THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

All redacted information exempt under b(1) and/or b(3) except where otherwise noted.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
[redacted]
PM 1:36

Pen Register/Trap and Trace FISA
NSA Review

[redacted]

Prepared by: Pen Register/Trap and Trace Team

(U) TABLE OF CONTENTS

I. (U) Background and Executive Summary Page 3

II. ~~(TS//SI//NF)~~ NSA's PR/TT Review Page 4

III. (U) Previously Reported Items and Newly Identified Areas of Concern Page 10

IV. (U//FOUO) NSA's Minimization and Oversight Procedures Page 21

V. (U//FOUO) NSA's Future Architecture Page 24

VI. (U) Conclusion Page 25

~~(TS//SI//NF)~~ Figures 1-10: PR/TT Workflow Diagrams Page 26

(U) Appendix: Glossary of Terms Page 36

~~(TS//SI//NF)~~ Implementation of the Foreign Intelligence Surveillance Court Authorized Pen Register/Trap and Trace – NSA Review

[redacted]

I. (U) Background and Executive Summary

~~(TS//SI//NF)~~ The Pen Register/Trap and Trace (PR/TT) Court Orders have given the National Security Agency (NSA) access to Internet metadata on [redacted] This metadata contains information about individual Internet-based contacts (but not the content of those contacts) not available through other NSA SIGINT collection. PR/TT metadata provides value to NSA analysts tasked with identifying potential threats to the U.S. homeland and broadens their view of foreign-based terrorist networks with U.S. ties. The PR/TT metadata helps NSA analysts detect [redacted] Although PR/TT metadata is not the sole source available to NSA counterterrorism personnel, it helps NSA analysts develop a more complete picture of potential terrorist threats.

~~(TS//SI//NF)~~ The PR/TT Compliance Review Team of NSA, in response to instructions from the Director of NSA (DIRNSA) and as set out in DIRNSA's Declaration of [redacted] to the Foreign Intelligence Surveillance Court (FISC or Court), conducted an end-to-end systems engineering and process review of the instrumentation and implementation of the PR/TT authorization pursuant to the [redacted] PR/TT Order. The PR/TT review was focused on two major areas that were at risk for compliance issues – system-level technical engineering and implementation of the analytic process.

~~(TS//SI//NF)~~ The review covered the nine major system or process components of the PR/TT metadata workflow and surfaced eleven areas of concern, described in detail below. NSA has taken steps to remedy the areas of concern, and to ensure to the extent possible they will not recur. NSA is continually modernizing its architecture to incorporate stronger safeguards and provide more rigorous and efficient control and monitoring of the PR/TT metadata. Implementation of the envisioned changes in architectural design and oversight procedures described in this report will help mitigate vulnerabilities and correct the problems identified in the end-to-end review.

~~(TS//SI//NF)~~ There was no single cause of the issues identified through the PR/TT end-to-end review. In fact, a number of successful oversight, management and technology processes in place operated as designed. The problems NSA experienced stemmed from a lack of shared understanding of the full scope of the program, to include its implementation and end-to-end design among the key mission, technology, legal and oversight stakeholders. The complexity of the overall configuration, due in part to the intricacy of the system and the differing rules associated with NSA's various authorizations, was also a contributing factor, as was the fact that NSA oversight was primarily focused on analyst access to and use of the archived metadata.

~~(TS//SI//NF)~~ This report, which assumes a basic knowledge of NSA's structure and some familiarity with the FISC documents associated with the PR/TT program, addresses previously identified and newly uncovered areas of concern, as well as the associated corrective actions already taken, and those on-going or proposed, to address these issues. It also describes the minimization and oversight procedures NSA proposes to employ should the FISC decide to approve NSA's resumption of previously authorized activities involving the PR/TT metadata, to include automated alerting and automated querying of the metadata. Additionally, the report outlines the checks, balances and safeguards engineered into the system; points to the need, in some cases, to clarify existing language in the Court Order and associated documents; and describes enhanced training for the workforce that is designed to help prevent future instances of non-compliance. Finally, the report includes a summary of a proposed technical architecture designed to further protect PR/TT metadata.

~~(TS//SI//NF)~~ In moving forward, NSA will not only address the specific technical and process issues identified in this report, but will also implement changes in order to increase transparency and awareness among accountable parties and establish an overarching common view of the entire PR/TT program.

(U//~~FOUO~~) NSA may produce additional supplements to this report or other documents to the extent necessary to respond to additional items that may be of interest to the Court.

II. ~~(TS//SI//NF)~~ NSA's PR/TT Review

A. (U) Methodology and Scope

~~(TS//SI//NF)~~ NSA established a team of experts to conduct an end-to-end systems engineering and process review of the PR/TT metadata workflow and invited representatives from the National Security Division (NSD) of the Department of Justice (DoJ) to participate in certain discussions.

~~(TS//SI//NF)~~ For this review, NSA focused on the requirements of the [redacted] PR/TT Primary Order and associated documents since these reflected the technical architecture and operational practices as of the commencement of the review. Although NSA's review of certain technical and operational processes reached back in time, NSA did not embark on a complete review of each of the Court Orders over the five-year history of this program. Since [redacted] the Court has issued new Orders renewing NSA's PR/TT authority[1] and Supplemental Orders[2] seeking additional information and further defining NSA's PR/TT authority, in some instances resolving areas of concern noted during the review. Where applicable, this report references provisions from these later Orders.

~~(TS//SI//NF)~~ During the review, the team sought to identify systemic areas of concern, in which either a risk of non-compliance had materialized into multiple incidents of non-compliance, or a risk of non-compliance had not materialized into an incident but nonetheless warranted

[1] ~~(S//NF)~~ Docket Number PR/TT [redacted]
[2] ~~(S//NF)~~ Docket Number PR/TT [redacted] Supplemental Orders dated [redacted]

additional preventive measures. NSA revisited individual incidents of non-compliance previously reported to the Court only if they suggested a larger area of concern.

~~(TS//SI//NF)~~ The team reviewed 113 requirements extracted from the [redacted] PR/TT Primary Order and associated documents, as well as dataflow diagrams and system documentation (to include systems engineering and security plans) to ensure a complete understanding of how the requirements were being applied in the PR/TT program. The team then used the requirements as a basis to examine six key aspects (systems architecture, analyst workflow, management control, compliance auditing, oversight, and training) of NSA's handling of PR/TT metadata, and to establish a comprehensive plan to ensure that all requirements are addressed and properly implemented.

B. (U) Summary

~~(TS//SI//NF)~~ A critical step in preparing to conduct the end-to-end review was to identify and map how all the system and process components fit together. The team reviewed the following nine "components," listed as systems (items 1 through 5) and processes (items 6 through 9):

1. [redacted]
2. [redacted] NSA's corporate file transfer/distribution system
3. [redacted] NSA's corporate contact chaining system
4. [redacted] an NSA corporate repository for Digital Network Intelligence (DNI) metadata
5. [redacted] an NSA database analytic system and user interface tool
6. Reasonable Articulable Suspicion (RAS) Approval Process
7. Activity Detection (Alerting) Process
8. PR/TT Analytic Tools and Processes
9. PR/TT Analyst Decision and Reporting Process

~~(TS//SI//NF)~~ The interaction of these systems and processes as of [redacted] can be summarized briefly as follows: [redacted] The PR/TT metadata is then forwarded to [redacted] which then forwards one full copy of the PR/TT metadata to [redacted] and another to [redacted] serve as storage repositories for the PR/TT metadata. [redacted] processes the PR/TT metadata, including generation of contact chain summaries,[4] and organizes and stores the PR/TT metadata [redacted] in a way that enables queries with RAS-approved seeds and in a format that is usable by PR/TT-authorized

[3] ~~(TS//SI//NF)~~ Unless otherwise noted, "PR/TT metadata" refers to the authorized categories of metadata that are forwarded to NSA, but excludes any information returned as the result of a query against that metadata. The Court's Orders and associated documents also refer to PR/TT metadata as, among other things, "PR/TT information," "PR/TT data," "PR/TT datasets," and "information derived from the pen registers and trap and trace devices."

[4] ~~(TS//SI//REL TO USA, FVEY)~~ A "contact chain summary" summarizes the communications between two selectors, for example, that Selector A communicated with Selector B, their first and last contact dates, the data source information, and the total number of communications between A and B.

analysts.[5] Until recently, [redacted] also processed automated queries of RAS-approved seeds and pushed the results to [redacted] to allow non-PR/TT-authorized analysts to view query results. This automated process was disabled in [redacted] Query results[6] had been made available to PR/TT-authorized and other NSA analysts through [redacted] analytic results and through [redacted] Analysts also used the following processes: the *RAS Approval Process*, the *Activity Detection (Alerting) Process*, the PR/TT *Analytic Tools/Processes*, and the *PR/TT Analyst Decision/Reporting Process* to identify, query, analyze and ultimately disseminate information derived from the PR/TT metadata. These nine components, part of a large and complex system, are further described below and are pictured in Figures 1-10. Figure 1 provides a top-level view of the overall architectural system, Figure 2 highlights the nine components and Figures 3-10 highlight each of the individual components for ease of readability. Each component is reflected with corresponding colors in the diagrams.

~~(TS//SI//NF)~~ In concert with this systems engineering end-to-end review, NSA conducted a thorough review of its analytic tools and processes, management controls, auditing mechanisms, oversight, and training for handling the PR/TT metadata. The review led to several additional audits to ensure that no compliance incidents had occurred, and to examine whether the individuals who worked with the PR/TT metadata fully understood the applicable authority and limitations. As a result, documentation and training are being updated. Each part of the review compared the component or process being reviewed with the relevant requirements extracted from the Court documents.

(U//~~FOUO~~) The following provides a short description of the each of the nine components and any associated issues identified as part of the review.

1. ~~(TS//SI//NF)~~ [redacted] Access to the [redacted] system that handles the PR/TT metadata is strictly controlled by a group administrator account with limited access (the group account is being replaced with individual accounts to further enhance accountability). The [redacted] system resides on NSA's private, classified network. Further, access to the [redacted] network from the rest of the NSA network is controlled by a firewall, segmenting it from other classified networks.

[5] ~~(TS//SI//NF)~~ "PR/TT-authorized analysts" refers to those analysts authorized by the Court Order to query the PR/TT metadata.

[6] ~~(TS//SI//NF)~~ "Query results" could include information provided orally or in writing, and could include a tip or a lead, a written or electronic depiction of a chain [redacted] a compilation or summary of direct or indirect contacts of a RAS-approved seed, a draft or finished report, or any other information that would be returned following a properly predicated PR/TT query.

~~(TS//SI//NF)~~ Discrepancies in the description of NSA's practices associated with collection and extraction were identified in the end-to-end review and are described in Section III.B.11. It is believed that these can be resolved with changes to language in the next application for renewal of PR/TT authority.

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

~~(TS//SI//NF)~~ [redacted] NSA's corporate file forwarding service, provides for distribution of the PR/TT metadata from the collection source to the analytic repositories. [redacted] accepts files from the sources and transports those files to the end destinations as identified in the filename assigned.

~~(TS//SI//NF)~~ [redacted] is configured to allow the PR/TT dataflows and system accesses by technical personnel to be monitored and logged. The [redacted] system has security controls that are documented across multiple System Security Plans (SSPs). [redacted] employs security access controls, such as Public Key Infrastructure (PKI), to verify users and their system level access and likewise employs file transfer controls[7] to verify file transfer access, file source and file destination. The [redacted] system also employs a stringent configuration management methodology such that software changes cannot be implemented without the required testing and approval.

