tasking auditor will perform the second level review.		•	
	(b) (1) (b) (3) - P.L. 86-36		(S//SI) The [redacted] reviews tasking to ensure the required information has been entered. [redacted]		•	
			(U//FOUO) SIO Oversight & Compliance (O&C), in coordination with the OGC, has developed mandatory training for analysts tasking under the PAA and analysts accessing information collected under the PAA.	•		
	(U//FOUO) [redacted]	(U) Exhibit A	(U//FOUO) The PAA Procedures and Analytic Support (PPAS) Team was established [redacted] to detect incidents of targets entering the United States. [redacted] has been particularly successful. [redacted] The PPAS team also [redacted] to follow up with analysts on potential violations, detect, and purge data as needed.	•		

~~TOP SECRET//COMINT//NOFORN~~

(U) ASSESSMENT OF MANAGEMENT CONTROLS

	Control Objective	Source	Description	Assessment		
				Good	Adequate	Needs Improvement
Foreignness	(U// FOUO) [redacted]	(U) Exhibit A	(U// FOUO) To meet the requirements for documenting "foreignness determinations" in Exhibit A of the DIRNSA Affidavit, [redacted] to ensure that analysts fully document "foreignness" determinations when targeting under the PAA.	•		
	(b) (1) (b) (3) - P. L. 86-36		(U// FOUO) The Analyst Checklist states that "the target analyst is required to create a permanent record of the citations associated with each target and associated selectors." [redacted] The Checklist further describes [redacted] to retain "foreignness" documentation. Procedures to retain source documents are nearing completion.		•	
	(U// FOUO) [redacted]	(U) Exhibit A	(U// FOUO) NSA personnel support mandated AG/DNI reviews of PAA targeting decisions. So far, AG/DNI have not formally reported any violations to NSA.		•	
			(U// FOUO) The AG and DNI conducted 12 independent reviews of "foreignness" determinations as mandated in Exhibit A. Initial reviews were conducted 14 days after the certification was signed, and subsequent reviews are conducted every 30 days thereafter. [redacted] the AG and DNI decided to conduct reviews every 30 days. Agency personnel track resolution of feedback and recommendations provided by the AG/DNI review teams during the reviews.	(b) (3) - P. L. 86-36 •		
	(U// FOUO) [redacted]	(U) Exhibit A	(S// FOUO) O&C was checking selectors pulled for AG/DNI reviews but had no formal standard operating procedures or rigorous methodology for conducting [redacted] independent of the reviews. O&C was working to develop procedures that will complement AG/DNI reviews without being redundant. See Recommendation #3.			•
			(U// FOUO) The PPAS team does limited checks for foreignness. However, the PPAS team does not have a documented methodology for conducting the [redacted] See Recommendation #3.			•

~~TOP SECRET//COMINT//NOFORN~~

SI-08-0001

(U) ASSESSMENT OF MANAGEMENT CONTROLS

	Control Objective	Source	Description	Assessment		
				Good	Adequate	Needs Improvement
Foreign Intelligence Purpose	(U//FOUO) "In determining whether each of the persons targeted for collection pursuant to this request possesses and is likely to communicate information [of a foreign intelligence value], NSA considers [certain information]."	(U) DIRNSA Affidavit	(U//FOUO) The Analyst Checklist includes steps that analysts must follow to ascertain under which certification the target can be tasked.		•	
			(U//FOUO) Tasking tools were modified [redacted] to ensure consistency and accuracy in targeting information entered by analysts. [redacted]	•		
			(U//FOUO) Analysts must also document, in the tasking tools, the Information Need that a target is expected to satisfy.			
			(U//FOUO) The Analyst Checklist requires analysts to routinely review intercepted data and confirm that tasked selectors are producing foreign intelligence from the expected targets. A SoP is planned that will provide full instructions on an analyst's review obligation. In addition to the SoP, management should develop controls to ensure analysts are conducting required reviews. See Recommendation #2.			•
			(U//FOUO) In conjunction with [redacted] of foreignness, the PPAS team does limited checks of foreign intelligence purpose. However, the PPAS team does not have a documented methodology for conducting the [redacted]. See Recommendation #3.			•
	(b) (3) - P.L. 86-36		(U) Routine audits of queries of raw traffic databases are performed to validate that the queries will likely produce foreign intelligence information.		•	

