

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](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.

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



U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT
U.S. Department of Justice
National Security Division

PM 2:18

CLERK OF COURT

Washington, D.C. 20530

Honorable John D. Bates
Presiding Judge
United States Foreign Intelligence Surveillance Court
Washington, D.C.

Dear Judge Bates:

I am pleased to enclose written answers to the questions that you sent me in your letter of [REDACTED] concerning bulk collection of metadata through pen register/trap and trace (PR/TT) devices authorized under the Foreign Intelligence Surveillance Act. The Government is prepared to discuss our responses with you and your staff at the Court's convenience.

Let me once again thank both you and those members of your staff for your consideration of the Government's proposal to re-initiate the National Security Agency's PR/TT metadata collection and analysis program. Should the Court have any additional questions, comments or concerns, please do not hesitate to contact me. Thank you.

Sincerely,

David S. Kris
Assistant Attorney General

Enclosures

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

~~TOP SECRET//COMINT//NOFORN//20320108~~



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

MEMORANDUM FOR ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY
DIVISION, DEPARTMENT OF JUSTICE

SUBJECT: (U//~~FOUO~~) Response to Questions Posed by Foreign Intelligence Surveillance
Court (FISC) in [REDACTED] Letter - INFORMATION
MEMORANDUM

(U//~~FOUO~~) I am happy to provide on behalf of the National Security Agency (NSA) the enclosed information in response to the questions the Foreign Intelligence Surveillance Court (FISC) posed in its [REDACTED] letter to you. As you know, intelligence officers and attorneys at NSA worked with you and members of your staff as well as personnel at the Office of the Director of National Intelligence to carefully and comprehensively review the Court's questions and provide these responses. I very much appreciate the spirit of cooperation shown by all involved in the effort.

(U//~~FOUO~~) We would be happy to answer any additional questions the Court may have and to meet with the Court as necessary. If you have any questions in connection with this correspondence, please contact [REDACTED]

[REDACTED] Many thanks.

Sincerely,

KENTH B. ALEXANDER
Lieutenant General, U.S. Army
Director, NSA/Chief, CSS

Encl:
a/s

THIS DOCUMENT MAY BE DOWNGRADED TO UNCLASSIFIED//FOR OFFICIAL
USE ONLY UPON REMOVAL OF ENCLOSURES.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: [REDACTED]