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

~~(TS//SI//NF)~~ [redacted] NSA's corporate contact chaining system, accepts metadata from multiple sources. It accepts the PR/TT metadata files from [redacted] stores the metadata in a separate partition; performs data quality, preparation and sorting functions; and then [redacted] represented in the processed data. [redacted] stores the resulting [redacted] and transaction records and provides authorized analysts with access to these [redacted] nd subsequent transaction records.

~~(TS//SI//NF)~~ [redacted] provides the necessary protection of the PR/TT metadata while it is in the [redacted] domain. [redacted] has always employed access controls such as a corporate authentication and authorization service, system security, and configuration management practices to protect the PR/TT metadata residing in its database and ensure it is accessed only by authorized analysts. These controls include, but are not limited to, a fully certified and accredited system under an SSP and effective use of a corporate authentication and authorization service. In addition, on [redacted] in response to a compliance issue identified with the Business Records (BR) FISA program, NSA installed a software restriction, the Emphatic Access Restriction (EAR), which ensured that only RAS-approved selectors could be used in queries of the BR or PR/TT metadata in [redacted]. Also on [redacted] NSA removed the system level certificate that had been used by automated tools to access the PR/TT metadata. In so doing, NSA disabled automated querying of the PR/TT metadata in [redacted]. Access to the PR/TT metadata chaining information in [redacted] is strictly controlled

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

via individual user access authentication/permission and this access is logged in accordance with the PR/TT Court Order.

~~(TS//SI//NF)~~ Three issues of concern identified in the end-to-end review relate to [redacted] One involves a data enrichment feature available through the [redacted] the Graphical User Interface (GUI) for analyst access to [redacted] data and services. A second involves use of a defeat list which included [redacted] PR/TT-derived selectors to manage data ingest volumes more effectively. The third involves retention of chain summaries beyond the timeframe allowed by the Court. These issues are more fully described in Sections III.B.8, III.B.2 and III.B.4.

4/5. (U//~~FOUO~~) [redacted]
~~(TS//SI//NF)~~ Prior to [redacted] when the automated processing was still functioning, [redacted] a corporate metadata repository, processed automated queries of RAS-approved seeds. [redacted] pushed the results to [redacted] a database analytic system and user interface tool used for [redacted] to facilitate more comprehensive target activity tracking. Through [redacted] non-PR/TT-authorized analysts could view these automated query results without assistance from a PR/TT-authorized analyst. The practice of sharing PR/TT query results with non-PR/TT-authorized analysts was later determined not to have been adequately described to the Court. Since [redacted] non-PR/TT-authorized analysts no longer have access to any PR/TT-derived query results. Further discussion of this issue can be found in Section III.B.5.

~~(TS//SI//NF)~~ No issues related to [redacted] were identified as access to PR/TT data was appropriately protected and queries were performed using only RAS-approved seeds. Other than the sharing of PR/TT automated query results with non-PR/TT-authorized analysts, no other issues related to [redacted] were identified.[8]

6. (~~TS//SI//NF~~) Reasonable Articulable Suspicion (RAS) Approval Process:
~~(TS//SI//NF)~~ The PR/TT RAS Approval Process includes the mechanisms NSA employs to determine that a particular selector is associated with the Foreign Powers[9] before a PR/TT-authorized analyst may use the selector as a seed to query the PR/TT metadata. RAS Approval requests are evaluated by a designated approval authority as defined in the PR/TT Order, and in the case of email [redacted] reasonably believed to be used by U.S. persons, by NSA's Office of General Counsel (OGC).

~~(TS//SI//NF)~~ The RAS Approval Process in place for querying PR/TT metadata incorporates a combination of documented guidance and well-understood procedures as

[8] ~~(TS//SI//NF)~~ Although NSA did not identify any compliance concerns related to [redacted] or [redacted] NSA realized on [redacted] that the automated query process was still running within [redacted] and [redacted] after NSA had represented to the Court that the automated query processes had ceased on [redacted] NSA immediately stopped this automated query process, and the Court was informed of this misstatement via a Rule 10(b) notice filed on [redacted]

[9] ~~(TS//SI//NF)~~ Foreign Powers, in the context of the current PR/TT Order, refers to [redacted]

outlined in an OGC RAS Memo and a Working Aid used by NSA's Office of Counterterrorism. The one RAS-related issue that was uncovered during the review involved only two selectors and is detailed in Section III.B.3.

7. (~~TS//SI//NF~~) Activity Detection (Alerting) Process:

(~~TS//SI//NF~~) The now-disabled Activity Detection (Alerting) Process was a process by which NSA could determine when certain high-priority terrorist-associated email accounts [redacted] NSA disabled this process on [redacted] with the implementation of the EAR.

(~~TS//SI//NF~~) The only issue uncovered during the review related to the Activity Detection Process concerns automation and is covered in Section III.B.1.

8. (~~TS//SI//NF~~) PR/TT Analytic Tools and Processes:

(~~TS//SI//NF~~) Homeland Security analysts from NSA's Office of Counterterrorism used a variety of tools and processes to help them identify and evaluate terrorist communications or activities associated with the U.S. homeland. These tools and processes can be characterized in three categories: those that helped analysts view and manage activity detection (alerting), those that helped PR/TT-authorized analysts and automated processes chain email communications from RAS-approved seeds, and those that [redacted]

(~~TS//SI//NF~~) [redacted] analytic tools and processes were identified and examined in the end-to-end review, but only one tools-related issue was identified. The [redacted] tool, which is under the [redacted] architecture, left NSA indirectly vulnerable to using correlated selectors (including non-RAS approved selectors) to query PR/TT metadata prior to the implementation of the EAR, but audits showed that no such querying actually occurred. Further discussion of this issue can be found in Section III.B.9.

(~~TS//SI//NF~~) [redacted] analytic tools and processes examined were developed under the [redacted] systems architecture and are well-documented, configuration-controlled and audited. Another was developed outside of the [redacted] architecture and is also well-documented, configuration-controlled and audited. The remaining [redacted] examined were developed in whole or in part by engineers working in the Office of Counterterrorism to meet constantly changing mission requirements, resulting in limited configuration and change management control. Of the [redacted] tools and processes, only one, a tool that helps build lists of unwanted [redacted] is currently used against the PR/TT metadata. The others were disabled through the implementation of the EAR, the removal of system level certificates or, out of an abundance of caution, through other

means. Audits have shown no indications of compliance issues associated with any of the tools.

9. (~~TS//SI//NF~~) PR/TT Analyst Decision and Reporting:

(U//~~FOUO~~) The Analyst Decision and Reporting Process encompasses target knowledge, analytic procedures and legal and policy guidance. This overall process helps analysts determine which information meets customer requirements, assists them in prioritizing those requirements and informs their report drafting and dissemination decisions.

(~~TS//SI//NF~~) The analyst decision and reporting workflow formerly included notification to an analyst when a match occurred between a known, RAS-approved selector and an identifier in the ingested PR/TT metadata which was reasonably believed to be in the United States. Such alerts sometimes provided the lead, or starting point, for the analytic process.[10] With the exception of alerts, today as previously, leads are prompted by an external customer, such as FBI, with a Request for Information (RFI); derived from the work of other counterterrorism-related NSA target analysts; or generated by an analyst during the course of target development and discovery. While monitoring intercept related to existing RAS-approved selectors, analysts often discover that a target is in communication with previously unknown email selectors. Analysts use RAS-approved selectors as the starting point for PR/TT chaining in order to identify unknown selectors that may be terrorist-related. Based on these PR/TT-derived chaining results, analysts are then able to determine if the previously unknown selector is in contact with any of the Foreign Powers. If NSA has reason to believe the information constitutes valid terrorist-related activity, NSA applies Court-approved minimization procedures, as needed, before reporting the results of PR/TT analysis outside NSA.

(~~TS//SI//NF~~) As part of the end-to-end review, NSA also developed a detailed description of the analytic workflow which was examined to ensure the PR/TT metadata was appropriately handled, analyzed and disseminated. The new areas of concern related to dissemination and reporting are discussed in Sections III.B.5, III.B.6, and III.B.7.

III. (U) Previously Reported Items and Newly Identified Areas of Concern

(~~TS//SI//NF~~) The PR/TT review considered one previously reported item and identified eleven additional areas of concern, many of which are similar to those uncovered in the BR FISA end-to-end review.

A. (U) Previously Reported Item

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

[10] (~~TS//SI//NF~~) As of [redacted], when implementation of the EAR shut down the Activity Detection Process, the Analyst Decision and Reporting workflow changed accordingly.

(U) Description

~~(TS//SI//NF)~~ Through a Declaration filed on [redacted] NSA described to the Court two separate practices NSA had employed in support of the RAS determinations on certain selectors. Through the first, [redacted] those foreign selectors that would meet the RAS standard as soon as NSA identified a direct contact between the proposed seed and one of the Foreign Powers. [redacted] Through the second, [redacted] NSA stopped both of these practices in [redacted] NSA provided the Court with a thorough description of each of these processes in the [redacted] Declaration and again in the 90-Day Report submitted in support of the Application to renew the PR/TT authority.[12] In its [redacted] Primary Order, the Court recognized that neither practice was in use and ordered that NSA should not resume either practice without obtaining prior Court approval.

(U) Remedial Steps

(U//~~FOUO~~) These practices ceased in [redacted] and NSA does not intend to reinstitute them.

B. (U) Newly Identified Areas of Concern

~~(TS//SI//NF)~~ The PR/TT end-to-end review revealed eleven areas of concern, as discussed below, the last three of which can more precisely be described as vulnerabilities or discrepancies in describing NSA practices.

1. ~~(TS//SI//NF)~~ Automation of Activity Detection (Alerting) Process
2. ~~(TS//SI//NF)~~ PR/TT Metadata Retention and Destruction
3. ~~(TS//SI//NF)~~ RAS Approval based on Attorney General Authorizations
4. ~~(TS//SI//NF)~~ Use of PR/TT Metadata [redacted]
5. ~~(TS//SI//NF)~~ Sharing of Unminimized Query Results with Non-PR/TT-Authorized Analysts
6. ~~(TS//SI//NF)~~ External Access to Unminimized PR/TT Metadata Query Results
7. ~~(TS//SI//NF)~~ Approval of the Dissemination of U.S. Person Identities
8. ~~(TS//SI//NF)~~ [redacted]
9. ~~(TS//SI//NF)~~ Risk of Using Non-RAS-Approved Correlated Selectors to Query PR/TT Metadata
10. ~~(TS//SI//NF)~~ Handling of the PR/TT Metadata
11. (U//~~FOUO~~) Discrepancies in Descriptions of NSA's Practices

---

[11] ~~(TS//SI//NF)~~ The Station Table serves as the historic reference of all PR/TT selectors that have been assessed for RAS – and their associated RAS determinations.

[12] ~~(S//NF)~~ Docket Number PR/TT [redacted] Exhibit B at pp. 7-11.

1. ~~(TS//SI//NF)~~ Automation of Activity Detection (Alerting) Process

(U) Description

~~(TS//SI//NF)~~ NSA's Activity Detection Process, formerly known as the alerting process, involved [redacted] automated queries using RAS-approved seeds against the PR/TT metadata stored in NSA's [redacted] database. These automated queries returned all of the direct (one-hop) and indirect (two-hop) contacts, and provided "alerts" to PR/TT-authorized analysts when either the RAS-approved seed or a direct contact of the RAS-approved seed appeared to have been accessed [redacted] On [redacted] NSA [redacted] when it implemented the EAR to address BR FISA issues. The EAR prohibited queries with non-RAS-approved selectors against either the BR FISA metadata [redacted] the PR/TT metadata in [redacted]. Although, unlike the BR FISA, the PR/TT alerting process had not queried with non-RAS-approved selectors, the corrective measure deemed necessary for the BR FISA – the EAR – had foreseeable, but unavoidable consequences, including the disruption of the PR/TT Activity Detection Process. After [redacted] NSA reported to the Court that its Activity Detection Process had stopped.