Appendix B
Page 3 of 6~~TOP SECRET//COMINT//NOFORN~~

ST-08-0001

~~TOP SECRET//COMINT//NOFORN~~**(U) ASSESSMENT OF MANAGEMENT CONTROLS**

	Control Objective	Source	Description	Assessment		
				Good	Adequate	Needs Improvement
Minimization Procedures	(S) NSA will follow: (a) the Standard Minimization Procedures for Electronic Surveillance Conducted by the NSA (also known as Annex A to United States Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with the Foreign Intelligence Surveillance Court (except as modified by Exhibit D to each Certification);	(U) Exhibit B	(U//FOUO) Standard minimization procedures have been promulgated as USSID SP0018—Legal Compliance and Minimization Procedures (USSID 18), since 1993. The current version of USSID 18 supersedes a prior version issued in 1980. The policies and procedures prescribed by USSID 18 are well-established and well-known to analysts. Also, USSID CR1610 requires analysts be briefed by OGC and SID O&C on USSID 18 before obtaining access to raw SIGINT databases. CR1610 also requires USSID 18 briefings every two years in order to maintain database access. (U//FOUO) Although PAA training has been implemented, improvements could be made when discussing the differences between USSID 18 and the minimization procedures for each certification. A working aid for analysts would help analysts distinguish between authorities and their related minimization procedures. See Recommendation #4.	•		
	(U//FOUO)	(U) Exhibit A	(S//SI) The PPAS team [redacted] to detect incidents of targets entering the United States. [redacted] has been particularly successful. [redacted] The PPAS team also [redacted] to follow up with analysts on potential violations, detain, and purge data as needed. (b) (1) (b) (3) - P. L. 86-36	•		
	(U//FOUO)	(U) Exhibit A	(U//FOUO) The PPAS team and SID O&C verify compliance with reporting minimization procedures [redacted] for compliance with Certification minimization procedures or performed for published reports. However, O&C has not documented procedures or a methodology for such reviews. See Recommendation #3.			•

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

~~TOP SECRET//COMINT//NOFORN~~Appendix B
Page 4 of 6

~~TOP SECRET//COMINT//NOFORN~~

ST-08-0001

(U) ASSESSMENT OF MANAGEMENT CONTROLS

	Control Objective	Source	Description	Assessment		
				Good	Adequate	Needs Improvement
Communication	(U) "Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities."	(U) Standards for Internal Control in the Federal Government	(U//AFDQAO) An internal web site has been established to centralize communication of PAA-related information to the NSA workforce. The website serves as a single point of contact for PAA-related information. From one location, analysts can access PAA SOPs, DIRNSA affidavits and related exhibits for each certification, archived PAA communications from NSA leadership, and PAA Help Team contact information.	•		
		(b) (3) - P.L. 86-36	(U//FOUO) NSA leadership has emphasized the importance of the PAA through various Agency all e-mails and presentations.	•		
			(U//AFDQAO) A system to post PAA Standard Operating Procedures is in place. [] sets of standard operating procedures have been posted so far: Analyst Checklist, Incident Reporting, Training, []	•		
		(b) (1) (b) (3) - P.L. 86-36 (b) (3) - 50 USC 3024(i)	[] In addition, a number of procedures were still in draft and various local procedures had either been formalized or were in draft.			
			(U//AFDQAO) Although a process is in place to promulgate SOPs, a similar process does not exist for communicating and posting interim guidance until O&C and OGC can publish more formal policy, as needed. Given the newness of the PAA, more questions on applying and complying with the PAA will inevitably emerge. Answers to such questions have been communicated by e-mail to O&C; however, existing procedures had not been updated to reflect any changes. A process to post such questions and answers for future reference will eliminate confusion on the part of the Analysts until SOPs are updated. See Recommendation #5.			•
			(U//AFDQAO) PAA SOP has been developed for incident reporting and published on the PAA website. Published SOPs enable analysts to quickly recognize reportable incidents and take appropriate action.	•		
			(U//FOUO) The PPAS Team assists S2 product lines by guiding analysts through the targeting and tasking processes.	•		

