NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U//~~FOUO~~) Implementation of §215 of the USA PATRIOT Act and §702 of the FISA Amendments Act of 2008

ST-14-0002
20 February 2015

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

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

Classified By: [redacted]
Derived From: NSA/CSS Manual 1-52
Dated: 30 September 2013
Declassify On: ~~*20400220*~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to ensure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

ST-14-0002

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL

20 February 2015
IG-11763-15
Re-Issued

TO: DISTRIBUTION

SUBJECT: (U//~~FOUO~~) Report on the Implementation of §215 of the USA PATRIOT Act and §702 of the FISA Amendments Act of 2008 (ST-14-0002)

1. (U//~~FOUO~~) Attached please find the report on *Implementation of §215 of the USA PATRIOT Act and §702 of the FISA Amendments Act of 2008*, as requested by members of the Senate Committee on the Judiciary.

2. (U) In September 2013, ten members of the Senate Committee on the Judiciary requested a comprehensive, independent review of the implementation of §215 of the USA Patriot Act and §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008 (FAA §702) for calendar years 2010 through 2013. In January 2014, NSA's Office of the Inspector General (OIG) and staff members of the Senate Committee on the Judiciary agreed on the scope of a review the OIG would conduct on NSA's use of both authorities.

3. (U) The following is the NSA OIG's report on both authorities which will be sent to the ten members of the Senate Committee of the Judiciary who requested the review, the Chairman and Ranking Member of the House Committee on the Judiciary, the Chairman and Vice Chairman of the Senate Select Committee on Intelligence, and the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence.

4. (U//~~FOUO~~) We appreciate the cooperation and courtesies extended to our personnel throughout the review.

George Ellard

DR. GEORGE ELLARD
Inspector General

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

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

ST-14-0002

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

(U//~~FOUO~~) DISTRIBUTION:
SID DIR (Ron Moultrie)
TD DIR
OGC (Raj De)

AIG
CLPO (Rebecca Richards)
ODOC (Catherine Aucella)

LAO (Ethan Bauman)
OGC
S0
S1
S1S
S2
S2I
S3
S313
S35
S354
ST
SV
SV4
T1
T13
TE
TE2
TS
TV

DL BMD_Weekly (ALIAS) STC1
DL SIDIGLIAISON
DL TD_REGISTRY
DL TD_Strat_Ops_Grp
DL D_COMPLY_TASKER
DL d_gc_registry
DL d_lao_tasker

(U//~~FOUO~~) cc:
AIG
ODOC
OGC

DL S02 frontoffice (ALIAS) S02
S01
S02
S1
S1S
S203
S203
S2D
S2I4
S3
S3M
S31324
S35409
S35411
S35423
S35433
ST
SV3
SV42
TE2
T113
T121
T1222
T13
T1323
TS
TV
V07

IG
D/IG
D1
D11, D12, D13, D14

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

(U) TABLE OF CONTENTS

I. (U) INTRODUCTION

(U) Reason for Review

(U) In September 2013, ten members of the Senate Committee on the Judiciary requested a comprehensive, independent review of the implementation of §215 of the USA PATRIOT Act and §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008 for calendar years 2010 through 2013.

(U) Objectives

(U) In January 2014, the National Security Agency/Central Security Service's (NSA) Office of the Inspector General (OIG) and Committee staff agreed that the NSA OIG would review NSA's implementation of both authorities for calendar year 2013. The study has three objectives:

(U) Objective I

- (U) Describe how data was collected, stored, analyzed, disseminated, and retained under the procedures for §215 and FAA §702 authorities in effect in 2013 and the steps taken to protect U.S. person information.
- (U) Describe the restrictions on using the data and how the restrictions have been implemented, including a description of the data repositories and the controls for accessing data.
- (U) Describe oversight and compliance activities performed by internal and external organizations in support of §215 Foreign Intelligence Surveillance Court (FISC) Orders and FAA §702 minimization procedures.

(U) Objective II

- (U) Describe incidents of non-compliance with §215 FISC Orders and FAA §702 Certifications and what NSA has done to minimize recurrence.

(U) Objective III

- (U) Describe how analysts used the data to support their intelligence missions.

(U//~~FOUO~~) Our study of NSA's implementation of §215 and FAA §702 authorities was based largely on program stakeholder interviews and reviews of policies and procedures and other program documentation. For this review, the NSA OIG documented the controls implemented to address the requirements of each authority; however, we did not verify through testing whether the controls were operating as described by program stakeholders.

II. (U) SECTION 215 OF THE USA PATRIOT ACT

(U) Background

(U) Business Records Order

(U) Since May 2006, the Foreign Intelligence Surveillance Court (FISC) has authorized the National Security Agency/Central Security Service's (NSA) bulk collection program under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §1861, as amended by §215 of the USA PATRIOT Act, legislation enacted by the U.S. Congress and signed into law by the President. From its first authorization in May 2006 through December 2014, the program has been approved 40 times under Business Records (BR) Orders issued by 18 FISC judges.

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

~~(TS//SI//NF)~~ Pursuant to the series of BR Orders issued by the FISC, NSA receives certain call detail records (or BR metadata) from [redacted] U.S. telecommunication s providers. NSA refers to the series of BR Orders approved by the FISC as the "BR Order" and the control framework NSA has implemented as the "BR FISA program."

(U) The BR Order requires that providers produce to NSA certain information about telephone calls, principally those made within the United States and between the United States and foreign countries. This information is limited to BR metadata, which includes information concerning telephone numbers used to make and receive calls, when the calls took place, and how long the calls lasted but does not include information about the content of calls, the names of the participants, or cell site location information (CSLI).

(U) The BR FISA program was developed to assist the U.S. government in detecting communications between known or suspected terrorist s who are operating outside the United States and communicating with others inside the United States, as well as communications between operatives within the United States. The BR Order authorizes NSA analysts to query BR metadata only for identified counterterrorism purposes. The BR FISA program includes oversight mechanisms to maintain compliance with the BR Order and external reporting requirements to the FISC and Congress.