~~(TS//SI//NF)~~ The Activity Detection Process itself – a process comprising several distinct steps – did stop on [redacted]. Because this process had not been designed to integrate with the EAR, the EAR precluded one-hop or two-hop chaining, [redacted] What continued to run, without interference by the EAR, was the very first step of the Activity Detection Process, *i.e.*, the scanning and comparison of the incoming PR/TT metadata against the list of RAS-approved selectors and the storage of those records where a RAS-approved selector was identified.

~~(TS//SI//NF)~~ During the end-to-end review of NSA's Activity Detection Process, representatives from DoJ's NSD and NSA concluded that the Court had not been told that the first step of the Activity Detection Process continued to scan and compare the PR/TT metadata against the list of RAS-approved selectors, although the results were not presented to analysts.

(U) Remedial Steps

~~(TS//SI//NF)~~ On [redacted], NSA further disabled the Activity Detection Process by replacing the list of RAS-approved selectors that served [redacted] As a result, the incoming PR/TT metadata stream is no longer queried with any selectors pursuant to this process. DoJ's NSD filed a Rule 10(b) notice with the Court on [redacted] to explain in greater detail the operation and disabling of the first step of the Activity Detection Process.

2. (~~TS//SI//NF~~) PR/TT Metadata Retention and Destruction

(U) Description

(~~TS//SI//NF~~) The Court's Orders require that "[i]nformation obtained from the authorized pen registers and trap and trace devices shall be available online for querying . . . for four and one-half years. Metadata shall be destroyed no later than four and one-half years after its initial collection."[13] To assess compliance with this requirement, the end-to-end review team considered the repositories, databases and archives in which PR/TT metadata might be stored, and the controls in place – whether technical or management controls – to ensure destruction in accordance with the Court's Orders.

(~~TS//SI//NF~~) NSA has relied on both technical controls and management controls to ensure destruction of the PR/TT metadata no later than four and one-half years after its initial collection. Both [redacted] automatically purge PR/TT metadata within the applicable timeframe [redacted]). NSA provides training to technical personnel, including guidance on the destruction requirements in the Court's Orders. Technical personnel are permitted to place samples of PR/TT metadata in shared directories for quality control analysis. As part of the end-to-end review, NSA searched for PR/TT records in these shared directories and found none derived from PR/TT metadata collected more than four and one-half years ago.

(~~TS//SI//NF~~) NSA currently maintains back-up tapes of PR/TT metadata for each calendar year for mission assurance and continuity of operations purposes. The back-up metadata is not online and is not available for querying. Since an entire calendar year of data is saved on one set of tapes, NSA cannot purge individual metadata records as they initially reach the four and one-half year mark without purging an entire calendar year's worth of data. Therefore, a set of PR/TT metadata back-up tapes is purged once the latest date of information stored on that set reaches the four and one-half year mark. As the latest date of information on the 2004 PR/TT metadata back-up tapes has since reached the four and one-half year mark set by the Court, in [redacted] NSA sent these tapes for destruction.

(~~TS//SI//NF~~) During the end-to-end review, NSA's technical experts described chain summaries to the participating representatives from DoJ's NSD, and explained how NSA treated chain summaries. A chain summary summarizes communications contacts between two selectors. When a PR/TT-authorized analyst enters a query with a RAS-approved selector, [redacted] looks to [redacted] associated with that seed and returns all of the one- or two-hop contacts of the seed (depending upon how the analyst has structured his query). The information returned from the chain summaries will include, among other things the seed; the direct (and possibly indirect) contacts of the seed; [redacted]

[13] (~~S//NF~~) Docket No. PR/TT [redacted], Primary Order at p.12.

~~(TS//SI//NF)~~ [redacted] When the last contact date of a PR/TT-derived contact chain summary hits the four and one-half year mark, NSA's automated purging processes destroys the entire contact chain summary. However, because NSA's automatic purging processes will not destroy any contact chain summary reflecting communications if the "last contact date" has not yet reached the four and one-half year mark, contact chain summaries exceeding a total span of more than four and one-half years (*e.g.*, first contact in August 2004, last contact in May 2009) would continue to be retained. Because contact chain summaries do not reflect dates of each individual communication between communicant pairs, NSA cannot destroy the four and one-half years old or older portion of the contact chain summary without destroying the entire contact chain summary.

(U) Remedial Steps

~~(TS//SI//NF)~~ DoJ's NSD and NSA concluded that NSA's retention of contact chain summaries that spanned more than four and one–half years of continuing communications between two identifiers did not comply with the terms of the Court's Orders, nor did the retention of back-up tapes containing PR/TT metadata older than four and one-half years. In July 2009, NSA also submitted the 2005 tapes for destruction, which will result in no data older than three years seven months being stored offline, well within the Court's destruction requirements. A notice was filed with the FISC on this matter on [redacted] and NSA intends to work with DoJ's NSD to resolve this issue.

3. ~~(TS//SI//NF)~~ RAS Approval Based on Attorney General Authorizations

(U) Description

~~(TS//SI//NF)~~ Since [redacted], the PR/TT Orders have permitted NSA to rely on the Court's finding of probable cause that a U.S. person selector is used by an agent of one of the Foreign Powers in lieu of a formal RAS determination by one of the designated approval authorities and NSA's OGC.[14] The PR/TT Orders made no exception for a probable cause finding by anyone else; in other words, NSA could not rely on the Attorney General's finding of probable cause under an emergency authorization in advance of Court review. In that circumstance, NSA would be required either to proceed with a formal RAS determination through a designated approval authority and NSA's OGC or to wait for the Court's ratification of the Attorney General's finding. In [redacted], NSA determined that it had deemed two email addresses to be RAS-approved based on the Attorney General's finding of probable cause in advance of the Court's issuance of FISA orders. NSA chained on these two email addresses in the brief interval between the RAS-approval and the Court's issuance of FISA orders, but the chain queries produced no results. These incidents were reported to the Court on [redacted], in both NSA's 30-Day Report filed in docket number PR/TT [redacted] and a Rule 10(c) notice.[15]

[14] ~~(S//NF)~~ Docket No. PR/TT [redacted], Primary Order at p. 12.
[15] ~~(S//NF)~~ Docket No. PR/TT [redacted]

(U) Remedial Steps

~~(TS//SI//NF)~~ In [redacted], NSA determined that selectors had been deemed RAS-approved based on the Attorney General's emergency authorization and conducted an audit which was completed in [redacted] NSA provided guidance on [redacted] to all of the designated approval authorities to ensure that email [redacted] would not be deemed RAS-approved based solely on the Attorney General's emergency authorization.

4. ~~(TS//SI//NF)~~ Use of PR/TT Metadata [redacted]

(U) Description

~~(TS//SI//NF)~~ During the end-to-end review, the team determined that NSA had not provided the Court with a full description of the processes employed to block or purge certain unwanted metadata from NSA's repositories. Although NSA had described to the Court [redacted] NSA had not explained that both technical personnel, in the conduct of their metadata management and organization functions, and analysts, in the conduct of their analytic processes, flagged [redacted] for inclusion on a "defeat list" used to block and purge unwanted metadata. Nor had NSA explained that it used this defeat list, which included PR/TT-derived selectors, to block and purge metadata from both PR/TT metadata repositories and non-PR/TT metadata repositories.

(U) Remedial Steps

~~(TS//SI//NF)~~ In a Supplemental Declaration filed on [redacted] NSA explained its defeat list practices to the Court. By Supplemental Order dated [redacted], the Court authorized NSA to (1) continue to use the master defeat list for metadata reduction and management purposes in both repositories containing PR/TT metadata and repositories containing non-PR/TT metadata; (2) add to the master defeat list [redacted] discovered by technical personnel during the [redacted] and (3) add to the master defeat list [redacted] discovered by NSA analysts reviewing the results of authorized queries of PR/TT metadata.

5. ~~(TS//SI//NF)~~ Sharing of Unminimized Query Results with Non-PR/TT-Authorized Analysts

(U) Description

~~(TS//SI//NF)~~ The results of PR/TT metadata queries have been routinely made available to the broader population of NSA analysts working counterterrorism targets. This sharing helps ensure that analysts with specific foreign target expertise can apply the full scope of their knowledge to the PR/TT-generated information to identify all possible terrorist connections quickly and characterize them within the context of the target's known activities. With [redacted] NSA analysts approved to query the PR/TT metadata and more than [redacted] NSA analysts working various aspects of the counterterrorism mission enterprise-wide, less than ten percent of NSA's counterterrorism analysts currently are authorized to access the PR/TT metadata. Thus, the

collective experience of the PR/TT-authorized analysts represents a small fraction of NSA's overall expertise on counterterrorism targets. Counterterrorism target analysts beyond the small number currently authorized to query the PR/TT metadata are responsible for analyzing the data in the context of SIGINT information and writing reports. NSA believed such internal sharing of PR/TT metadata query results (as distinct from the PR/TT metadata itself) was consistent with the Court's Orders which required that query results be treated in accordance with United States Signals Intelligence Directive 18 (USSID 18), but NSA had not included a complete description of this necessary sharing practice to the Court in its periodic reports prior to [redacted]

(U) Remedial Steps

~~(TS//SI//NF)~~ In the [redacted] Order, the Court explicitly authorized NSA to continue internal sharing of query results with NSA analysts other than PR/TT-authorized analysts, provided all analysts receiving such results receive appropriate and adequate training and guidance regarding all rules and restrictions governing the use, storage and dissemination of such information. NSA is in the process of coordinating this training with DoJ's NSD, as required.

6. ~~(TS//SI//NF)~~ External Access to Unminimized PR/TT Metadata Query Results

(U) Description

~~(TS//SI//NF)~~ In examining NSA's practice of sharing PR/TT metadata query results internally with other NSA analysts working authorized counterterrorism targets, NSA learned of CIA, FBI and NCTC analyst access to unminimized PR/TT metadata query results and target knowledge information via an NSA counterterrorism database. This matter stemmed from a collaboration practice recommended by the Directors of NSA, CIA and FBI that was in place prior to the inception of the first PR/TT Order. An interagency group established by the Directors of NSA, CIA and FBI had recommended in 2002 that NSA create a common target knowledge database to allow joint research and information exchanges [redacted] Over time, approximately 250 analysts at CIA, FBI and NCTC had been granted access to this target knowledge base. [redacted] this practice was not modified to conform with the Order's requirements for the dissemination of PR/TT metadata-derived query results outside of NSA.

(U) Remedial Steps

~~(TS//SI//NF)~~ While NSA disabled the hyperlink button used by the external analysts to access this target knowledge database in [redacted] NSA learned that the external analysts could have still accessed the data if they had retained the URL address. Upon identifying this as an area of concern on [redacted] NSA began terminating external customer account access to the target knowledge database, completing the action by [redacted] In the [redacted] Order, the FISC directed NSA to provide the Court with "a full explanation of why the government has permitted the dissemination outside NSA of U.S. person information without regard to whether such dissemination complied with the clear and acknowledged requirements for sharing U.S.

person information ... pursuant to the Court's [PR/TT] orders." This "full explanation," which covers both BR and PR/TT, will be provided in a separate document.

7. ~~(TS//SI//NF)~~ Approval of the Dissemination of U.S. Person Identities

(U) Description

~~(TS//SI//NF)~~ The Court's Order requires NSA to apply USSID 18 to minimize information concerning U.S. persons obtained from the PR/TT authority. The Court's Order also requires that "[p]rior to disseminating any U.S. person information outside of the NSA, the Chief of Information Sharing Services . . . shall determine that the information is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance."[16]

~~(TS//SI//NF)~~ As part of the end-to-end review, NSA examined the [redacted] intelligence reports issued that included PR/TT-derived information. NSA confirmed that [redacted] of these reports contained U.S. person identities, but that the Chief of Information Sharing Services approved the release of only [redacted] of these [redacted] reports. Other NSA officials authorized under USSID 18 to approve the dissemination of U.S. person identities but not listed specifically in the Court's Order approved the release of the remaining reports. These officials included the Deputy Chief of Information Sharing Services and the Senior Operations Officer (SOO) of NSA's 24-hour National Security Operations Center.