~~TOP SECRET//COMINT//NOFORN~~

(U) ASSESSMENT OF MANAGEMENT CONTROLS

	Control Objective	Source	Description	Assessment		
				Good	Adequate	Needs Improvement
Communication	(U// FOUO) [redacted]	(U) Exhibit A	(U// FOUO) O&C and OGC developed training that requires watching a video briefing from OGC, reading the certifications and related documents, and taking and passing a competency test with a score of 80% or better. (U// FOUO) O&C has made improvements to the training based on feedback from the initial course. The updated training clarifies key points for analysts and draws distinctions between PAA and other NSA authorities.	•		
	(b) (1) (b) (3) - P. L.	86-36	(U// FOUO) A Training SoP has been developed and published on the internal PAA website. The SoP outlines the training requirements to obtain access to PAA derived collection, as well as, the process to obtain the training.	•		
Monitoring	(U) Internal control monitoring should assess the quality of performance over time and ensure findings are resolved. It includes regular management and supervisory activities, such as ongoing comparisons and reconciliations, to ensure controls are functioning properly.	(U) Standards for Internal Control in the Federal Government	(U// FOUO) Periodic reconciliation of selections on collection in NSA systems [redacted] should be performed to detect potential over-collection or under-collection. Although collection managers prepared draft reconciliation procedures, the procedures were designed to [redacted] See Recommendation #1.		(b) (1) (b) (3) - P. L. 86-36 (b) (3) - 50 USC 3024 (i)	
	(U// FOUO) [redacted]	(U) Exhibit A	(U// FOUO) O&C currently conducts supervisory of queries to raw traffic database for USSID 18 compliance. O&C will conduct [redacted] supervisory of queries made to PAA data partitions to ensure compliance with appropriate certifications and USSID 18. See Recommendation #3.			•

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

(U) APPENDIX C

(U) Full Text of Management Comments

(U) This page intentionally left blank

~~TOP SECRET//COMINT//NOFORN~~

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO OIG	EXREG CONTROL NUMBER 1250-08	KCC CONTROL NUMBER
THRU	ACTION <input type="checkbox"/> APPROVAL <input type="checkbox"/> SIGNATURE <input checked="" type="checkbox"/> INFORMATION	EXREG SUSPENSE KCC SUSPENSE ELEMENT SUSPENSE
SUBJECT (U//FOUO) SID Response to OIG Draft Report on the Assessment of Management Controls to Implement the Protect America Act (PAA) of 2007 (ST-08-0001)		
DISTRIBUTION SID, SV, S2, S3, PPAS; OGC		

SUMMARY

PURPOSE: (U//FOUO) To provide the SID response on the OIG Draft Report on the Assessment of Management Controls to Implement the Protect America Act (PAA) of 2007 (ST-08-0001).

BACKGROUND: (S//SI//REL) The OIG performed an assessment of the procedures established by the Director NSA (DIRNSA) to ensure NSA's adherence to three PAA requirements: that targets are located overseas, that the foreign intelligence purpose is significant, and that personnel follow applicable minimization procedures. The OIG draft report was published on 31 January 2008 and provides a complete summary of the OIG's assessment. The SIGINT Directorate (SID) was tasked to review and comment on the OIG Draft Report.

DISCUSSION: (U//FOUO) The Office of Oversight & Compliance (SV), the SID Directorate for Analysis & Production (S2), and the SID Directorate for Data Acquisition (S3) have reviewed and concurred with the recommendations in the OIG Draft Report. These organizations have responded with detailed plans of action, to include their expected target completion dates.