(U) BR renewal process

(U) Approximately every 90 days, the Department of Justice (DoJ) on behalf of the Federal Bureau of Investigation (FBI) and NSA files an application with the FISC requesting that certain providers continue to provide calling records to NSA for another 90 days. If the FISC approves the government's applications to renew the program, the Court issues a "primary order" delineating the scope of what the providers must furnish to NSA and the provisions for NSA's handling of BR

metadata. The FISC issues "secondary orders" separately to each provider, directing them to deliver an electronic copy of certain calling records to NSA daily until the expiration of the BR Order.

(U) Methodology and Scope

(U) Our review of the BR FISA program control framework, incidents of non-compliance, and NSA's use of the authority to support its counterterrorism (CT) mission was based largely on BR program stakeholder interviews and reviews of policies and procedures and other program documentation. For this review, we did not verify through testing whether the controls were operating as described by BR program stakeholders. However, we tested controls of the BR program during previous NSA Office of the Inspector General (OIG) reviews (see the Oversight section for a list of those reviews).

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

(U) Our study focused on the processes and controls in place in 2013. We used BR Order 13-158, approved by the FISC [redacted] and compared the requirements listed in that Order with the processes and controls NSA used to maintain compliance with that Order. In addition, we documented the changes implemented in the BR FISA program following the President's directives in 2014.

(U) Presidential directives affecting querying controls in 2014

(U) On 17 January and 27 March 2014, the President of the United States directed that NSA implement the following changes to the BR FISA program:

1. (U//~~FOUO~~) Submit selection terms to the FISC for reasonable articulable suspicion (RAS) approval (see Querying section for RAS discussion). Before 17 January 2014, RAS selection terms were approved by the Chief or Deputy Chief of NSA's Homeland Security Analysis Center (S2I4) or one of the twenty specially authorized Homeland Mission Coordinators (HMCs) as the BR Order required, and NSA's Office of General Counsel (OGC) performed First Amendment reviews for selection terms associated with U.S. persons (USPs).
2. (U//~~FOUO~~) Restrict contact chaining to two hops from seed selection terms (see Querying section for contact chaining discussion). Before 17 January 2014, the BR Order authorized appropriately trained and authorized NSA analysts to query to three hops; however, NSA guidance restricted those analysts to query BR FISA repositories two hops from seed selection terms and one additional hop (three hops from seed selection terms) with Analysis and Production (S2) management approval.
3. (U) Store BR metadata in provider controlled repositories and not in NSA repositories. Once implemented, NSA will submit FISC-approved RAS selection terms to providers for them to query their repositories. Providers will provide to NSA only the results of those queries.

(U//~~FOUO~~) NSA implemented the first two directives by February 2014. The third directive, storing BR metadata in provider repositories and obtaining only those query results from providers, will require Congressional approval of a new statute for the production of business records, which had not been implemented before this report was issued.

(U//~~FOUO~~) The following sections describe how the BR FISA program control framework complies with BR Order 13-158 (including the changes implemented following the President's directives in 2014), the 2013 BR FISA program incidents of non-compliance, and NSA's use of the BR FISA authority.

(U) BR FISA Program Control Framework

(U//~~FOUO~~) The BR FISA program control framework describes how NSA collects, samples, stores, accesses, queries, disseminates, and retains BR metadata and the oversight mechanisms to comply with the BR Order. This section summarizes the provisions of the BR Order and the controls implemented for each phase of the BR FISA production cycle.

(U) Collection

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

(U) Provisions of BR Order 13-158

~~(TS//SI//NF)~~ The BR Order requires [redacted] U.S. telecommunications providers to provide [redacted] an electronic copy of certain call detail records (hereinafter referred to as "BR metadata"). The BR Order defines BR metadata as comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, and International Mobile Station Equipment Identity (IMEI) number), trunk identifier, telephone calling card numbers, and time and duration of call.[1] BR metadata does not include the substantive content of communications; the name, address, or financial information of a subscriber or customer; or CSLI.

(U) Data received from providers

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

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

[redacted]

[1] (U) The IMEI number is a type of metadata related to mobile telephony. It is permanently embedded in a mobile telephone handset by the manufacturer and generally is not changeable by the user. In most instances, the IMEI does not travel with the Subscriber Identity Module (SIM) card, in contrast to the IMSI number, which does. The IMSI number is another type of metadata related to mobile telephony. It is a 15-digit number used to identify a customer. IMSI numbers are permanently stored on SIM cards, allowing a user to plug a card into any mobile telephone and be billed correctly. Calling card numbers are numbers used for billing telephone calls. A calling card number may be a telephone number, as the phrase is commonly understood and used, plus a personal identification number, or may be another unique set of numbers not including a telephone number.

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

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

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

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

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

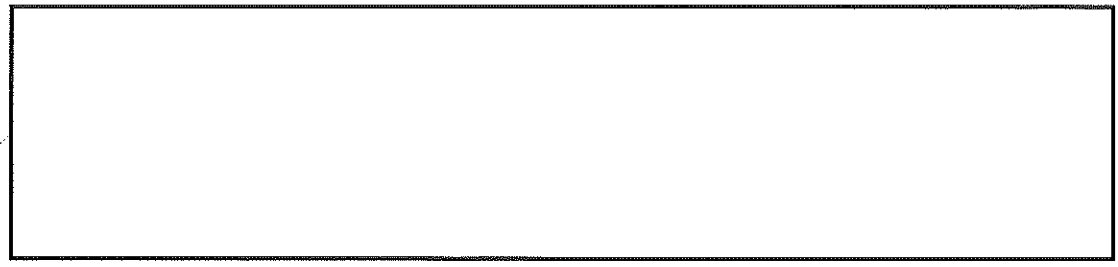
[2] (U//~~FOUO~~) A SCIF is an accredited area, room, or installation, incorporating physical control measures (e.g., barriers, locks, alarm systems, armed guards), to which no person has authorized access unless approved to receive the particular category of sensitive compartmented information and has a need to know the sensitive compartmented information activity conducted therein.