~~(TS//SI//NF)~~ On [redacted], NSA submitted a Supplemental Declaration to the Court describing its past practices with respect to the dissemination of reports containing U.S. person identities. In a Supplemental Order, the Court found that "NSA has generally failed to adhere to the special dissemination restrictions originally proposed by the government, repeatedly relied upon by the Court in authorizing the collection of the PR/TT metadata[.]"[17]

(U) Remedial Steps

~~(TS//SI//NF)~~ On [redacted] NSA's OGC advised the Office of Information Sharing Services that the Chief of that office was the only NSA official authorized to approve the dissemination of any U.S. person identity derived from PR/TT metadata, and that the Chief must make the required findings and document those findings prior to any such dissemination. NSA, in conjunction with DoJ's NSD, is reviewing the [redacted] intelligence reports issued that contained U.S. person identities to determine whether the U.S. person identities were derived in whole or in part from PR/TT metadata and whether the NSA officials made the necessary findings required under the Court's Orders. The results of this review will be reported to the Court.

~~(TS//SI//NF)~~ On [redacted] the Court ordered that NSA provide the Court with a weekly report listing each instance in which NSA shared in any form information obtained from either BR or PR/TT metadata with anyone outside of NSA, and that the Chief of Information Sharing

[16] ~~(S//NF)~~ Docket No. PR/TT [redacted] Primary Order at p. 12.
[17] ~~(S//NF)~~ Docket No. PR/TT [redacted], Supplemental Order of [redacted] at p. 4.

Services certify that any dissemination of U.S. person information satisfied the requisite standard. NSA submitted the first of these reports on [redacted]

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

(U) Description

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

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

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

(U) Remedial Steps

~~(TS//SI//NF)~~ [redacted] DoJ orally notified the Court of this matter on [redacted] and a rule 10(C) notice was filed with the Court on [redacted]

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

~~(TS//SI//NF)~~ The following three issues were identified either as areas of vulnerability without any known incidents or discrepancies in describing NSA practices.

9. ~~(TS//SI//NF)~~ Risk of Using Non-RAS-Approved Correlated Selectors to Query PR/TT Metadata

(U) Description

~~(TS//SI//NF)~~ [redacted] is populated in a variety of ways including input from individual analysts whose information may come from diverse sources, such as [redacted]

~~(TS//SI//NF)~~ Prior to the development of the EAR, which prevents chaining the PR/TT metadata in [redacted] with non-RAS-approved selectors, an analyst had the ability to chain on any selector (whether RAS-approved or not) identified using [redacted] Though this vulnerability existed, audits revealed that no violations occurred. NSA believes this was due to effective analyst training and management oversight.

(U) Remedial Steps

~~(TS//SI//NF)~~ On [redacted] PR/TT-authorized analysts' access to [redacted] was disabled as a preventive measure.

~~(TS//SI//NF)~~ Based on this vulnerability and the potential for violating the Court Orders for PR/TT, NSA's Oversight and Compliance (O&C) conducted an audit of [redacted] covering [redacted] and found no compliance violations. This audit identified any correlations provided to an authorized PR/TT analyst by [redacted] and then verified that none of those correlated selectors had been used to query PR/TT metadata.

10. ~~(TS//SI//NF)~~ Handling of the PR/TT Metadata

(U) Description

~~(TS//SI//NF)~~ During the end-to-end review, it was discovered that PR/TT-authorized analysts stored query results in shared directories. PR/TT-authorized technical personnel also stored PR/TT metadata in a shared directory for testing and evaluation purposes and normally deleted the metadata when the evaluation was complete. NSA personnel beyond those specifically authorized to access PR/TT metadata had access to these shared directories, either directly or through a development server. Although these individuals could have found their way to stored PR/TT metadata and query results, it is highly unlikely that they would have done so. To find files holding PR/TT metadata and query results within these shared directories would have required either specific knowledge of the directory and file names, or chance. Nonetheless, the placement of PR/TT metadata and query results in these shared directories resulted in a vulnerability to improper use.

(U) Remedial Steps

~~(TS//SI//NF)~~ NSA immediately implemented additional access controls which ensure that only those specifically authorized personnel required to access the files as part of their assigned duties can now access the PR/TT metadata and/or query results.

11. (U//~~FOUO~~) Discrepancies in Descriptions of NSA's Practices

(U) Description

~~(TS//SI//NF)~~ Over time, NSA's Applications for renewal of the PR/TT authority and supporting documents have not always successfully conveyed NSA's implementation of the authority. Additionally, the Applications and supporting documents have not always reflected modifications in NSA's implementation of this authority based on changes in technology, capabilities or practices. This is an area of concern because in certain respects NSA's implementation may not be precisely aligned with the official Court documents. For example:

- Though it is stated that [redacted] is applied under certain circumstances but not under others due to technical limitations of the PR/TT metadata generators.
- [redacted]
- The Court Order states that "any processing by technical personnel of the PR/TT metadata acquired pursuant to this Order shall be conducted through the NSA's private network, which shall be accessible only via select machines and only to cleared technical personnel, using secured encrypted communications."[21] While the way in which NSA protects the data is not precisely as stated in the Court Order,[22] we believe NSA's implementation *is* consistent with the intent of preventing unauthorized users from accessing the data.[23]

---

[19] ~~(S//NF)~~ Docket No. PR/TT [redacted] Exhibit A at pp. 16-17, n. 7.
[20] ~~(S//NF)~~ Docket No. PR/TT [redacted] Application at pp. 13.
[21] ~~(S//NF)~~ Docket No. PR/TT [redacted] Exhibit A at p. 21 (citing Docket No. PR/TT [redacted] Declaration at page 19).
[22] ~~(TS//SI//NF)~~ There are not specifically designated or "select" machines from which technical personnel access and process the data on NSA's private, secure network. The internal NSA communications paths on its classified networks are not encrypted, but are subject to strong physical and security access controls.
[23] ~~(TS//SI//NF)~~ The NSA complex is a Sensitive Compartmented Information Facility (SCIF) that is an accredited installation, incorporating strong physical and security access control measures (barriers, locks, alarm systems, armed guards), to which only authorized personnel are granted access. Within NSA, only approved users of NSANet can gain access to the network through login and password. Once on the network, the user can only access the PR/TT metadata if additional access controls specifically allow such access. Access to particular data sets is granted based on need-to-know and is verified via PKI.

(~~TS//SI//NF~~) In several other cases, NSA's implementation is precisely aligned with the official documents, but that alignment is at risk with changes in technology. Examples include:

- [redacted]
- [redacted]

(U) Remedial Steps

(~~TS//SI//NF~~) NSA has not consistently articulated to the Court how NSA's practices have evolved or the effect that changes in technology have on implementation. NSA intends to clarify the language regarding its practices in its next application to renew the PR/TT authority.

IV. (U//~~FOUO~~) NSA's Minimization and Oversight Procedures

(~~TS//SI//NF~~) NSA has well-documented and long-standing minimization procedures for ensuring protection of U.S. persons' information in SIGINT analysis and reporting under all SIGINT authorities, to include the PR/TT Order. NSA's normal regime of compliance oversight for handling PR/TT is a comprehensive, multi-pronged approach involving DoJ's NSD and NSA's OGC, Signals Intelligence Directorate's O&C, Office of the Inspector General (OIG) and the Signals Intelligence Directorate. Since [redacted], DoJ's NSD has been meeting with the appropriate NSA representatives at least once every renewal period to review the program and also conducts "spot checks" to review a sampling of justifications (RAS determinations) for querying the metadata. NSA, in turn, provides internal oversight to the PR/TT program by a variety of oversight controls and compliance mechanisms to prevent, detect, correct and report incidents and violations of the procedures. These include technical, physical and managerial safeguards such as: examining samples of records to ensure NSA is receiving only compliant data; ensuring analysts are trained in the querying, dissemination and storage restrictions for the metadata; monitoring analytic access to the metadata; auditing queries on a weekly basis by O&C; monitoring audit functionality; reviewing the PR/TT metadata database repositories; and examining the list of RAS-approved selectors.

(~~TS//SI//NF~~) In light of the compliance issues that surfaced specific to the handling of the PR/TT metadata, NSA reviewed its minimization procedures as well as its oversight procedures, to include auditing, documentation, and training, to identify areas for potential improvement. All were identified as areas for enhancement to ensure that personnel handling the PR/TT metadata are aware of and compliant with the Court Orders governing its use and dissemination.

---

[24] (~~S//NF~~) Docket No. PR/TT [redacted] Application at p. 13.
[25] (~~S//NF~~) Docket No. PR/TT [redacted] Application at p. 13.

A. (U) Minimization

~~(TS//SI//NF)~~ Every NSA intelligence analyst is required to complete training and pass a test on USSID 18 minimization procedures every two years as a prerequisite for access to unminimized/unevaluated SIGINT data. Additionally, intelligence analysts must receive an OGC compliance briefing and on-the-job training (OJT) regarding their responsibilities for handling metadata containing U.S. person information prior to being granted access to the PR/TT metadata. They also have on-line access to detailed working aids including required minimization procedures. NSA will continue to emphasize to PR/TT-authorized analysts the criticality of applying USSID 18 and the Court Order requirements as they relate to the handling and dissemination of information derived from PR/TT metadata.

B. (U) Oversight

1. (U//~~FOUO~~) Oversight Auditing Mechanisms

~~(TS//SI//NF)~~ NSA assessed requirements for auditing of systems, tools, processes and analyst queries to ensure the proper compliance procedures were in place. Seventeen audits related to PR/TT metadata access and querying have been conducted to date either as the result of standing requirements or in response to issues identified through the end-to-end review.

~~(TS//SI//NF)~~ NSA audits samples of queries conducted by PR/TT-authorized intelligence analysts in [redacted] on a weekly basis. As a result of a review of its oversight processes, O&C created a dedicated senior intelligence analyst position to enhance auditing of PR/TT FISA metadata queries.

2. (U//~~FOUO~~) Oversight Documentation and Procedures

~~(TS//SI//NF)~~ Oversight documentation and procedures governing both PR/TT and BR FISA metadata handling consists of a set of Standard Operating Procedures (SOP) that NSA previously has provided to DoJ's NSD and likewise has reviewed, revised and revalidated. They are as follows:

- **"Access":** This SOP outlines the procedures for gaining and maintaining access to the PR/TT metadata consistent with the PR/TT Court Order.
- **"Weekly Audit Procedures":** This document outlines the procedures used to audit PR/TT-authorized analyst queries of [redacted]
- **"Compliance Notification":** This document addresses the procedures to be followed when compliance issues are noted.
- **"DoJ and OGC Spot Checks":** This SOP addresses the procedures to be followed for the required, regular DoJ and/or OGC spot checks.
- **"Oversight":** This document outlines the roles and responsibilities of DoJ, DIRNSA, OGC, O&C, the OIG, SSO and those Office of Counterterrorism analysts approved for PR/TT metadata access.

~~(TS//SI//NF)~~ Prior to the review of all processes associated with NSA's PR/TT handling, the Associate Directorate of Education and Training (ADET) had already been working with O&C

and OGC to redesign the required training for accessing PR/TT metadata[26] to better enforce appropriate handling of this data and to introduce competency testing as part of the O&C curriculum. The curriculum will be administered on-line to allow students 24/7 access to the course material.