~~TOP SECRET//COMINT//NOFORN//20320108~~

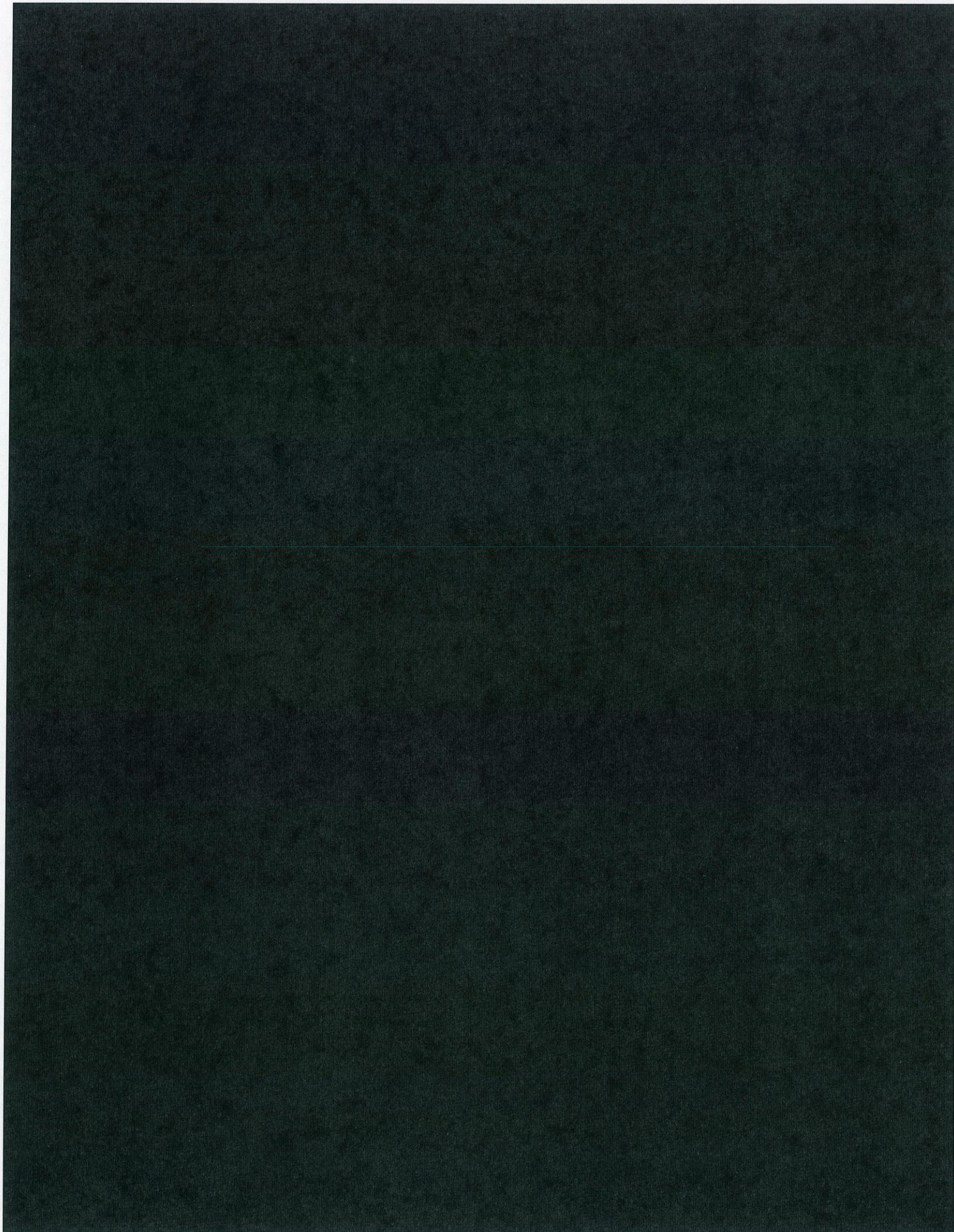
~~TOP SECRET//COMINT//NOFORN~~

NSA Response to FISA Court Questions

Regarding Re-Initiation of Bulk PR/TT Collection



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