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

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
SID	K. SID 4/27/08	966-7700			
SV	24 Mar 2008	966-2479			
ADDAP	/s/ 11 Mar 08	963-3335			
DDDA	/s/ 21 Mar 08	963-1921			
PAA Team	/s/ 25 Mar 08	966-2044			
ORIGINATOR	SID IG Liaison	ORG. SV	PHONE (Secure)	DATE PREPARED	
			966-2464	17 March 2008	

FORM A5706
REV NOV 85Derived From: NSACSSM 1-52
Dated 8 January 2007
Declassify on: 20020400

SECURITY CLASSIFICATION

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(U//~~FOUO~~) **SID RESPONSE to the OIG Draft Report on the
Assessment of Management Controls to Implement the Protect
America Act (PAA) (ST-08-0001)**

Recommendation 1: (S//SI) Implement [redacted] process to routinely reconcile
PAA-tasked selectors [redacted] (ACTION: Chief, S332)

(U) SID ACTION: S3/Chief, S332

(b) (1)

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

SID Response (March 2008): (U//~~FOUO~~) [redacted] (S332) concurs
with the OIG Draft Report and Recommendation 1 and provides the following
description of planned corrective actions and a target completion date.

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

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

(b) (1)

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

(b) (3) - 50 USC 3024(i)

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

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~• ~~(TS//SI//NF)~~ [REDACTED]

[REDACTED]

• ~~(TS//SI//NF)~~ [REDACTED]

[REDACTED]

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

1. [REDACTED]

2. [REDACTED]

3. [REDACTED]

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

[REDACTED]

(U//~~FOUO~~) The Target Completion Date for S3 to implement [REDACTED] process is
 15 May 2008.

(b) (1)

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

(U//~~FOUO~~) SID POC(s): [REDACTED]
 (S33243), NSTS: 963-4886.

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

**Recommendation 2: ~~(S//SI)~~ Implement controls to verify that target analysts
 routinely review intercepted data and confirm that tasked selectors are producing
 foreign intelligence from the expected targets. (ACTION: Chief, S2)**

(U) SID ACTION: DDAP (Chief, S2)

**SID Response (March 2008): ~~(S//SI)~~ The Deputy Director for Analysis & Production
 (DDAP) will continue to work with Oversight & Compliance (SV) to formally establish
 the requested controls. The system currently being devised will cover both DNI and
 telephony.** [REDACTED]

[REDACTED] The system should

~~TOP SECRET//COMINT//NOFORN~~

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

(b) (1)

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

(b) (3) - 50 USC 3024(i)

~~TOP SECRET//COMINT//NOFORN~~

(U) The **Target Completion Date** for official implementation of these procedures is 30 June 2008.

(U//FOUO) SID POC(s):

[redacted] NSTS: 963-1161.

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

Recommendation 3: (U//FOUO) Develop and document rigorous methodologies for conducting [redacted] of PAA compliance. (ACTION: Chief, O&C and Chief, PPAS)

SID Response (March 2008): (U//FOUO) Oversight and Compliance (SV) concurs with this recommendation.

(b) (1)

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

~~(S//SI//REL)~~ Oversight and Compliance (O&C) is currently documenting the methodologies and procedures for conducting [redacted] of targeting decisions, intelligence disseminations, and queries in data repositories to ensure compliance with established procedures and in accordance with Exhibits A under the [redacted] PAA certifications. O&C is currently conducting [redacted] of intelligence disseminations by reviewing 100% of all reporting [redacted]

[redacted] In addition, O&C is conducting [redacted] super-audits against a [redacted] file, [redacted]

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

[redacted] All query terms are reviewed to ensure that there are no terms that will inherently return U.S. entity communications. These procedures will be documented. Finally, Oversight and Compliance is working with DOJ and ODNI attorneys in every review of all targeting decisions. Procedures for these reviews will also be documented. It should be noted that these procedures may change pending the passage of permanent legislation.

(U) The **Target Completion Date** for the documentation of the methodologies and procedures is 2 May 2008.

(U//FOUO) SID POC(s):

[redacted] Chief, [redacted] (SV2), NSTS: 963-0248; [redacted] PPAS (S0), NSTS: 963-0363.

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

Recommendation 4: (U//FOUO) Issue and maintain an up-to-date working aid or quick reference that compares key elements and requirements of and links to NSA's various authorities. (ACTION: O&C with OGC)

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(U) SID ACTION: O&C (SV)

SID Response (March 2008): SV concurs with this recommendation.

~~(TS//SI//REL)~~ Prior to receiving this recommendation, Oversight and Compliance (O&C) had already levied a requirement with ADET in October 2007 to develop an overview course of NSA's surveillance authorities. The Training Control Document for this course was completed on 1 February 2008 and includes a requirement for a job aid to fulfill this recommendation. The development of the course is well underway. Details of the course are available upon request. It should be noted that some course content may change pending the passage of permanent legislation.

(U) The Target Completion Date for the course and the job aid is 25 April 2008.

(U//~~FOUO~~) SID POC(s): [redacted] Chief, [redacted]
(SV3), NSTS: 966-4887; and [redacted] FISA Technical Lead, SV09,
NSTS: 963-8168.

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

Recommendation 5: (U//~~FOUO~~) Implement a process to vet, communicate, and post PAA guidance until it can be incorporated into policy or SOPs. (ACTION: O&C)

(U) SID ACTION: O&C (SV)

(b) (1)

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

SID Response (March 2008): SV concurs with this recommendation.

~~(S//SI//REL)~~ Immediately after the temporary PAA legislation was passed, SID established a PAA implementation team, which consisted of [redacted] sub-teams that included the following: [redacted]

[redacted] and a Legal/Policy/Oversight (LPO) team. The LPO team, led by the Chief of Oversight and Compliance (SV), has been meeting periodically since August 2007 to discuss and develop guidance related to PAA implementation. The team has promulgated [redacted] SOPs and is in the process of developing [redacted]. These SOPs are posted on both the PAA and O&C websites. In addition, members of the LPO team (which includes SID Policy, OGC, S2, and S3 members) participate in the almost daily PAA team lead sessions where additional information is discussed to include the need for further guidance. Although this recommendation is somewhat vague in terms of expected deliverables, Oversight and Compliance will work with the OIG Office, OGC, SID Policy, and the LPO team to document the process for vetting, communicating and posting PAA guidance. It should be noted that some guidance may change pending passage of permanent legislation.

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

(U) The Target Completion Date for documenting the process is 2 May 2008.

(U//~~FOUO~~) SID POC(s): [redacted] Chief, Oversight and Compliance (SV), NSTS: 966-2479.

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

~~TOP SECRET//COMINT//NOFORN~~

~~SECRET//SI//NOFORN~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL
9800 Savage Road
OPS 2B, Suite 6247
Ft. George Meade, MD 20755-6247



17 December 2014

The Honorable Dianne Feinstein
Chairman, Select Committee on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, DC 20510

Dear Madame Chairman:

(U) Section 702 (I) (2) of the Foreign Intelligence Surveillance Act (FISA) of 1978, as amended by the FISA Amendments Act of 2008 (FAA), authorizes the National Security Agency/Central Security Service (NSA/CSS) Office of the Inspector General (OIG) to assess the Agency's compliance with procedures for targeting non-U.S. persons reasonably believed to be located outside the United States. My Office reviews incidents involving compliance with procedures for targeting non-U.S. persons reasonably believed to be located outside the United States and incidents involving minimization of U.S. person information as they are reported to the OIG and quarterly. Each incident is evaluated by NSA against the targeting and minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, and approved by the Foreign Intelligence Surveillance Court (FISC). This letter covers the 12-month period ending 31 August 2014.

(b) (1)

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

~~(S//SI//NF)~~ During the reporting period, the OIG performed two special studies of the FAA §702 program: [redacted] and the Implementation of Section 702 of the FISA Amendments Act of 2008. [redacted]

[redacted] The second study, requested by members of the U.S. Senate Judiciary Committee and scheduled to be published in January 2015, documents NSA's implementation of the FAA §702 authority, the controls used to protect U.S. person privacy, past incidents of non-compliance, and use of FAA §702 data to support intelligence missions.

~~(S//NF)~~ In compliance with the FAA §702 targeting and minimization procedures, [redacted] intelligence reports were disseminated by NSA/CSS [redacted] based on signals intelligence (SIGINT) derived in whole or in part from FAA §702 authorized [redacted]

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

Classified By: [redacted]

Derived From: NSA/CSS Manual T-52

Dated: 30 September 2013

Declassify On: 20391217

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

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

~~SECRET//SI//NOFORN~~

Approved for Release by NSA on 11-10-2015. FOIA Case # 80120 (litigation)

(b) (1)
(b) (3) - P.L. 86-36~~SECRET//SI//NOFORN~~

collection. ● of the [] disseminated reports, [] contained one or more references to U.S. persons.¹

(U//FOUO) NSA/CSS released [] U.S. person identities in response to customer requests for U.S. person identities not referred to by name or title in the original reporting.² The majority of these requests were received from elements of the United States Intelligence Community and federal law enforcement agencies.

~~(S//NF)~~ During this reporting period, NSA determined that, on [] occasions, selectors belonging to non-U.S. persons reasonably believed to be located outside the United States at the time of tasking were later suspected or confirmed to have been []

(b) (1)
(b) (3) - P.L. 86-36 ~~(S//SI//NF)~~ [] the Department of Justice (DoJ) filed with the FISC a preliminary notice of a compliance incident that advised the Court that []

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

~~(S//NF)~~ [] the references to U.S. person identities might have resulted from collection pursuant to FAA §702 or from other authorized SIGINT activity NSA conducted that was reported in conjunction with information acquired under FAA §702. For the previous reporting period, NSA reported that [] intelligence reports contained one or more references to U.S. persons, including references to U.S. electronic communications providers as part of a communications identifier.

~~(S//NF)~~ The Central Intelligence Agency (CIA) does not conduct acquisitions under FAA §702. However, it receives unminimized non-upstream communications from NSA and FBI and disseminates information based on those communications. []

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

~~(S//NF)~~ For the previous reporting period, NSA reported that [] identities were disseminated in response to requests for identities not referred to by name or title in the original reporting. For the current reporting period, approximately [] of the disseminated U.S. person identities were proper names of individuals or their titles. []

(U//FOUO)

~~SECRET//SI//NOFORN~~(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798
(b) (3) - 50 USC 3024(i)(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

~~SECRET//SI//NOFORN~~

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

(U) As explained in the OIG's quarterly report to the President's Intelligence Oversight Board on NSA activities, compliance incidents occurred under such circumstances as:

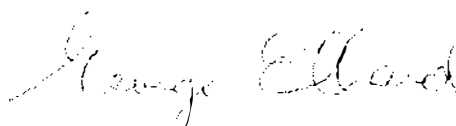
- (U//~~FOUO~~) Tasked selector not meeting the requirements of the certification,
- (U//~~FOUO~~) System errors resulting in improper storage or access,
- (U//~~FOUO~~) Delayed detasking of targets identified as U.S. persons [REDACTED]
- (U//~~FOUO~~) Dissemination errors,
- (U//~~FOUO~~) Poor construction of database queries, and
- (U//~~FOUO~~) Post-tasking discovery of U.S. person status.

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

(U) Action has been taken to correct mistakes, and management processes have been reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of U.S. person communications.

(U) This is the sixth year for which the OIG has reviewed for the Congress the Agency's compliance with FAA §702. To ensure consistency between DIRNSA's report of the annual review conducted in accordance with FAA §702 (I) (3) and this OIG report, the OIG and the Signals Intelligence Directorate worked together to achieve a common understanding of the reporting requirements and have agreed on a methodology for accumulating and analyzing compliance statistics.

(U) The OIG continues to exercise oversight of Agency intelligence activities.



DR. GEORGE ELLARD
Inspector General

Copy Furnished:
The Honorable Saxby Chambliss
Vice Chairman, Select Committee on Intelligence

~~SECRET//SI//NOFORN~~