~~(TS//SI//NF)~~ The PR/TT training will address the knowledge and procedural components of handling PR/TT data. Students will be required to complete the following six lesson tutorials:

1. "Overview of the Reasonable Articulable Suspicion standard," as covered in OGC instructions
2. "Summary of the RAS standard," to aid NSA analysts in preparing RAS justifications
3. "Association with [redacted]" to identify how associations are established in order to qualify a target for RAS justification
4. "First Amendment Considerations," to identify limitations and considerations when targeting U.S. persons within PR/TT data
5. "Sources of information," to identify the supporting information used to justify the RAS determination
6. "The PR/TT FISC Order," which explains the storage, access, use and dissemination requirements of the PR/TT Orders

~~(TS//SI//NF)~~ A computer-based competency examination will be administered upon completion of this training and remediation will be provided for missed questions. Once an analyst has demonstrated the necessary knowledge by successfully passing the exam, he or she will complete formalized OJT before O&C grants access to the data. The formalized OJT will address how analysts are permitted to use the PR/TT metadata, reinforce the unique privacy concerns and handling requirements of this data, and demonstrate the various tools and processes that can be used to query the PR/TT metadata. The OJT component, which has always been administered by an experienced analyst, will now also be evaluated by a qualified ADET OJT lead with operational and instructional design experience to ensure that OJT currently in place meets required criteria.

~~(TS//SI//NF)~~ As part of the PR/TT training redesign, complete training records will be maintained by ADET for each individual. The documentation will include the test score, answers to individual test questions and performance feedback from the OJT component. This documentation will allow for tracking of access to the PR/TT data on an individual basis.

~~(TS//SI//NF)~~ In accordance with the [redacted] Court Order, NSA will provide appropriate and adequate training and guidance regarding all rules and restrictions governing the use, storage and dissemination of the PR/TT metadata query results to any analysts with whom these results will be shared.

[26] ~~(TS//SI//NF)~~ NSA has not deemed it necessary under the Court Orders to provide PR/TT-specific training to technical personnel responsible for NSA's underlying corporate infrastructure.

V. (U//~~FOUO~~) NSA's Future Architecture

(~~TS//SI//NF~~) Using principles of system engineering, configuration management and access control, NSA is exploring various plans to migrate the dataflow and life cycle management of the PR/TT metadata to its next generation system architecture which offers more effective and efficient management and control. This architecture is designed to be flexible enough to adapt to changes in the legal and oversight requirements, while conforming to applicable governing authorizations such as EO 12333 and PR/TT.

(~~TS//SI//NF~~) In a proposed future architecture, the end-to-end PR/TT dataflow would be referred to as a system "thread." As such, NSA would manage the entire capability via a "Thread Engineering Team" to guide the requirements development, systems integration, use-case development, testing/validation and planning for current and future enhancements. Thread engineers would meet with representatives from the OGC and oversight and compliance organizations to define and validate requirements prior to development. System-wide configuration management would be implemented to log the expected software builds and patches. Similar practices exist now, but there is no thread focused specifically on the PR/TT process.

(~~TS//SI//NF~~) The proposed systems supporting PR/TT dataflow and life cycle within the next generation architecture encompass both technical- and personnel-based strategies to ensure that data is accessed, retained and purged in full compliance with authorities granted to NSA by the FISC. Moreover, the implementation of centralized processes and databases will ensure that all aspects of the dataflow will continue to be tracked and audited to further ensure that any non-compliance issues can be promptly identified and addressed. Proposed plans for addressing key requirements for PR/TT metadata are as follows:

1. (U//~~FOUO~~) Security / Access Control

(~~TS//SI//NF~~) A new access control application will be applied to all databases and systems supporting the PR/TT workflow. This application will validate the credentials of users to govern which systems they are approved to access, and validate that their required training is current. PKI, which offers security measures for identification and authentication, as well as for access control, and audit capability, will be used to manage users with access to the metadata or query results.

2. (U//~~FOUO~~) Data Standardization

(~~TS//SI//NF~~) A data standardization platform will date-stamp the incoming PR/TT metadata and ensure the data is consistent and has an accurate structure. This will allow quick and accurate date-based purging once the Court-ordered timeframe has been reached.

3. (~~TS//SI//NF~~) Databasing RAS Selectors

(~~TS//SI//NF~~) An updated and improved centralized target knowledge database for storing telephony and email selectors has been under development since [redacted] This database

will enable more efficient storage and retrieval of key information about each PR/TT email identifier such as its RAS status, justification and OGC approval, as appropriate, for those that have been RAS-approved. These features are scheduled for completion during the fourth quarter of FY09.

4. (~~S//SI//REL TO USA, FVEY~~) Analytical Processing and Chaining

(~~S//SI//REL TO USA, FVEY~~) An enhanced chaining function and data processing capability will support large volumes of [redacted] algorithms, handle growing ingest rates and deliver faster query responses. Additionally, the metadata will be stored using security tags, a measure which can be used to restrict the visibility of individual entries in the database to only personnel with the appropriate access credentials.

5. (U//~~FOUO~~) Auditing and Monitoring

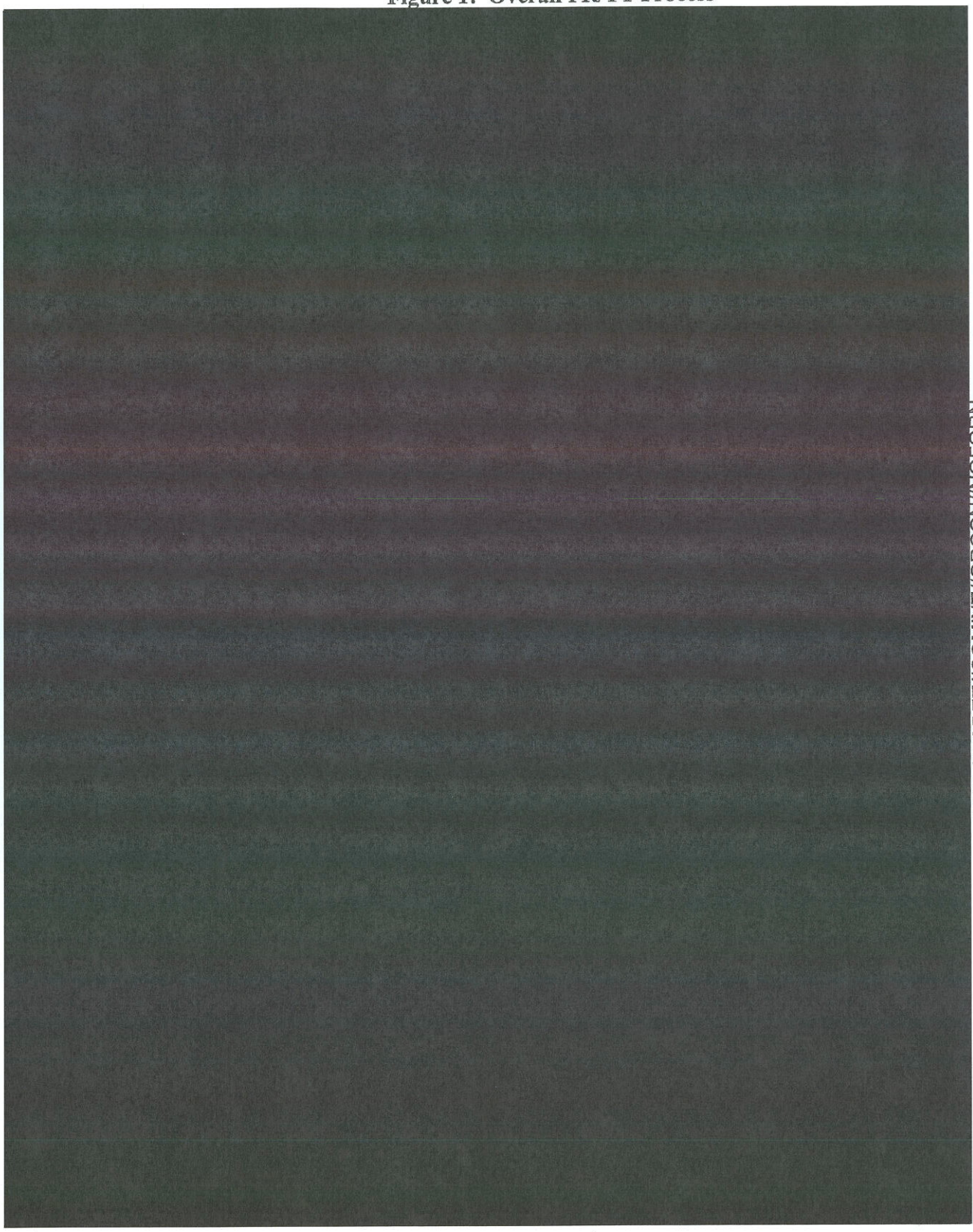
(U//~~FOUO~~) Enhanced auditing will provide a means to track a data user's activity patterns, the state of a user's operations, and the frequency and composition of queries. A formal metrics and monitoring system will also be used to monitor the status of the end-to-end processing and will alert management and operations personnel when processing anomalies are detected.

VI. (U) Conclusion

(~~TS//SI//NF~~) As discussed above, NSA has reviewed the technological systems, analytic workflows and processes associated with its implementation of the PR/TT Court Order, and has introduced corrective measures to address specific concerns and vulnerabilities. These new measures will ensure a balanced focus on technological solutions and management controls. The end-to-end review also revealed areas for improvement which have been documented and will continue to be addressed. Where changes were made impacting current manual operations, a combination of system evaluations, demonstrations and audits provided confidence that the technical fixes are actually configured and operating as intended.

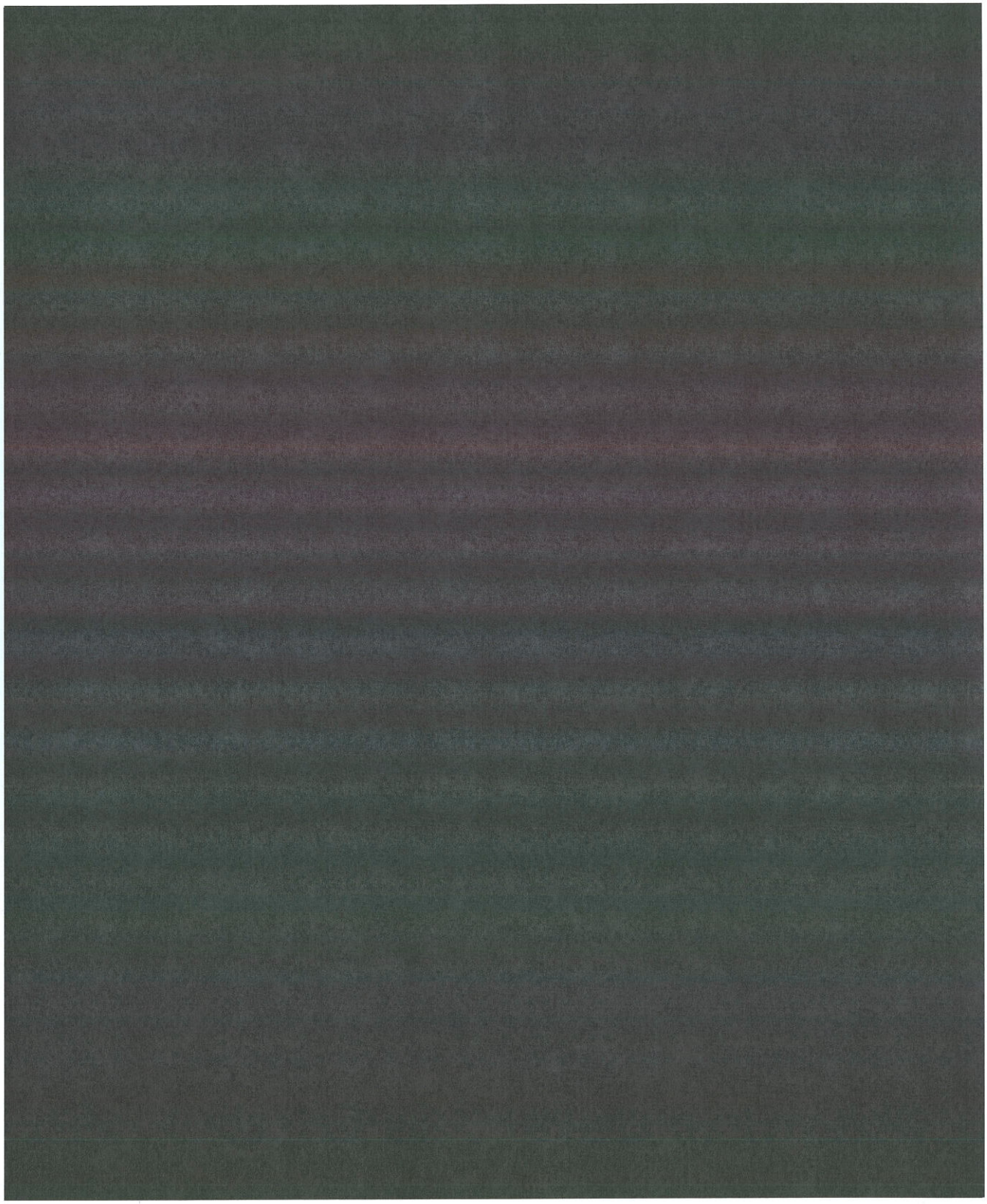
(~~TS//SI//NF~~) The remedial actions described in this report are subject to ongoing improvement and will support strict adherence to the Court Order. Although no corrective measure is infallible, NSA has taken significant steps designed to eliminate the possibility of any future compliance issues and to ensure that mechanisms are in place to detect and respond quickly if any were to occur.