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

[3] (U//~~FOUO~~) A contact chain shows that selection term A communicated with selection term B, their first and last contact dates, telephony type, and the total number of communications between selection terms A and B.

[4] ~~(C//REL TO USA, FVEY)~~

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

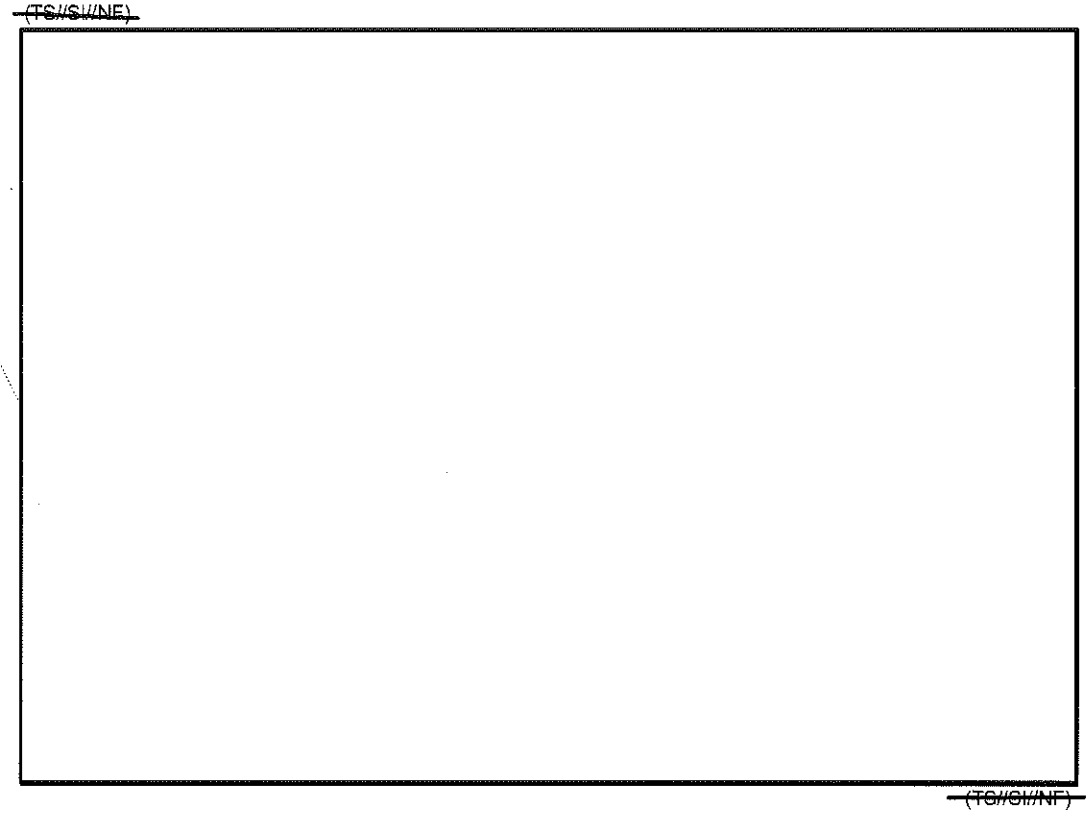


~~(TS//SI//NF)~~ Figure 1 illustrates the BR metadata dataflow from the provider to NSA and the various BR metadata repositories in 2013.

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

~~(TS//SI//NF)~~ Figure 1. BR Metadata Dataflow and Repositories

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



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

~~(TS//SI//NF)~~ The BR Order requires that [redacted] provide all BR metadata [redacted] for communications between the United States and abroad or wholly within the United States, including local telephone calls. The BR Order does not require [redacted]

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

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

~~(TS//SI//NF)~~ As of 31 December 2013, NSA received [redacted] BR metadata from [redacted] providers: [redacted]

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

(U) Table 1. BR FISA [redacted] (b)(3)-P.L. 86-36

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

(U) Metadata Sampling

(U) Sampling to verify BR metadata integrity

(U//~~FOUO~~) NSA's Data Integrity Analysts (DIAs) team [redacted] (b)(3)-P.L. 86-36 (S31324) has [redacted] full-time employees dedicated to the BR FISA program. DIA responsibilities include:

[6] (U//~~FOUO~~) The BR FISA Authority Lead is responsible to the NSA Director and the Director of the Signals Intelligence Directorate for implementation of FISC BR authorizations by the NSA organizations responsible for the collection, processing, and analysis of BR metadata under the BR Order.

- (U//~~FOUO~~) Verifying that BR metadata is correctly ingested, processed, and formatted into chains;
- (U//~~FOUO~~)
- (U//~~FOUO~~)
- ~~(S//NF)~~
- ~~(S//NF)~~
- ~~(S//NF)~~

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

~~(TS//SI//NF)~~ NSA has two types of controls to monitor data received from the providers and maintain compliance with the BR Order. The first is preventive control that uses rules. The second is a performed by the DIAs using data sampling techniques

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

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

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

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

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

~~(S//SI//NF)~~ The DIAs maintain the but changes are implemented by the project team. The are updated as needed and reviewed at least quarterly. The DIA team reviews proposed changes and decides which changes will be implemented by the team. hanges are tracked and maintained on the shared drive. The project team runs tests to verify that changes have been implemented and provides the test results to the DIA team to validate that the changes have been made.

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

(U//~~FOUO~~) **Sampling** DIAs run queries on the BR metadata to answer five questions as part of the sampling process controls to verify compliance with the BR Order:

[7] (U//~~FOUO~~) The standard format is

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

1. ~~(TS//SI//NF)~~ Did the BR metadata contain credit card numbers?
2. (U//~~FOUO~~) Did NSA detect CSLI in the [redacted] identification field?
3. (U) Did the BR metadata record structure adhere to expectations?
4. (U) Did the BR metadata record content adhere to expectations?
5. (U//~~FOUO~~) Did [redacted] adhere to expectations?

