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

~~(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[1] [redacted] 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.

[1] ~~(S//SI)~~ Includes all e-mail communications [redacted] (b) (1)
(b) (3)-P.L. 86-36

[2] ~~(TS//SI//NF)~~ The current version of the Order [redacted]

(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,

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

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 DoJ 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

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

(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.[1] 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,

---

[1] ~~(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 PRTT 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] PRTT 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 PRTT queries, unlike SIGINT keyword queries, do not undergo front-line audits by supervisors. O&C personnel also agreed that reconciliation of PRTT 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 PRTT data are traceable to seed addresses that meet the terms of the Order [redacted], and
- a Shift Coordinator approved the originating seed addresses of all queries made against PRTT data.

~~(TS//SI//NF)~~ **Audit log reports are incomplete.** The audit log reports that O&C spot-checks do not include all queries made against PRTT data. The reports include only the queries of analysts that the Program Management Office (PMO) lists as being approved for access to PRTT data. This data is incomplete because it does not include queries of excluded individuals—those that have the ability to query the PRTT 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 PRTT 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 PRTT data, were also omitted from the audit log reports. Because all potential queries made against PRTT 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 PRTT 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 PRTT 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* (ST-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 [redacted] audit logs to capture needed data, such as originating seed address, U.S. identifiers, number of hops, and PRTT identifiers.

(ACTION: [redacted] 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. [redacted] 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 OGC approval of U.S. seed addresses.

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

Status: **OPEN**
Target Completion Date: [redacted]

(U) OIG Comment

(U//~~FOUO~~) Because we did not receive detailed plans from [redacted] 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: [redacted] (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 [redacted] and monitors the audit log function. OGC does not, however, document the date, scope, or results of the reviews. The purpose of the spot checks is to ensure that filters and other controls in place on the [redacted] 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)

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

(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//STLW//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 PRTT 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: [redacted] (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 integrees) 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 PRTT 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.

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

APPENDIX A

(U) About the Audit

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

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

(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) (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] 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 PRTT queries, additional action is needed to make the monitoring effective.

- While personnel are notified of changes in renewals of the PRTT Order and new orders are posted on a centralized website, refresher training is still needed to ensure that NSA personnel implement the Order correctly.

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

APPENDIX B

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

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

This page intentionally left blank

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

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

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

Order Number	Effective Dates	Changes from Previous Order
		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]
		• [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."
		• [redacted] • Added requirement to discuss the nature of the data collected on [redacted] in the 30-day report.
		No changes
		No changes
		• [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).
		• [redacted] • [redacted] • Increased the number of analysts allowed access to the metadata to from 15 to 20.

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

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

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

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

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

This page intentionally left blank

APPENDIX C

(U//~~FOUO~~) Mandated Terms and Control Procedures

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

This page intentionally left blank

(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//STLW//NF)~~ I. Collection

(b)(1) (b)(3)-P.L. 86-36 Terms of the Order	Responsible Entity	Mandated Control Procedures
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) (b) (3) -P.L. 86-36 (b) (3) -50 USC 3024(i) The authority granted is within the United States. (Pg 12, Para (3))	PMO/DOJ	1. Every Sixty (60) days during the authorized period of surveillance, NSA shall file with the Court a report that includes: ... (ii) any changes in the descriptions [redacted] and (iii) 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)
B. Collection of the contents of such communications as defined by 18 U.S.C. §2510(8) is not authorized. (Pg. 8-9, Para (1))	SSO	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
Addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications, includes • the "to," "from," "cc," and "bcc" fields for those communications [redacted]	PMO OGC	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)
	OGC	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 (v))

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

~~(TS//SI//STLW//NF)~~ I. Collection (continued)

Terms of the Order	Responsible Entity	Mandated Control Procedures
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. (Pg 14, Para (D)) This authorization [redacted]	PMO	1. None

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

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

Control Area II: Processing

~~(TS//SI//STLW//NF)~~ II. Processing

Terms of the Order	Responsible Entity	Mandated Control Procedures
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]	PMO	1. The NSA shall ensure that the mechanisms for accessing such information will automatically generate a log of auditing information for each occasion when the auto-caution is accessed, to include the accessing user's login, IP address, date and time, and retrieval request. (Pg 13, Para (5)b)
	OGC	2. OGC shall monitor "the functioning of the automatic logging of auditing information required by [the order]." (Pg 15, Para (5)d.ii)
Provided, 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)	OGC	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.ii)
	PMO, OGC	4. Every thirty (30) days during the authorized period of surveillance, NSA shall file with the Court a report that includes: (1) the dissemination 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 (5)c above to those queries. (Pg 15, Para (5)g)

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

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

~~(TS//SI)~~ This Order, PRTT [redacted] is the first one that includes [redacted]

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

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

Terms of the Order	Responsible Entity	Mandated Control Procedures
A (continued)	OGC	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 (5)(a)) "[I]t shall be incumbent on NSA's Office of General Counsel to review the legal adequacy for the bases of such queries, including the First Amendment proviso, set out at paragraph c. above." (Pg 16, Footnote 19)
(b) (1) (b) (3)-P.L. 86-36 (b) (3)-50 USC 3024(i)	PMO	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 Shift Coordinator in the Analysis and Production Directorate of the Signals Intelligence Directorate. (Pg 15, Par. (5)c)
B. Such information shall be accessed only through queries using the contact chaining[2] [redacted] methods described at page 13 of the Court's July 14, 2004 Opinion and Order in Docket No. PR/TT [redacted] (Pg 14, Para (5)c)	AAD	7. Note:

~~(TS//SI//STLW//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)~~ 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(3) of the Court's July 14, 2004 Opinion and Order in Docket No. PR/TT [redacted]

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

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

~~(TS//SI//STLW//NF)~~ **II. Processing** (continued)

Terms of the Order	Responsible Entity	Mandated Control Procedures
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 new seed[s] [redacted] such prohibition remains in effect. (Pg 3, Para (1) of [redacted] • In addition, NSA is hereby prohibited from querying FISA meta data in any manner [redacted] based on seed[s] [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] (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 3, Para (3) of [redacted]	AAD PMO/OGC	1. None **(b) (1)** **(b) (3)-P.L. 86-36** 2. The government was ordered to submit a description of procedures for preparing 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 1-3 of the [redacted] letter. (Pg 3, Para (4) of [redacted]

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

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

~~(TS//SI//STLW//NF)~~ **II. Processing** (continued)

Terms of the Order	Responsible Entity	Mandated Control Procedures
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. (Pg 15, Para 5K)	AAD	1. None (b) (1) (b) (3) -P.L. 86-36 (b) (3) -50 USC 3024(i)

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

Control Area III: Dissemination

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

Terms of the Order	Responsible Entity	Mandated Control Procedures
A. The NSA shall apply the Attorney General approved guidelines in United States Signals Intelligence Directive DA (Attachment D to the application in Docket No. PR/TT [redacted] to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein. (Pg. 16, Para 15)c)	AAD & OGC	1. Prior to disseminating any U.S. person information outside of the NSA, the Chief of Information Sharing 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. (Pg. 16, Para 15)e)

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

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

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 (5)H)	[redacted] & Technical[1] 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 13 Para (5)a)	OGC	1 OGC shall monitor the designation of individuals with access to such information under [the order]. (Pg 15[1], Para (5)d iv)
B The ability to retrieve information derived from the pen register and trap and trace devices shall be limited to twenty[10] specially cleared analysts and to specially cleared administrators. (Pg 13 Para (5)b)	[redacted] & 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/TT [redacted] increased the number of people with PR/TT data access to 20.