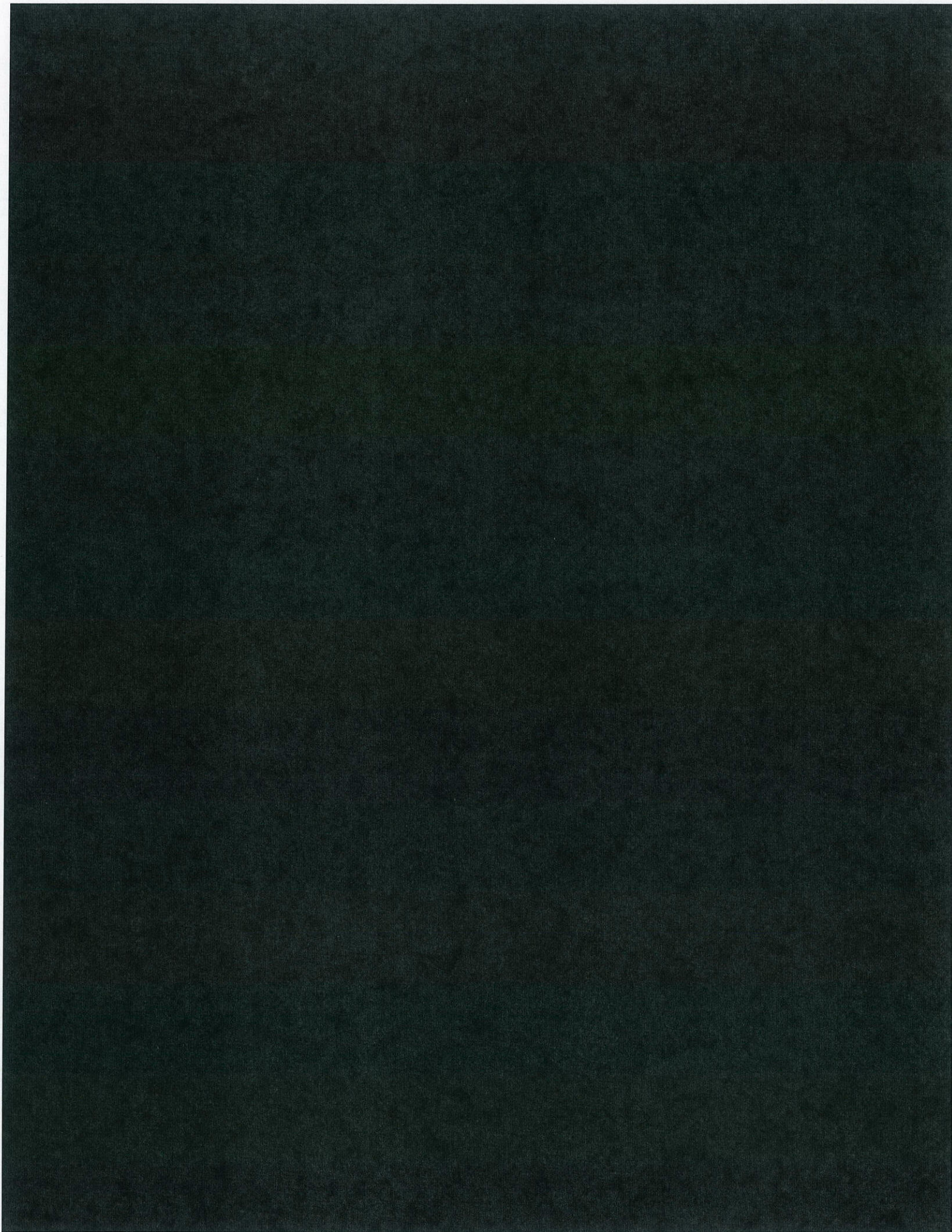














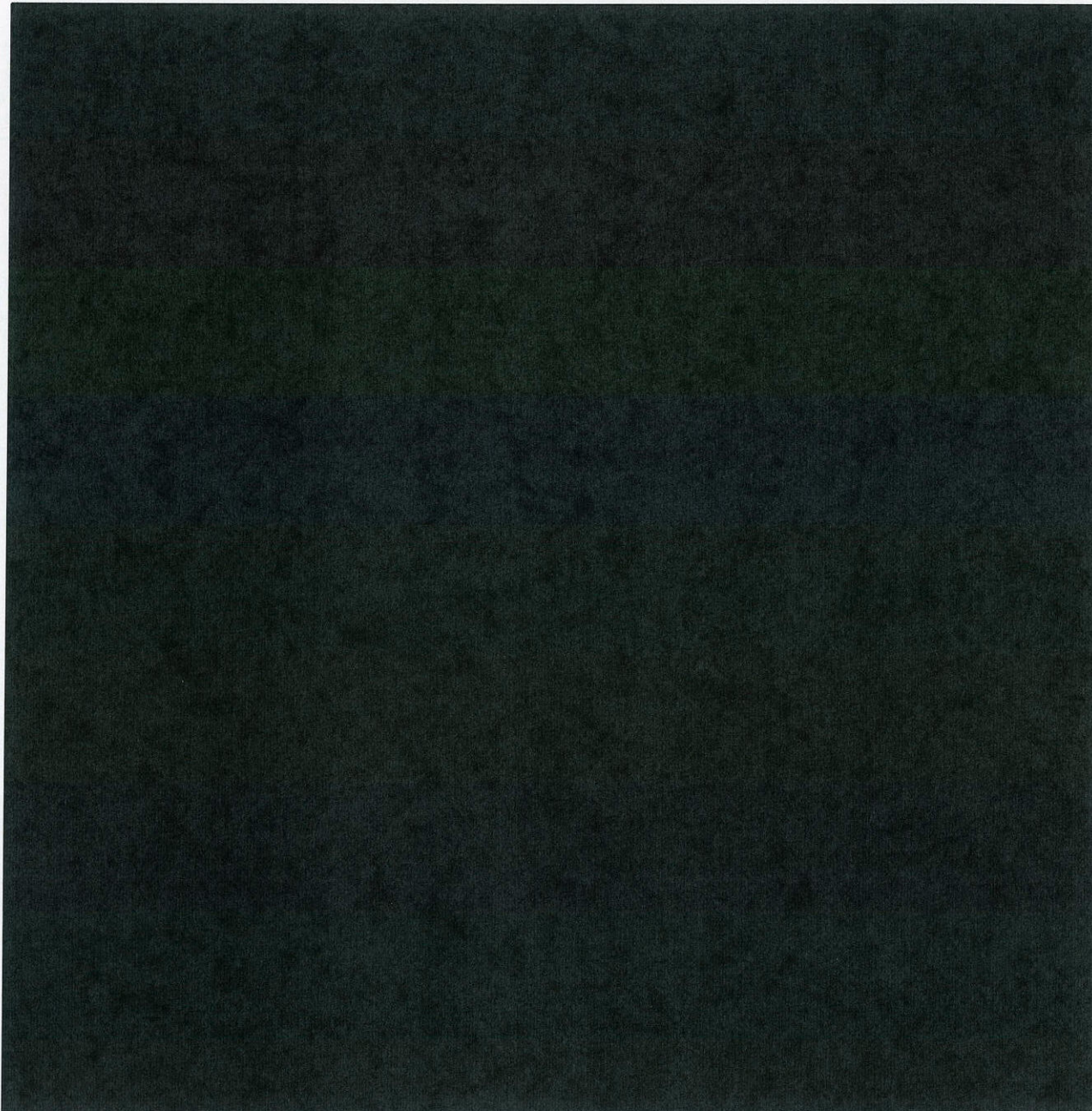












IV. Storage, Access, Query

A. Previous applications stated

How does NSA propose to store data now?