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

(U) The sampling results are submitted to NSA's Office of the Director of Compliance (ODOC) in weekly BR FISA compliance reports. ODOC compiles the information with other compliance reports and provides it to the Director of Compliance for review. The BR FISA Authority Lead summarizes the weekly BR FISA compliance reports for the DoJ National Security Division's (NSD) review before quarterly compliance review meetings (see Oversight section).

~~(TS//SI//NF)~~ **Credit card numbers** [redacted] DIAs sample the [redacted] known to have contained credit card numbers used as part of calling card personal identification numbers. The BR Order does not authorize NSA to receive customer financial information. [redacted] DIAs sample all BR metadata records for the [redacted] that could contain credit card numbers. The sampling of BR metadata is performed to identify [redacted] to screen for credit card numbers. When specific [redacted] are identified, DIAs test to determine whether they pass [redacted]

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

~~(TS//SI//NF)~~ [redacted] DIAs identify them as credit card numbers and forward them to [redacted] DIAs determine whether the credit card numbers were ingested into [redacted] and notifies stakeholders, including DoJ NSD.

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

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

~~(TS//SI//NF)~~ To demonstrate the number of files and BR metadata records that are sampled daily for credit cards, the OIG randomly selected [redacted] for review (Table 2).

(U) Table 2. [redacted] Sampling Metrics for Credit Cards

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

[redacted]

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

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

~~(TS//SI//NF)~~ To demonstrate the number of files and BR metadata records sampled [redacted] for credit cards, the OIG randomly selected the [redacted] testing performed on [redacted] (Table 3).

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

(U) Table 3. [redacted] Sampling Metrics for Credit Cards

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

[redacted]

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

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

[redacted]

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

~~(TS//SI//NF)~~ **Cell site location information (CSLI)** DIAs test the [redacted] to verify that it does not contain CSLI because the BR Order prohibits NSA from receiving this data. The DIAs sample [redacted]

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

[redacted] DIAs have identified no CSLI data in the [redacted] feed since it became operational [redacted]

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

~~(TS//SI//NF)~~ **Record structure** The DIAs sample BR metadata records [redacted] for each feed to test whether the BR metadata record structure has changed [redacted]

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

[redacted] (b)(1) (b)(3)-P.L. 86-36

[redacted] If any tests show differences, a warning message is generated for the DIAs to address. Changes in BR metadata record structure are very rare, but, if identified, the provider is contacted to determine whether the change is permanent or a one-time processing anomaly.

(U//~~FOUO~~) **BR metadata record content** DIAs review the BR metadata record content for each feed [redacted][8] According to the DIAs, exceptions are very rare. (b)(3)-P.L. 86-36

(U//~~FOUO~~) Table 4 shows the percentage of the [redacted] feeds tested for BR metadata record structure and content during 2013.

(U//~~FOUO~~) Table 4 [redacted] Sampling Percentages for BR Metadata Record Structure and Content Testing

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

[redacted]

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

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

~~(TS//SI//NF)~~ **Data feed volumes** DIAs monitor data feed volumes [redacted] for anomalies by reviewing the [redacted] Status Report," which lists for each feed the number of raw BR metadata records [redacted] received and the number of [redacted] records [redacted]

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

(U//~~FOUO~~) Table 5 shows the number of BR metadata records received [redacted] (b)(1) (b)(3)-P.L. 86-36

[8] (U//~~FOUO~~) BR metadata record content is distinct from the content of communications: BR metadata record content does not contain the content of communications, defined in 18 U.S.C. §2510, as the substance, purport, or meaning of a communication.

(U) Table 5. Total Number of BR Metadata Records Received

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

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

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

(U) Table 6 summarizes the provisions of BR Order 13-158 for collection and the controls NSA implemented to maintain compliance.

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

(U) Table 6. Collection Provisions and Controls

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

Provision	Control
~~(TS//SI//NF)~~ Provide Daily BR Metadata Records	~~(TS//SI//NF)~~ monitor for data flow problems. DIAs monitor data feed volumes for anomalies.
(U) NSA Only Receives Authorized Data	~~(TS//SI//NF)~~ Parser rules are designed to prevent unauthorized data from being ingested into operational systems. DIAs sample data to detect unauthorized data.

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

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

(U) Repositories

(U) Provisions of BR Order 13-158

(U) NSA will store and process BR metadata in repositories within secure networks under NSA control.

(U) NSA repositories that store BR metadata

(U//~~FOUO~~) All NSA systems that store and process BR metadata are certified as secure through an accreditation and certification process and are in NSA controlled SCIFs. During 2013, the following systems stored and processed BR metadata.

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

- ~~(S//SI//REL TO USA, FVEY)~~ is the corporate contact chaining database

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

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

- ~~(S//SI//REL TO USA, FVEY)~~ is the corporate database repository that stores BR metadata

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

- (U//~~FOUO~~) is the contingency system for and has the same hardware and software as
- ~~(S//REL TO USA, FVEY)~~ is the system backup
- (U//~~FOUO~~) **Backup tapes** are maintained at The BR metadata electronically stored in are saved to tape backup

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

- (U//~~FOUO~~) designed for the BR FISA program is software that runs on a system.
- (U//~~FOUO~~) data distribution systems move BR metadata between NSA systems.