Figure 1: Overall PR/TT Process



TOP SECRET//COMINT//ORCON//NOFORN

Figure 2: Components of PR/TT Process addressed in End-to-End Review



DOJ CONGRESSIONAL PRODUCTION JANUARY 2010 91

Figure 3: Component of PR/TT Process addressed in End-to-End Review

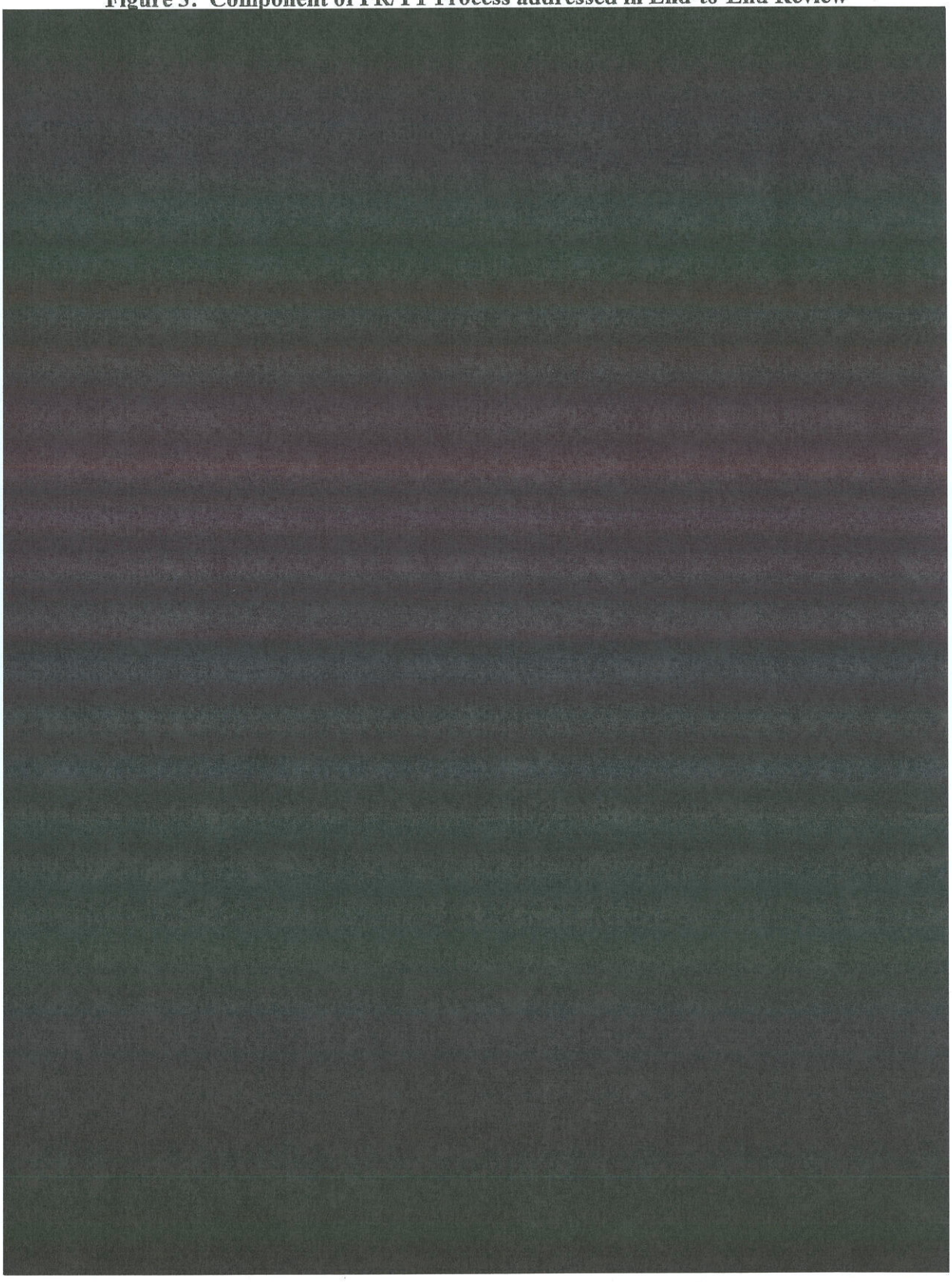


Figure 4: Component of PR/TT Process addressed in End-to-End Review

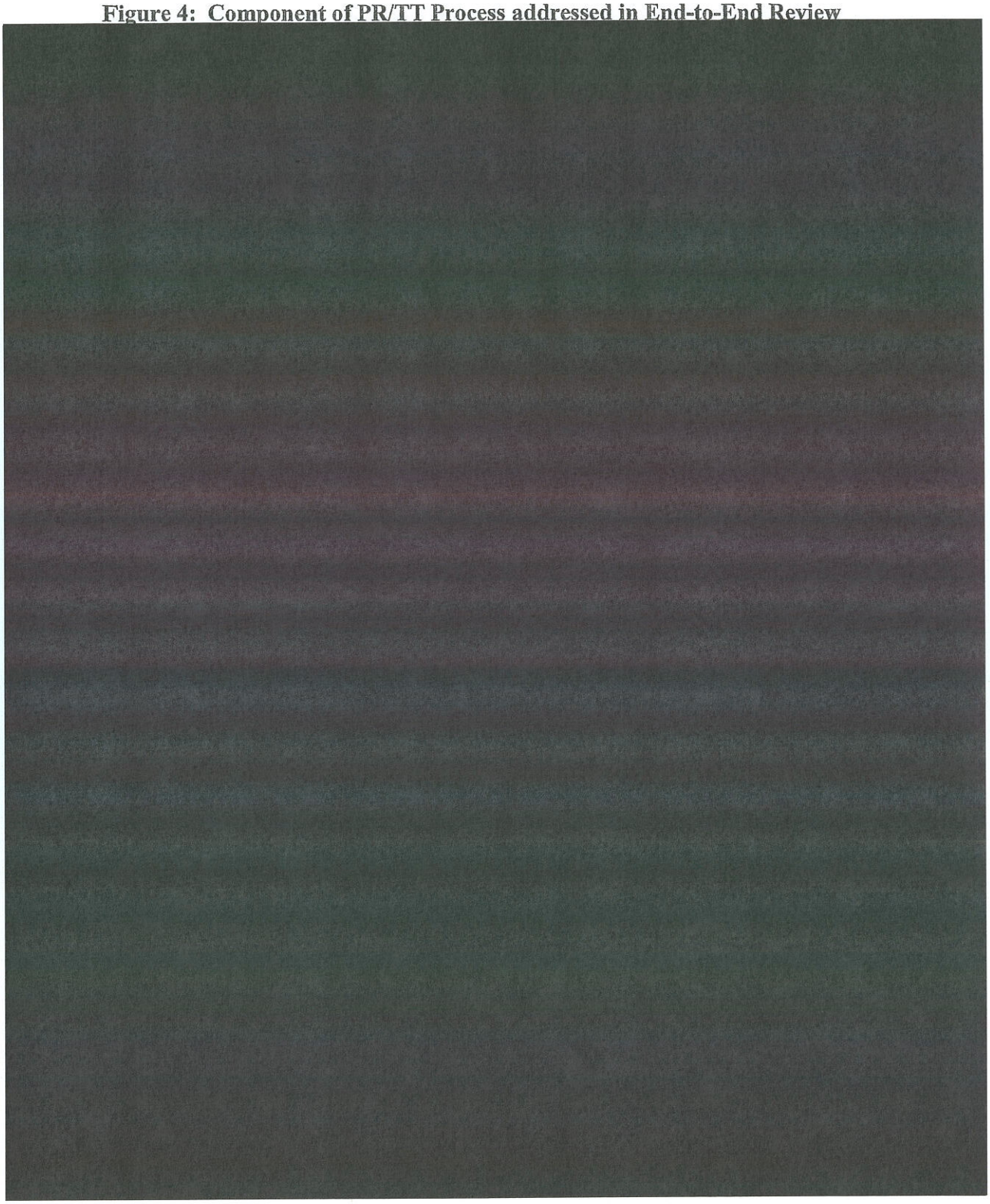
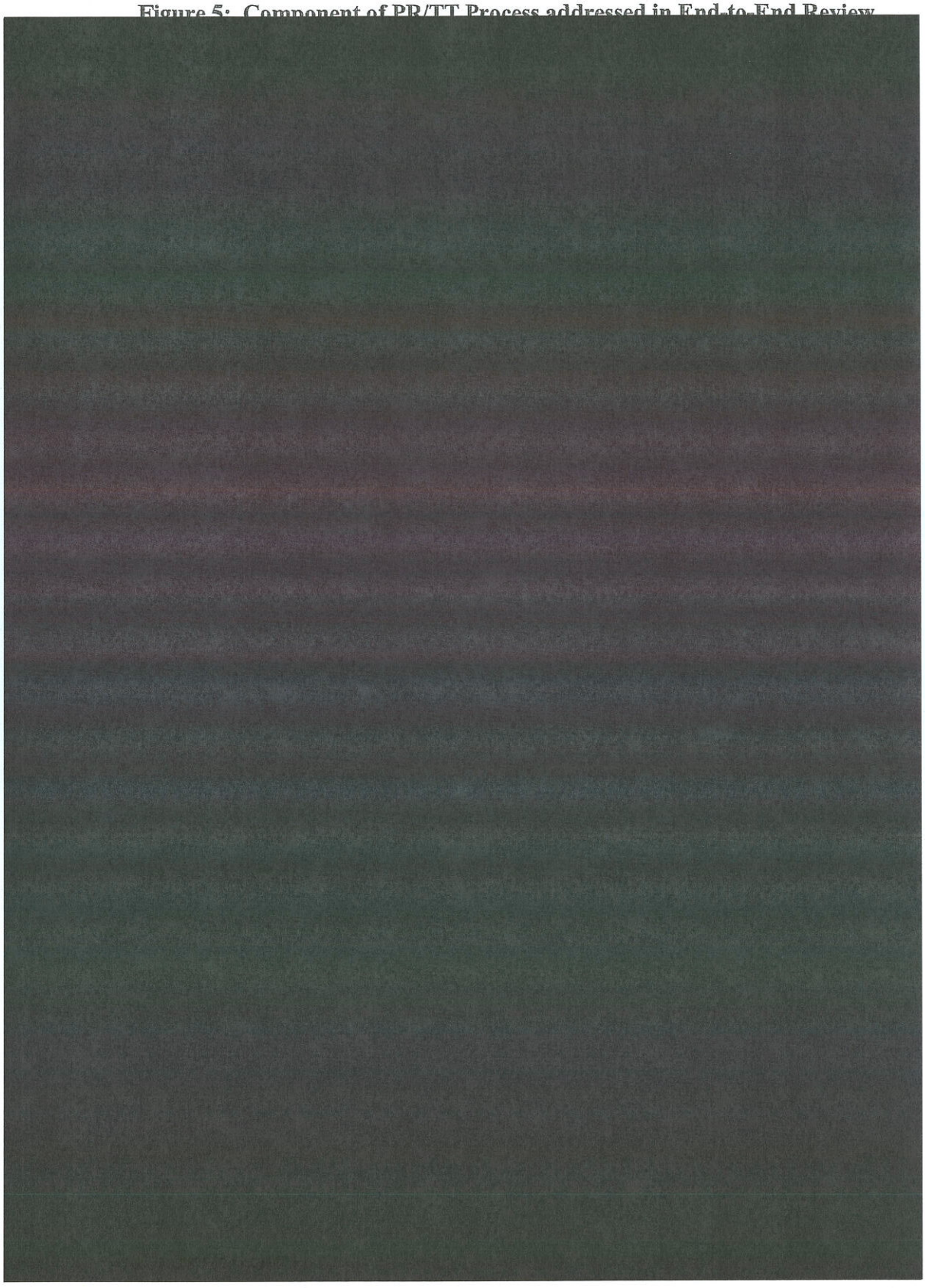