Please describe the technical protections against improper use, disclosure, or dissemination of this data.

NSA: ~~(TS//SI//NF)~~ NSA intends to store and process the collected metadata in repositories within secure networks under NSA's control. The metadata will carry unique markings, or "tags," such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to the authority. These tags are applied to the metadata during the metadata ~~processing~~ processing stages, and remain attached to the metadata as it is stored in the metadata repository.

~~(TS//SI//NF)~~ The pre-query metadata residing in NSA's PR/TT repositories is highly sensitive metadata pertaining to ~~Internet~~ of Internet communications, a substantial portion of which will be communications of United States persons located in the United States who are not the subject of any FBI investigation. This makes this data set unique and extraordinary, and forms the basis for the special access and handling controls NSA will apply.

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

Nonetheless, query results may still include unminimized United States person information; for this reason, query results must be handled and disseminated in accordance with NSA's legal compliance and minimization procedures (USSID SP0018).

~~(TS//SI//NF)~~ PR/TT query results will be handled and protected according to USSID-18 guidelines. In addition, the PR/TT provenance of the query results will be preserved as the information passes from one system or process to another consistent with NSA product sourcing requirements. In particular, NSA policy states that sourcing information is necessary for the preparation of intelligence reports (all of which must include references to the sources of the information contained therein), and for later tracking of any disseminated information. If information derived from PR/TT metadata is included in a dissemination, PR/TT would be reflected in the source record for that product.

⁶ ~~(TS//SI//NF)~~ Query results could include information provided orally or in writing, and could include a tip or a lead (e.g., "A query on RAS-approved Identifier A revealed a direct contact with Identifier Z"), a written or electronic depiction of a chair ~~or~~ 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)

B. What is the reason for granting an unlimited number of analysts access to the data? Is it because of increased collection?

NSA: ~~(TS//SI//NF)~~ Under previous Court Orders, NSA safeguarded against queries using non-RAS-approved seeds by limiting the number of analysts with authority to query the metadata and providing those analysts with special training to emphasize the importance of the proper use of RAS-approved seeds. NSA monitored the effectiveness of these safeguards, by logging all analytic queries for auditing purposes.

~~(TS//SI//NF)~~ In [REDACTED] NSA implemented technical controls which block any analytic query of the metadata with a non-RAS-approved seed. Accordingly, NSA has not proposed to limit the number of analysts with query authority under its application. However, as also described below in the response to question V.A., NSA will exercise internal management controls to identify analysts who may make such queries. In addition, the logging of analytic queries will continue to serve as a compliance measure. NSA is also seeking explicit authority to share query results, as needed, throughout NSA's analytic enterprise. (This topic is discussed more fully in the response to question V.A., below.)

C. Is "contact chaining" the only form of querying used to access the raw data? Please describe the data which is presented to the analyst in contact chaining.

NSA: ~~(TS//SI//NF)~~ Yes – contact chaining is the sole means of querying by which intelligence analysts access the raw data. The starting point for such queries is a RAS-approved identifier submitted by an authorized analyst. The result of a query consists of a logically organized presentation of the authorized metadata contained in the PR/TT repository associated with a RAS-approved identifier and the metadata that occurred within up to two hops from the seed.

D. What is an "auditable record" of accesses? What specifically will the record contain? Does this apply only to use of the analytic tools, or to any access of the data?

NSA: ~~(TS//SI//NF)~~ An auditable record is created each time the PR/TT metadata is queried using an intelligence analysis (IA) query tool. Analyst utilization of an IA query tool is most typical, but technical support personnel may also utilize an IA query tool in support of their activities; auditable records are created in either case. Currently the auditable record captures the date/time of the query, the analyst SID ("Standard ID", a unique identifier for each NSA employee), the identifier that was used to query the metadata, and the IP address of the machine used to perform the query.

~~(TS//SI//NF)~~ Technical access to the systems that support the processing, transport, and storage of PR/TT metadata is logged consistent with the standards required by the System Security Plans associated with those systems. While the exact format of the logged records varies according to the specific system, a majority of the technical log records contain: (a) the user performing the action, (b) information about the location of the user, and (c) a date/time stamp.

E. What are the reasons for the different expiration dates proposed for RAS determinations? If FISC orders are used as one basis, why not 90 days for USPs?

NSA: ~~(TS//SI//NF)~~ The proposed dates (180 days for identifiers believed to be associated with a U.S. person, 365 days for other identifiers) are identical to those approved by the Court beginning in September 2009 (docket number BR 09-13) for Business Records (BR) FISA. In the reality of mission operations, in which analysts work on a day-to-day basis with the query results from approved identifiers, it is typical to revisit and reaffirm RAS determinations more frequently than the Court requires. As new information becomes available for a particular RAS identifier it is promptly assessed. This assessment may result in a decision to revalidate or invalidate the identifier. NSA seeks to maintain consistency in the expiration dates used by the two authorities in order to reduce possible confusion and support the adoption of standard analytic procedures.