~~(C//REL TO USA, FVEY)~~ **How information is stored in**

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

~~(S//SI//REL TO USA, FVEY)~~ are the only operational databases used to store BR metadata for intelligence analysis. As previously mentioned,

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

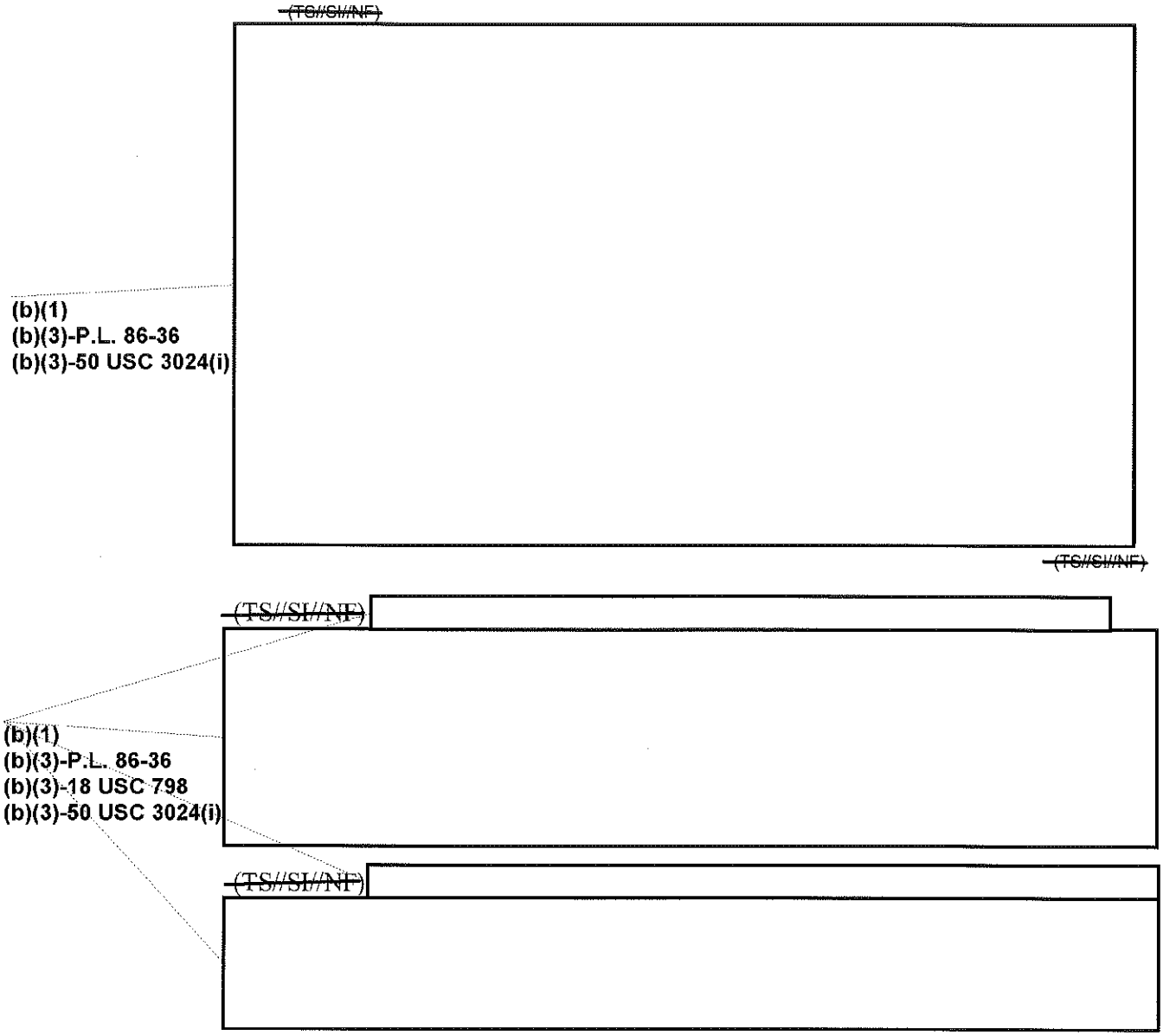
~~(TS//SI//NF)~~

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

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

[9] (U//~~FOUO~~)

(U//~~FOUO~~) Figure 2. [redacted] Architectures (b)(3)-P.L. 86-36



(U) NSA system accreditation and certification processes

(U//~~FOUO~~) **Accreditation** [redacted] (TS) is responsible for managing the risk on all NSA networks and the computer systems and devices connected to those networks. TS responsibilities include:

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

[10] (U) A relational database stores data in tables using a standardized data format. This allows similar information to be organized and queried on the basis of specific data fields.

- (U//~~FOUO~~) Guiding, prioritizing, and overseeing the development of information assurance programs necessary to ensure protection of information systems and networks by managing the NSA Information Security Program,
- (U//~~FOUO~~) Serving as the NSA Director's Authorizing Official to accredit all NSA information systems,
- (U//~~FOUO~~) Conducting information systems security and accreditation and risk management programs, and
- (U//~~FOUO~~) Establishing, maintaining, and enforcing information systems security policies and implementation guidelines for NSA.

(U//~~FOUO~~) Accreditation is the official management decision to permit operation of an information system in a specific environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

(U//~~FOUO~~) When accrediting systems, TS uses a risk management framework to determine the appropriate level of risk mitigation needed to protect systems, information, and infrastructure. The framework comprises six steps.

- (U) Categorize the information and information system,
- (U) Select an initial baseline of security controls and tailor as appropriate for the system, data, and environment,
- (U) Implement and build the security controls in the information system,
- (U) Authorize the operation of the information system (accept the risk), and
- (U) Monitor continually and assess the effectiveness of the security controls.

(U//~~FOUO~~) Before a system is authorized to be put on a network, it must go through the accreditation process and be approved by TS. Table 7 lists the dates through which the BR repositories are accredited.

(U) Table 7. Dates through which BR Repositories Are Accredited

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

Repository	Accredited Through

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

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

(U//~~FOUO~~) **Certification** In addition to the TS system accreditation requirement, all systems containing FISA data must be certified by [redacted] (TV) [redacted] (TV4). TV4 is the NSA authority for certification of systems to ensure they are compliant with the legal and policy regulations protecting USP privacy.