Figure 5: Component of PR/TT Process addressed in End-to-End Review



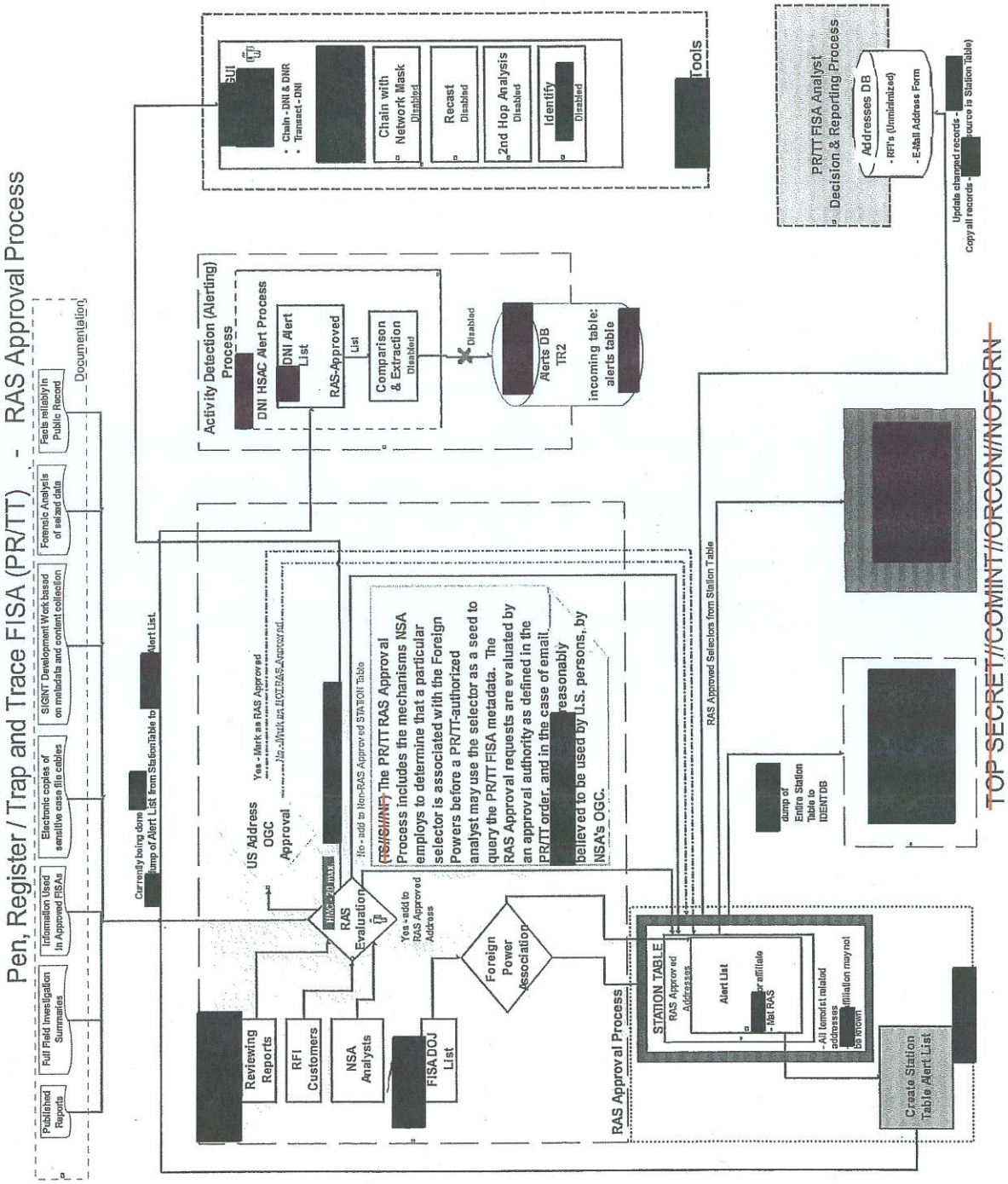
~~TOP SECRET//COMINT//ORCON//NOFORN~~

DOJ CONGRESSIONAL PRODUCTION JANUARY 2010 93

Figure 6: Component of PR/TT Process addressed in End-to-End Review



Figure 7: Component of PR/TT Process addressed in End-to-End Review
"RAS Approval Process"



DOJ CONGRESSIONAL PRODUCTION JANUARY 2010 96

Figure 8: Component of PR/TT Process addressed in End-to-End Review "Activity Detection (Alerting) Process"