F. What are the qualifications and training of the 20+ people making RAS determinations? Is there formal training and/or guidance on application of the standard?

NSA: ~~(TS//SI//NF)~~ Currently there are 15 individuals at NSA (of the 23 approved in the Orders) who make RAS determinations under the BR and PR/TT authorities: All of

these individuals have been trained about and understand the requirements for RAS and the need for additional OGC review of U.S. person identifier nominations.

~~(TS//SI//NF)~~ In March 2009, NSA established a process for certifying individuals to make RAS determinations. This process consisted of two mandatory steps: a period of on-the-job training provided by already-qualified individuals, and an oral test of knowledge of the applicable requirements jointly administered by SID Oversight & Compliance and the NSA's Education and Training organization. All 15 of the individuals who currently make RAS determinations took and passed the test between March and May 2009. The certification process was designed originally for use within the BR authority; it is currently undergoing review and revision so that it explicitly applies to both the PR/TT and BR authorities.

~~(TS//SI//NF)~~ NSA carefully selects the analysts to be trained to make RAS determinations. While there is no cast-iron set of qualifications for this responsibility, all of the 15 people who make RAS determinations possess substantial experience both as intelligence analysts and, specifically, as intelligence analysts working the CT target set. Currently the group has an average of 8-10 years of experience. In addition to possessing deep experience, these individuals usually carry additional functional responsibilities as team leaders or senior analysts.

~~(TS//SI//NF)~~ Training and guidance on the RAS standard, its application, and the evidence that is required to meet it, is routinely provided to analysts who work with PR/TT and BR metadata. Senior intelligence analysts and NSA's OGC provide this training as needed.

G. With regard to information previously collected, can you provide a sense of the proportion of information authorized for collection relative to information that was outside the scope of authorized collection?

NSA: ~~(TS//SI//NF)~~ Virtually every PR/TT record contains some metadata that was authorized for collection, and some metadata that was not authorized for collection (e.g.,

Without a detailed technical analysis of the repository holdings, it would be very difficult to determine how much of the collected data was authorized as opposed to unauthorized, but, as stated earlier, virtually every PR/TT record contains some data that was authorized by prior orders, and some that was not.





V. Dissemination and Retention

A. What is the reason for unlimited internal sharing of query results? Will those to whom dissemination is made receive training?

NSA: ~~(TS//SI//NF)~~ Internal sharing of query results will not be unlimited; such sharing will be strictly limited to a distinct population within NSA- those individuals who are fully indoctrinated for USSID-18 and who are also engaged in the analysis and reporting of counterterrorism and other relevant foreign intelligence targets- a process directed and controlled by NSA leadership. No additional PR/TT-metadata-specific training will be required for internal sharing of query results.

~~(TS//SI//NF)~~ The Government believes that USSID-18-based dissemination processes provide well-tested and consistent procedures for analytic sharing of query results, and that they appropriately balance the Government's need for foreign intelligence information while protecting the privacy interests of persons under the Fourth Amendment. They afford the highest protections where the privacy interests of U.S. Persons are involved, whether at the point of collection, use, or dissemination.

~~(TS//SI//NF)~~ Results of queries of PR/TT-sourced metadata are inherently germane to the analysis of counterterrorism-related foreign intelligence targets. This is because of NSA's adherence to the RAS standard as a prerequisite for querying PR/TT metadata. In order for an Internet communications address to be approved as a "seed" with which to query the collected metadata, facts must be produced that give rise to a reasonable, articulable suspicion that it is associated with a designated terrorist-related Foreign Power (associated with [REDACTED])

~~(TS//SI)~~ The authority to share the results of PR/TT queries throughout the USSID-18-indoctrinated intelligence analyst population is critical to the success of the NSA's counterterrorism mission. NSA's collective expertise in the Foreign Powers resides in [REDACTED] intelligence analysts, who sit not only in the NSA's Counterterrorism Analytic Enterprise, but also in other NSA organizations or product lines.

~~(TS//SI)~~ The Counterterrorism Analytic Enterprise, a mission element which comprises approximately [REDACTED] language analysts, intelligence analysts, and target developers, is the intelligence analysis core of NSA's counterterrorism effort. The vast majority of these analysts focus their efforts on specific terrorist organizations and threats, e.g., [REDACTED]. The ability to share the results of authorized PR/TT queries across this workforce compliantly and in accordance with USSID-18 guidelines will maximize the likelihood

that the metadata will contribute to intelligence outcomes against the enterprise's challenging target set.

~~(TS//SI)~~ In addition, NSA seeks to expand the sharing of PR/TT query results beyond the Counterterrorism Analytic Enterprise. The overarching purpose for doing so is to produce better counterterrorism intelligence as a consequence of putting PR/TT-sourced terrorism-related query results into the hands of analysts with knowledge and expertise in other topics or targets relevant to counterterrorism. For example, in the International Security Issues product line, intelligence analysts pursue foreign intelligence information on [REDACTED] including [REDACTED]

[REDACTED] The mission of the Combating Proliferation product line includes identifying connections between proliferators of weapons of mass destruction and terrorists, including those terrorists associated with the Foreign Powers. The International Crime and Narcotics product line has the responsibility to identify connections between terrorism and human smuggling or other forms of international crime. [REDACTED]

[REDACTED] Each of the NSA's ten product lines has some role in protecting the homeland from terrorists, including the Foreign Powers. Because so many analysts work to address terrorism-related analysis and reporting requirements from myriad different angles, it is impossible to estimate how many of these individuals might be served by the ability to integrate the metadata resulting from PR/TT queries into their analysis.

~~(TS//SI)~~ In addition to requesting authority to expand the sharing of PR/TT query results for the reasons described above, NSA also seeks to increase the number of analysts eligible to query the raw PR/TT metadata repository using RAS-approved identifiers. NSA will continue to employ the established, affirmative management controls and reviews currently in place to vet RAS nominations for their relevance to counterterrorism-related foreign intelligence targets. In addition, NSA will exercise internal controls to identify analysts who may query the raw PR/TT metadata using RAS-approved identifiers, and such individuals will receive appropriate training. NSA will also apply relevant policies and procedures governing access to raw SIGINT databases to the PR/TT queries. Technological safeguards and controls, such as vetted user interfaces, the EAR, and auditing tools, will continue to restrict and log access to the raw PR/TT metadata to authorized queries made by authorized intelligence analysts.

B. Will marking of this data attach to all disseminations, particularly if it is stored [REDACTED] and if the information is re-disseminated?

NSA: ~~(TS//SI//NF)~~ It may be helpful to describe data marking in terms of three sequential, but distinct, processing stages that PR/TT metadata may undergo as it is transformed from raw collection to published intelligence:

- **Stage 1** - raw, unselected collection;
- **Stage 2** - query results based on a RAS-approved identifier, the sharing and analysis of those results among and by NSA intelligence analysts and analytic tools, and the storage of this information in NSA databases; and
- **Stage 3** - intelligence disseminated to Intelligence Community customers via NSA's reporting mechanisms.

~~(TS//SI//NF)~~ In Stage 1, [REDACTED]

[REDACTED] This tag is the basis for applying the technical and management controls to the data necessary to ensure compliance with the Court's orders.

~~(TS//SI//NF)~~ In Stage 2, metadata selected by RAS queries, and subsequently shared, analyzed, and stored at NSA, will be handled and protected according to USSID-18 guidelines. The tagging information used in Stage 1 will still be retained with the initial query results, but it will no longer need to be used as a basis for invoking the technical and management controls associated with and required for raw PR/TT metadata.

~~(TS//SI//NF)~~ In Stage 3, PR/TT query results, and any analytic results arising from it, will be properly minimized prior to their inclusion and dissemination via an appropriate reporting vehicle. Per NSA policy, analysts are required to complete a sourcing record for every dissemination. Sourcing records list the collection sources (including PR/TT metadata) of the information contained in the dissemination. NSA does not include source information, or the sourcing record, in the actual disseminations outside of NSA. However, source information is retrievable by NSA if required.

C. Post-query and pre-dissemination, what safeguards are in place to ensure that the query and its results were in compliance with the RAS determination and any other query restrictions?

NSA: ~~(TS//SI//NF)~~ Since the Emphatic Access Restriction (EAR) was put into place [REDACTED], SID Oversight & Compliance [REDACTED] has conducted a complete (100 percent) audit of all PR/TT metadata queries, and this audit has confirmed that there has been no inappropriate access to the sensitive PR/TT metadata via intelligence analysis tools. Compliance audits have determined that the EAR has prevented all queries on non-RAS approved identifiers from accessing the metadata. NSA intends to continue with full auditing capability of all queries using intelligence analysis query tools.

D. What is the govt.'s current thinking on dissemination requirements: only USSID-18, or some case-specific requirements also? When do you expect to have a final proposal on this issue?

NSA: ~~(TS//SI//NF)~~ NSA seeks to implement the standard USSID-18 guidelines for the handling, internal NSA analytic sharing, and external dissemination of metadata information obtained or derived from PR/TT accesses. The Government expects to provide a proposal to the Court by no later than [REDACTED]. The Government would welcome the opportunity to discuss the factual and legal issues regarding implementation of the proposal.

E. Will there be, and what is the feasibility for, auditable records on dissemination and re-dissemination?

NSA: ~~(S//SI//REL)~~ NSA maintains written records of intelligence reports and other information disseminated to its intelligence customers; it is through review of these records that NSA has been able to provide the Court with its weekly dissemination reports. Included among these records are records of the releases of United States person identifying information and the facts that supported those release decisions. In this respect, NSA already has auditable records on disseminated information, although not all auditing capabilities are automated.

~~(S//SI//REL)~~ Recipients of NSA's intelligence reports or information are provided guidance on any requirements or restrictions on follow-on use or handling of the information, by means of the caveats included with the information. Although these caveats help to ensure that recipients are compliant with any such requirements or restrictions, NSA can monitor compliance with these caveats only through the cooperative efforts of all of the other Intelligence Community agencies.

F. Why is the retention time changed to 60 months (5 years), vs. 54 months?

NSA: ~~(S//SI//REL)~~ The PR/TT retention time was changed from 54 months to 60 months to develop and maintain consistency with the BR FISA Order. As described above in our response to Question 4 (E), NSA seeks to achieve consistency in the implementation of FISA procedures whenever possible.

VI. Reports, Training, Oversight

A. Why is the dissemination report requirement dropped?

NSA: ~~(TS//SI//NF)~~ NSA has provided the Court with the total number of disseminated intelligence reports containing PR/TT-derived information as part of its renewal applications. NSA intends to continue to provide the Court this number, and stands ready to provide the Court with additional information at any time.

~~(TS//SI//NF)~~ NSA excluded from the current application the weekly dissemination report that the Court had required since [REDACTED] because of other changes to the proposed collection, notably the proposed change to USSID-18 for internal sharing and dissemination. Prior PR/TT Orders imposed unique procedures and requirements for the dissemination of PR/TT-derived information outside of NSA. For example, to release United States person identifying information derived from E.O. 12333 metadata in a report, NSA's Chief of Information Sharing Services (or one of a few other specified NSA leaders) must determine that the identity is necessary to understand the foreign intelligence in the report. To release similar United States person identifying information derived from PR/TT metadata, a smaller subset of NSA leaders must determine that the identity is necessary to understand the counterterrorism information in the report. The weekly dissemination report served an important oversight function within this unique PR/TT dissemination framework; it was in this report that NSA confirmed that the appropriate findings had been made by the proper decision makers. The current application departs from this historic framework, and proposes to apply NSA's standard, USSID-18-defined dissemination procedures to PR/TT-derived information as these procedures form the very backbone for virtually all of NSA's dissemination practices. For this reason, NSA believes that a weekly dissemination report is no longer necessary.

B. It appears that the compliance meetings and NSA OGC spot checks have been modified from the previous order. Can you detail these changes and provide the bases for them?

NSA: ~~(TS//SI//NF)~~ NSA removed the pair of OGC spot checks from its current application because of the proposed changes to the nature of the collection. For example, prior PR/TT Orders authorized collection against [REDACTED] OGC's random spot checks ensured (among other things) that [REDACTED] Similarly, during spot checks OGC attorneys would review [REDACTED] Because the current application seeks authority for collection at facilities, [REDACTED] and no longer emphasizes [REDACTED] of the metadata, spot checks to confirm these characteristics are no longer necessary.

~~(S//SI//REL)~~ The elimination of the OGC spot checks should not be construed as abandonment of any periodic or aperiodic monitoring of the functioning of the collection. Many of these are written into the application. In terms of ensuring that only authorized categories or types of information are being collected, the application calls for a periodic meeting between NSA's OGC, Office of the Director of

Compliance (ODOC), and the National Security Division of the Department of Justice (NSD/DoJ) to review the metadata collected. Moreover, NSA's OGC and NSD/DoJ will continue to review a sample of justifications for RAS approvals for identifiers used to query the PR/TT metadata. Finally, NSA's OGC, as well as the ODOC and other oversight and compliance organizations, will continue to examine NSA's processes and practices to ensure compliance with the Court's orders. Nonetheless, NSA seeks to retain the discretion to implement any number of oversight mechanisms and to change those mechanisms over time in response to changing concerns.

C. Please describe in detail the oversight authorities that will be exercised.

NSA: ~~(TS//SI//NF)~~ With respect to oversight of the authorities in the proposed collection, NSA (including OGC, ODOC, and the Inspector General), DOJ, and ODNI will conduct oversight as outlined in the application. Among other oversight mechanisms, the application contemplates periodic meetings to assess compliance, including a review of the metadata collected to ensure that only those categories or types of information described in the application are being collected, and reviews of a sample of the justifications for RAS approvals for identifiers used to query the metadata.

~~(TS//SI//NF)~~ In addition to these oversight activities specific to the application, NSA is engaged in developing and implementing a comprehensive compliance program that is applicable to this collection as well as NSA's other collections.

1. ~~(U//FOUO)~~ Compliance and oversight are two parts of the same coin. Each is necessary to ensure that the Court-ordered activities remain lawful. Compliance is a management function designed to deliver (not oversee) well-planned, effective, and comprehensive compliance activities. Compliance starts with a set of rules (the Order), ensures a shared understanding among technical, operational, and legal personnel, and then puts in place managerial controls, awareness, training, monitoring, and technical safeguards to reach and maintain compliance. Oversight is an independent review focused on the quality and performance of the compliance program. Both are absolutely necessary, but one does not make up for the other.
2. ~~(U//FOUO)~~ The compliance and oversight efforts at NSA – and the oversight efforts at DOJ, ODNI, and DOD – go substantially beyond what is written in the DIRNSA's declaration or proposed Order. Effective compliance and oversight are not performed simply through meetings or spot checks. Compliance and oversight are continuous efforts that require continuous management within a structure that promotes a shared understanding of the applicable rules and the requirements necessary to implement such rules.
3. ~~(TS//SI//NF)~~ Accordingly, compliance and oversight activities and resources must be applied comprehensively across all NSA operations, systems, and people. The PR/TT program, like others at NSA, leverage multiple parts of the NSA community.
4. ~~(TS//SI//NF)~~ The Director of Compliance, in support of that continuous management approach, has instituted important structural and managerial improvements at NSA, in particular:
 - a. The appointment of an Associate Director for Special Compliance Activities to focus on compliance with the BR and PR/TT FISA Orders. In particular, this role ensures a continuous focus on a shared understanding among technical, operational, policy, and legal personnel in both the drafting and implementation of the Orders.

- b. The formation of a technology compliance office to ensure that system developers are properly trained, made aware of the requirements and restrictions in the Orders, and NSA prioritizes the actual implementation of important technical safeguards.
 - c. Clarifying, through written documentation and in-person discussions with NSA Senior Leaders, specific roles and responsibilities with respect to compliance efforts. Governance is one of the keys to a successful compliance program across NSA and one of the primary efforts to date has been clarifying those roles and responsibilities.
 - d. The use of documented verification procedures developed in conjunction with DOJ and ODNI to ensure that every statement in the NSA Declarations is appropriately checked for accuracy and completeness and, upon receipt of an Order, that every requirement is assigned a clear owner and that there is a shared understanding about each requirement. Furthermore, ODOC, working with others, monitors the implementations of these requirements using a risk-based methodology.
 - e. Initiated meetings between NSA's Director of Compliance and OGC, DOJ, and ODNI on a regular periodic basis (currently weekly) to discuss compliance and oversight matters.
 - f. With respect to the PR/TT program, the Office of the Director of Compliance will monitor the configuration governing the extraction of specific metadata fields to ensure robust compliance with the Order, recognizing this as a high-risk area for compliance issues.
 - g. Continued focus on training for the BR and PR/TT Orders. In the latter part of 2009, NSA finished its online course (which was previously delivered in-person) covering the BR-FISA program and was close to completion of the online PR/TT course (which is on hold pending a new Order). These courses allow NSA personnel to receive timely guidance in a consistent format to increase a shared understanding of the requirements and restrictions of these special FISA programs.
 - h. [REDACTED] NSA would continue to focus on the periodic review of a representative sample of RAS approved identifiers accompanied by the ability to audit all queries into the PR/TT metadata.
 - i. More generally, the formation of a Compliance Panel of the NSA Advisory Board, to provide external advice and guidance to the compliance activities at NSA. This Panel includes representatives from the legal profession, industry privacy officers, academia, and industry compliance offices.
5. (~~U//FOUO~~) Recognizing the importance of a comprehensive approach, the NSA Director of Compliance is prepared at the Court's convenience to discuss in detail the specific items listed above or more generally the approach and plan for continuing future improvements to the compliance program.

Has there been consideration of periodic and aperiodic monitoring to ensure compliance?

NSA: (~~TS//SI//NF~~) Yes. NSA has given substantial consideration to periodic and aperiodic monitoring and is committed to implementing and improving these activities. As ODOC establishes a Comprehensive Mission Compliance Program, one of the pillars

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

of that program is Monitoring and Assessment. One of the principal goals of this improvement will be substantially shortening the time between a potential issue and its detection.

~~(TS//SI//NF)~~ The NSA OIG has also proposed monitoring for oversight purposes as contained in the attachments.

~~(TS//SI//NF)~~ See the attached word and pdf documents provided by OIG on an intended audit of PR/TT prior to the last Order expiring as an example.

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