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

(U//~~FOUO~~) [redacted] TV began certifying FISA systems, including the repositories that contain BR metadata, to ensure that they comply with USP privacy protection. TV developed [redacted] the NSA corporate database for registration of NSA systems and their compliance certification and data flows. It is NSA's authoritative source for all compliance certifications. TV's certification process evaluates system controls for maintaining compliance in the following areas: purge, data retention and aging off, data access, querying, dissemination, data tagging, targeting, and analytical processes.

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

(U//~~FOUO~~) To be certified to handle FISA data, systems must be certified by TV as part of the Compliance Certification process. Table 8 shows the TV4 certification dates for repositories that contain BR metadata.

(U) Table 8. Certification Dates for Repositories Containing BR Metadata

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

Repository	Date Certified

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

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

(U) Table 9 summarizes the provision of BR Order 13-158 for repositories and the control NSA implemented to maintain compliance.

(U) Table 9. BR Repository Provision and Control

(U//~~FOUO~~)

Provision	Control
NSA will store and process BR metadata in repositories within secure networks under NSA control.	All BR FISA systems are certified as secure through NSA's system accreditation (TS) and certification process (TV4) and located in NSA controlled SCIFs.

(U//~~FOUO~~)

(U) Access and Training

(U) Provisions of BR Order 13-158

(U) BR metadata shall carry unique markings such that software and other controls (including user authentication services) can restrict access to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to BR metadata to authorized personnel who have received appropriate and adequate training.

(U) Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the

specified persons to NSA will not receive special training regarding the authority granted herein.

(U) NSA's OGC and ODOC will further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA will maintain records of all such training.

(U) OGC will provide DoJ NSD with copies of all formal briefing and/or training materials (including all revisions) used to brief or train NSA personnel concerning this authority.

(U) Restricting access to BR metadata to authorized personnel

~~(TS//SI//NF)~~ The Signals Intelligence Directorate's (SID) Office of Oversight & Compliance (SV) verifies semi-weekly that persons authorized access to BR metadata maintain the required credentials [redacted] The training required for these two credentials is listed in the "Appropriate and Adequate Training" heading of this section.

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

~~(TS//SI//NF)~~ The [redacted] credential signifies that an individual has been adequately and appropriately trained (discussed below) with regard to the BR FISA program and provides the authorization to view the results of BR metadata queries, in any form, including written and oral summaries of results. [redacted] does not provide access to the BR metadata in the bulk metadata (BMD) repositories or authorization to query the data.

~~(TS//SI//NF)~~ Table 10 shows a breakdown of the number of personnel with [redacted] as of 31 December 2013 by affiliation.

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

~~(TS//SI//NF)~~ Table 10. Number of Personnel with [redacted] by Affiliation

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

Affiliation	[redacted]
NSA Civilians	
NSA Military	
Non-Agency Civilians [redacted]	
Contractors	
Total	

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

~~(TS//SI//NF)~~ Table 11 shows a breakdown of the number of personnel with [redacted] as of 31 December 2013 by work role.

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

~~(TS//SI//NF)~~ Table 11. Number of Personnel with [redacted] by Work Role

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

Work Role	Number of Personnel
Analyst	
Oversight	
Leadership	
Staff	
Technical	
Contractor	
Total	

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

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

~~(TS//SI//NF)~~ The [redacted] credential signifies that a person is authorized to access BMD repositories and is the first step in obtaining the ability to use [redacted] to perform queries against BR metadata.[11] [redacted] is only authorized for specific intelligence analysts working CT targets described in the BR Order and technical personnel who maintain the systems that process and store BR metadata. The BR FISA Authority Lead is the ultimate authority for deciding which organizations are authorized to access BR metadata repositories.

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

~~(TS//SI//NF)~~ Table 12 shows a breakdown of the number of personnel with [redacted] as of 31 December 2013, by affiliation and work role.

~~(TS//SI//NF)~~ Table 12. Number of Personnel with [redacted] by Affiliation and Work Role

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

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

Affiliation and Work Role	Number of Personnel
NSA Civilians	
- Analyst	
- Oversight	
- Technical	
- **Total**	
NSA Military	
Contractors	
- Technical	
Total	

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

~~(TS//SI//NF)~~ [redacted] In addition to [redacted] if an individual needs to query BR metadata using the intelligence analyst contact chaining tool, a Division Chief, Deputy Division Chief, Branch Chief, or Deputy Branch Chief must submit to SV a written request that the individual be given query access. If the individual is current in all training and holds the [redacted] credentials, SV sends an e-mail to the [redacted] team and requests that the person be added to the

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

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

[11] (U//~~FOUO~~) [redacted] is the graphical user interface analysts use to query data, including BR metadata, in [redacted]

[redacted] User Group in [redacted][12] The [redacted] administrator verifies the person's credentials and training, adds the person to the user group, and notifies SV when complete. Upon completion, [redacted] automatically sends an e-mail to SV indicating that the person has been added to the user group. This additional management control helps ensure that only appropriately trained and authorized personnel are able to execute queries.

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

(U//~~FOUO~~) Table 13 shows a breakdown of the number of personnel on the [redacted] User Group with querying capability as of 31 December 2013.

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

(U) Table 13. Number of Personnel with Querying Capability as of 31 December 2013

(U//~~FOUO~~)

Work Role	Number of Personnel
Analysts	
Technical	
Total	

(U//~~FOUO~~)

~~(TS//SI//NF)~~ **Receiving query results** NSA personnel who receive query results are required to receive training and guidance regarding the procedures and restrictions for handling and disseminating such information. Before analysts send BR-unique query results containing USP information to another individual, they must first confirm that the recipient has the [redacted] credential.[13] Sharing BR-unique query results containing USP information with an individual without the [redacted] credential would violate the BR Order and require notice to the Court.

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

(U) **Training records** The BR Order requires that NSA maintain records of BR training. NSA's Associate Directorate for Education and Training (ADET) Enterprise Learning Management database is NSA's source system of record (SSR) for maintaining training completion records for all required training.

(U) Figure 3 shows the categories of individuals authorized access to BR data.

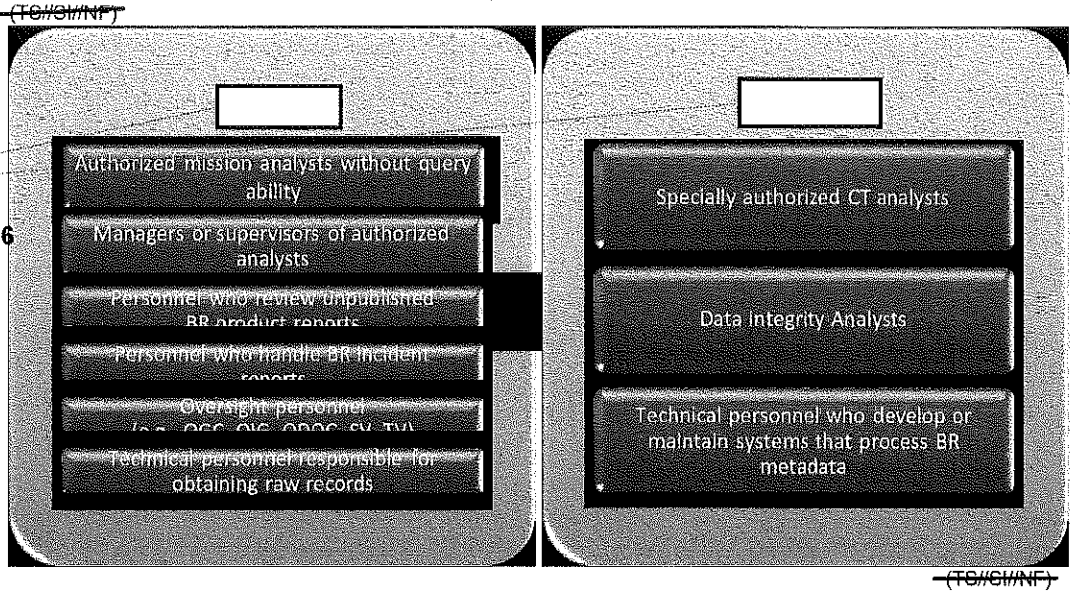
(b)(3)-P.L. 86-36

[12] (U//~~FOUO~~) [redacted] is NSA's Corporate Authorization Service Portal, which provides authorization attributes and access control services to NSA programs and projects.

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

(U//~~FOUO~~) Figure 3. Access to BR Information Determined by Credentials Maintained by BR Stakeholders

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



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

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

~~(TS//SI//NF)~~ **Obtaining the credential** To obtain the [redacted] credential, a request must be submitted in the [redacted] NSA's corporate credentialing system. A [redacted] request must contain the name of a valid sponsor who currently holds the requested credential. The Associate Directorate for Security and Counterintelligence (Q) reviews [redacted] requests for security concerns. If approved, the request is forwarded to SV for final adjudication. SV verifies that the individual is current on the required training (explained below) and that the request includes a valid mission justification. If all requirements are met, SV approves the credential in [redacted] for entry into [redacted]

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

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

~~(TS//SI//NF)~~ **Maintaining the credential** To ensure that personnel remain current on training, SV runs a [redacted] report several times a week that lists all the personnel with the [redacted] credential and their training status, which is color coded (green=current, red=expired). If someone's OVSC1000 or OVSC1100 training has expired, SV notifies that person by e-mail that training must be completed. If OVSC1800 or OVSC1205/OVSC1206 has expired, access is revoked immediately. Access is not restored until a new [redacted] request is submitted and all training is current. If an individual's training expires and the credential has been revoked, this would not violate the BR Order. However, if someone accesses BR metadata but has not completed the required training, this would violate the BR Order because the person has not been appropriately and adequately trained. The violation requires notice to the Court.[14]

[14] (U//~~FOUO~~) The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA will not receive special training regarding the authority granted herein.

(U//~~FOUO~~) **Appropriate and adequate training** NSA/CSS Policy 1-23, *Procedures Governing NSA/CSS Activities That Affect U.S. Persons*, 30 July 2013, requires that Agency personnel (civilians, military, military reservists, integrees, and most contractors) complete intelligence oversight (IO) training annually.

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

~~(TS//SI//NF)~~ In addition, to qualify for the [redacted] credential and comply with the requirements of the BR Order, persons must have completed specific training courses within the last 12 months. All courses are developed by NSA's ADET in conjunction with the OGC, mission subject matter experts, and mission compliance professionals.

- (U//~~FOUO~~) **OVSC1000**, NSA/CSS Intelligence Oversight Training, the Agency's core IO course is provided to the workforce to maintain a high degree of sensitivity to and understanding of intelligence laws, regulations, and policies associated with the protection of USP privacy rights during mission operations. Personnel are familiarized with the major tenets of the four core IO documents: Executive Order (E.O.) 12333, as amended; Department of Defense (DoD) Regulation 5240.1-R; Directive Type Memorandum (DTM) 08-052; and, NSA/CSS Policy 1-23. OVSC1000 is web based and includes knowledge checks for proficiency.[15]
- (U//~~FOUO~~) **OVSC1100**, Overview of Signals Intelligence Authorities, the core SIGINT IO course, provides an introduction to various legal authorities that NSA uses to conduct its operations. Upon completion, personnel should be able to identify applicable surveillance authorities at a high level, define the basic provisions of the authorities, and identify situations and circumstances requiring additional authority. OVSC1100 is web based and includes knowledge checks for proficiency. All personnel in the U.S. SIGINT System (USSS) working under the NSA Director's SIGINT authority with access to raw SIGINT are required to complete OVSC1100 every 12 months.
- (U//~~FOUO~~) **OVSC1800 (Analytic) and OVSC1806 (Technical)**, Legal Compliance and Minimization Procedures, advanced SIGINT IO course that explains policies, procedures, and responsibilities within missions and functions of the USSS to enable the protection of USP and foreign partner privacy rights. Upon successful completion, NSA analysts with mission requirements to access raw SIGINT databases will have met the additional training requirement imposed by SID. OVSC1800 and OVSC1806 are web based and include competency exams [redacted] Personnel who do not pass the test after [redacted] attempts must complete remedial training. All personnel in the USSS working under the NSA Director's SIGINT authority with access to raw SIGINT are required to complete OVSC1800 or OVSC1806 every 12 months.

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

[15] (U//~~FOUO~~) E.O. 12333, *United States Intelligence Activities*; DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons*; DTM-08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*.

- (U//~~FOUO~~) **OVSC1205 (Analytic) and OVSC1206 (Technical)**, Special Training on FISA, advanced IO courses that present legal policies surrounding the FISC Orders and RAS standards pertaining to specific CT focused programs. OVSC1205 and OVSC1206 are web based and include competency exams with a minimum passing score of 90 percent for OVSC1205 and 89 percent for OVSC1206, a higher proficiency threshold than other courses because BR FISA data has a greater probability of containing USP information. Personnel who do not pass the test after one attempt must complete remedial training. All personnel with access to the BR FISA program are required to complete OVSC1205 or OVSC1206 every 12 months.

(U//~~FOUO~~) **DoJ NSD review of training material** As the BR Order requires, NSA's OGC provides DoJ NSD copies of the material (e.g., OVSC1205 and OVSC1206 training courses) used to train NSA personnel on the authority. OGC most recently provided DoJ NSD copies of revisions to the training materials in February 2014. NSA had revised the training materials because of the 17 January 2014 program changes, which included the two-hop limitation and FISC RAS-approval process.

(U) Access requirements for technical personnel to BR repositories

(U//~~FOUO~~) The BR Order states that appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make the data usable for intelligence analysis. The following describes the repositories and systems and the access requirements for technical personnel.

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

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

[16] (U//~~FOUO~~) Backup tapes are securely stored in a locked cabinet inside a restricted access room at a secure facility and are only accessible by designated personnel.

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

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

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

- (U//~~FOUO~~) **NSA's Corporate Infrastructure** Technical personnel responsible for maintaining NSA's underlying corporate infrastructure and transmission of BR metadata to NSA (e.g., corporate personnel and SharePoint system administrators) are not required to receive special training regarding the BR program.

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

(U) Access requirements for analysts to query BR repositories

~~(TS//SI//NF)~~ To query the database using analysts, including DIAs, must be listed on the User Group in The process to be added to the user group was discussed in the section. When analysts log into using their public key infrastructure (PKI) password, verifies that the analysts are listed on the user group and they have the credentials.[18] If all three requirements are met, the analysts are able to select the mode in and query BR metadata. As of 31 December 2013, personnel had the ability to run queries on BR data using

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

(U//~~FOUO~~) Table 14 summarizes the provisions of BR Order 13-158 for access and training and the controls implemented by NSA to maintain compliance.

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

[17] (U//~~FOUO~~) TD technical personnel system accesses to were terminated.

[18] (U//~~FOUO~~) PKI is used to authenticate users on NSA networks. PKI binds public keys with users of a digital certificate authority.

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

(U) Table 14. Access and Training Provisions and Controls

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

Provision	Control
(U) Access to BR metadata shall be restricted to authorized personnel who have received appropriate and adequate training. (b)(3)-P.L. 86-36	~~(TS//SI//NF)~~ All personnel with access to BR metadata must be approved for the [redacted] credential. All personnel with access to the BMD repositories must have the [redacted] credential. All personnel who query the BR metadata in the BMD repositories must have the [redacted] credential and be on the [redacted] User Group in [redacted] All personnel with the [redacted] credential must complete appropriate and adequate training verified and monitored by SV.
(U) Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis.	~~(TS//SI//NF)~~ Technical personnel with access to the BR metadata must have the [redacted] credential and must have completed appropriate and adequate training verified and monitored by SV.
(U) Technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA will not receive special training regarding the authority granted herein.	(U) Technical personnel responsible for NSA's underlying corporate infrastructure do not receive special training regarding the BR program. (b)(1) (b)(3)-P.L. 86-36
(U) NSA's OGC and ODOC will further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.	~~(TS//SI//NF)~~ Before an analyst sends BR-unique query results containing USP information to another individual, the analyst must confirm that the recipient has the [redacted] credential.* An individual with the [redacted] credential must complete and remain current on required training, which includes training and guidance on handling and disseminating such data.
(U) NSA will maintain records of all such training.	(U//~~FOUO~~) NSA's ADET Enterprise Learning Management database is NSA's SSR for maintaining training completion records.
(U) OGC will provide DoJ NSD with copies of all formal briefing and/or training materials (including all revisions) used to brief/train NSA personnel concerning this authority.	(U//~~FOUO~~) NSA's OGC provides BR FISA training material to DoJ NSD for review before modifying material in the OVSC1205 and OVSC1206 training courses.
*~~(C//REL TO USA, FVEY)~~ [redacted]	

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

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

(U) Querying

(U) Provisions of BR Order 13-158

~~(TS//SI//NF)~~ NSA may access BR metadata for purposes of obtaining foreign intelligence information only through queries of the BR metadata to obtain contact

chaining information using selection terms approved as seeds.[19] A seed is a selection term approved for querying BR metadata. All selection terms to be used as seeds with which to query the BR metadata must first be approved by the S2I4 Chief or Deputy Chief or one of the twenty specially authorized HMCs in the SID Analysis and Production Directorate.[20] Approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a RAS that the selection term to be queried is [redacted] (hereafter the Foreign Powers). If the selection term is reasonably believed to be used by a USP, the NSA's OGC must first determine that the USP is not regarded as [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.[21] RAS approvals shall be effective for 180 days for any selection term reasonably believed to be used by a USP and one year for all other selection terms.

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

(U//~~FOUO~~) Furthermore, queries of the BR metadata using RAS approved selection terms may occur either by manual analyst query or through the automated query process.[22] