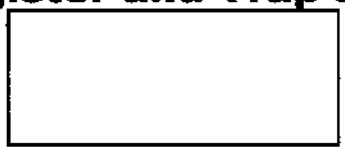
NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

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~~

(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~~

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]

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

George Ellard

GEORGE ELLARD
Inspector General

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

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

[redacted]

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

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

DOC (J. DeLong)
SID (T. Shea)
TD [redacted]

cc:
Director
OGC [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]
OGC IG POC [redacted]
SID IG POC [redacted]
TD IG POC [redacted]

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

DOJ NSD [redacted]

IG
D/IG
D1 [redacted]
D11
D12
D13
D14

(b)(6)

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

(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 [redacted] 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 [redacted] queries made between [redacted] the date when the Foreign Intelligence Surveillance Court signed [redacted] and [redacted] 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.* [redacted]

[redacted]

(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 [redacted]

[redacted]

~~(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 [redacted]

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

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

because of concern the Agency could not comply with the order as written. the FISC issued an Order substantially different from the previous versions in that, among other things, it redefined "facilities" 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 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 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 while an active Order was in place. Although the Order first became active in after the Agency had allowed it to expire, the Agency did not resume collection and querying of PR/TT metadata until (which closely mirrors its first renewal). [1].

(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 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.

[1] ~~(TS//SI//NF)~~ For the period reviewed, 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 we did not formally test dissemination objectives.

(b)(1)
(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 Articulable 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]

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

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.

(U) APPENDIX A

(U) About the Audit

(U) This page intentionally left blank.

(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

[redacted]

(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

[redacted]

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

(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

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

~~(TS//SI//NF)~~ We did not plan to test whether non-serialized reports were approved by the Chief, Information Sharing Services (S12), 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.

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

(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

(U) This page intentionally left blank.

(U) APPENDIX B

(U) Test Results

(U) This page intentionally left blank.

(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] 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)~~

(U) RATING SYSTEM

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

~~(TS//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**

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