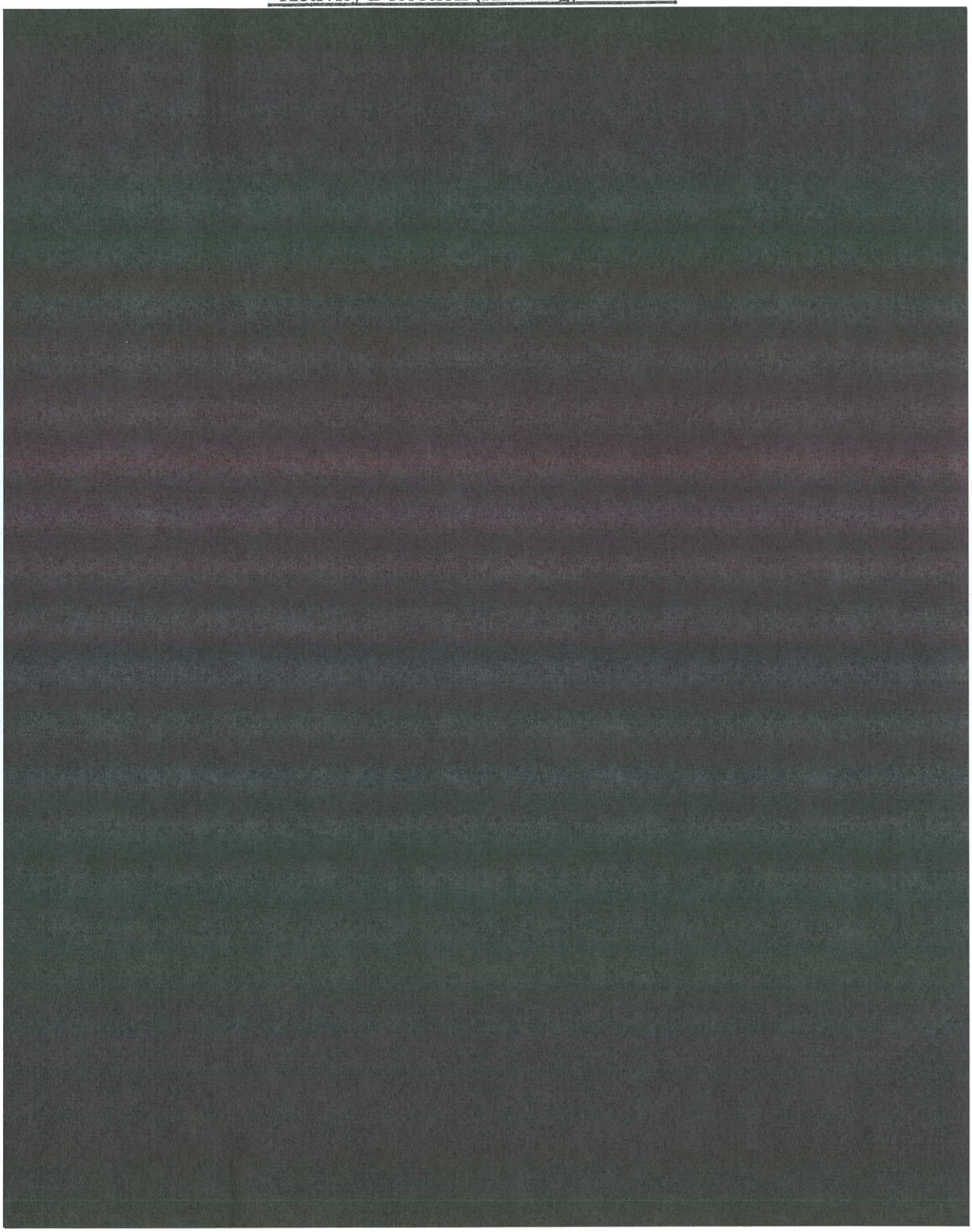
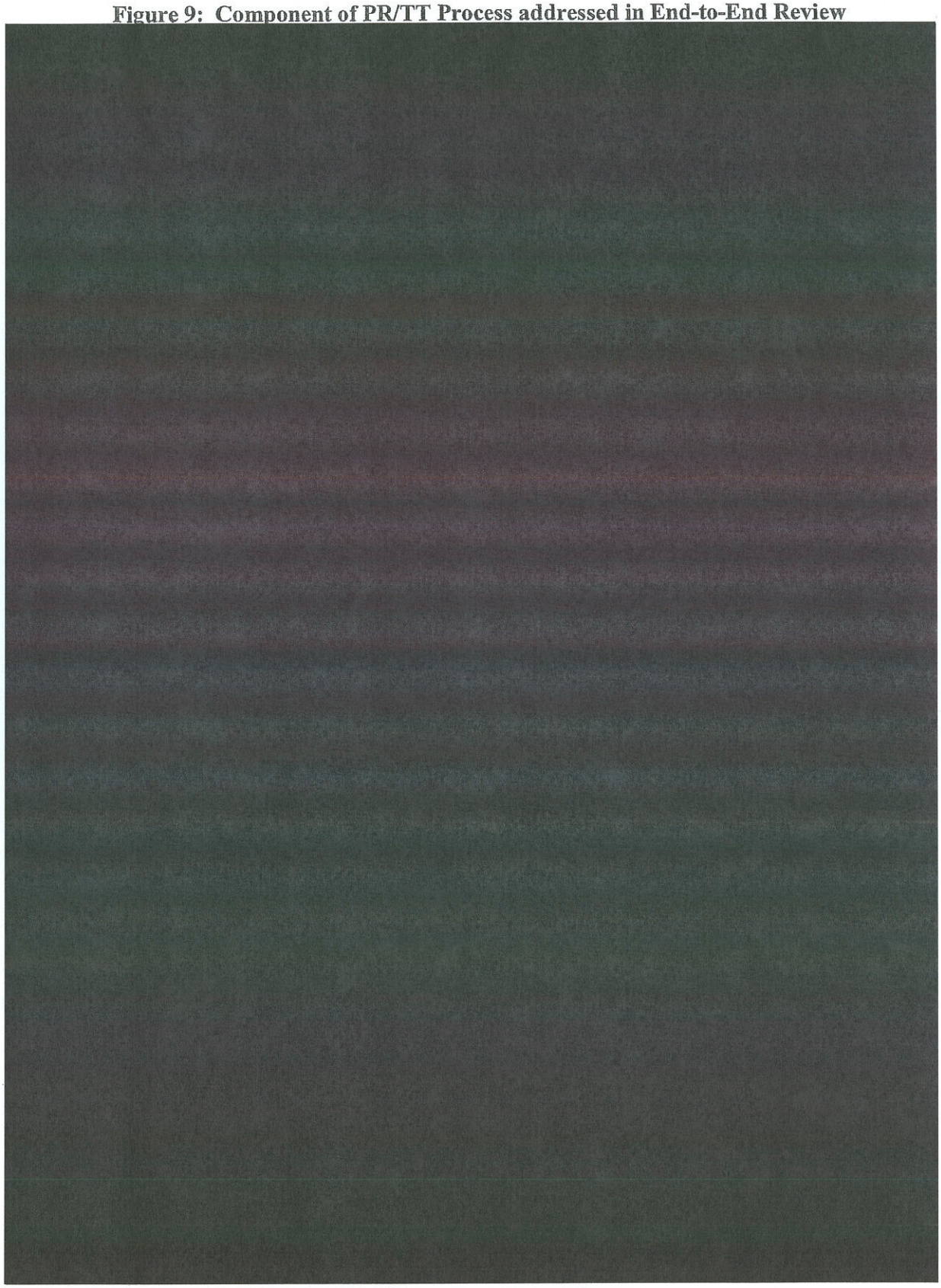
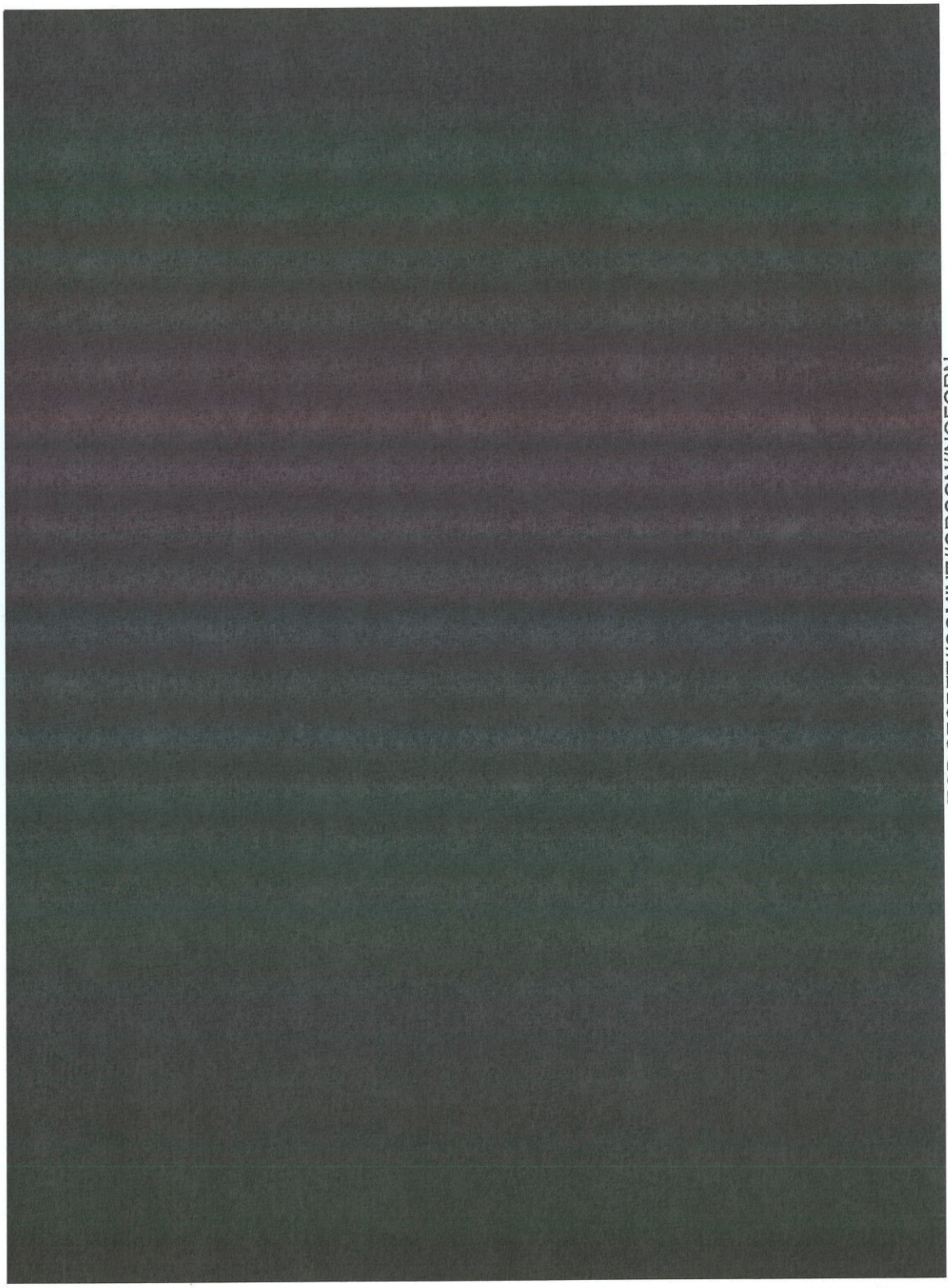


Figure 9: Component of PR/TT Process addressed in End-to-End Review



DOJ CONGRESSIONAL PRODUCTION JANUARY 2010 97

Figure 10: Component of PR/TT Process addressed in End-to-End Review
"PR/TT FISA Analyst Decision and Reporting Process"



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

Appendix: Glossary of Terms

Activity Detection List (also called Email Activity Detection List)	A list of high-priority foreign and domestic RAS-approved terrorist-associated [redacted] selectors, which were compared to incoming PR/TT FISA metadata in order to identify possible Foreign Powers-related communications in the U.S. The Activity Detection List is separate from the Station Table and is a subset of the RAS-approved selectors on the Station Table. Formerly called the Alert List, this list is now more commonly referred to as the Activity Detection List in order to be more descriptive.
Alert List	*See Activity Detection List*
Activity Detection Process	Now-disabled, a process by which NSA could determine when certain high-priority terrorist-associated email accounts [redacted] Formerly called the Alert Process, this is now more commonly referred to as the Activity Detection Process in order to be more descriptive.
Alert Process	*See Activity Detection Process*
Contact Chain Summary	A summary of communications between two selectors. A contact chain summary will, among other things, show that Selector A communicated with Selector B, [redacted]
Components	The core systems and processes identified as part of the PR/TT metadata workflow which were reviewed for compliance with the relevant requirements extracted from the Court documents.
Configuration Management	The process of tracking, controlling and documenting changes in software applications, including revision control and establishing baselines.
Defeat List	A list of selectors that are deemed of little

	analytic value for metadata analysis, used to block and purge unwanted metadata.
Dialed Number Recognition (DNR)	Dialed Number Recognition (DNR) is used to refer to information derived from the telephone network.
Digital Network Intelligence (DNI)	Digital Network Intelligence (DNI) is used to refer to information derived from both the Public Internet as well as private digital networks.
DNI	*See Digital Network Intelligence*
DNR	*See Dialed Number Recognition*
EAR	*See Emphatic Access Restriction*
Emphatic Access Restriction (EAR)	A software restrictive measure written into the [redacted] middleware on [redacted] to prevent a non-RAS approved selector from being used as a seed to chain query the PR/TT metadata.
[redacted]	NSA's corporate file forwarding service which provides for distribution of the PR/TT metadata from the collection source to the analytic repositories. [redacted] accepts files from sources and transports those files to the end destinations identified in the filename assigned.
[redacted]	NSA's corporate contact chaining system which accepts metadata from multiple sources. It accepts the PR/TT FISA metadata files from [redacted]; stores the metadata in a separate partition; performs data quality, preparation and sorting functions; and then summarizes contacts represented in the processed data. [redacted] stores the resulting contact chains and transaction records and provides the authorized analysts with access to these contact chains and subsequent transactions.
[redacted]	[redacted]
[redacted]	A database analytic system and user interface tool for integrated analysis of multiple types of metadata, facilitating more comprehensive target activity tracking.
[redacted]	[redacted]
Metadata	"Data about the data"; for example, information about an email, to include the

	sending and receiving address. [redacted] Metadata does not include content.
[redacted]	A corporate repository for DNI metadata which processes and forwards query results derived from RAS-approved PR/TT metadata to [redacted]
PKI	*See Public Key Infrastructure*
PR/TT FISA Analysis Decision and Reporting	A process that encompasses target knowledge, analytic procedures and legal and policy guidance. This overall process helps analysts determine which information meets customer requirements, assists them in prioritizing those requirements, and informs their report drafting and dissemination decisions.
PR/TT FISA Analytic Tools and Processes	Homeland Security analysts from NSA's Office of Counterterrorism used a variety of tools to help them identify and evaluate terrorist communications or activities associated with the U.S. homeland. These tools can be characterized in three categories: tools that helped analysts view and manage activity detection (alerting), tools that helped PR/TT-authorized analysts' chain email communications from RAS-approved seeds, and tools that [redacted]
Public Key Infrastructure (PKI)	An information assurance service that supports digital signatures and other public-key based security mechanisms, and offers security measures such as identification and authentication, access control and audit capability.
Query Result	A query result includes information provided orally or in writing, and could include a tip or a lead, a written or electronic depiction of a chain [redacted], a compilation or summary of direct or indirect contacts of a RAS-approved seed, a draft or finished report, or any other information that would be returned following a properly predicated PR/TT query.
RAS Approval Process	The mechanisms NSA employs to determine that a particular selector is associated with the

	Foreign Powers before a PR/TT-authorized analyst may use the selector as a seed to query the PR/TT metadata. RAS Approval requests are evaluated by a designated approval authority as defined in the PR/TT Order, and in the case of email [redacted] reasonably believed to be used by U.S. persons, by NSA's Office of General Counsel (OGC).
Requirements	An action, activity, capability or restriction that is specified or derived from the governing PR/TT metadata documents that NSA, DoJ or others must satisfy.
Seed	An initial selector used to generate a chain query.
Selector	An identifier used in [redacted] such as an email address [redacted]
SOP	*See Standard Operating Procedure*
[redacted]	[redacted]
SSP	*See System Security Plan*
Standard Operating Procedure (SOP)	Institutionalized documentation describing official processes and procedures.
Station Table	Historic reference of all DNI selectors that have been assessed for RAS – and their associated RAS determination (RAS-Approved or Non-RAS-Approved) - since the PR/TT Order was first signed on July 14, 2004.
System Security Plan (SSP)	Formal document describing the implemented protection measures for the secure operation of a computer system.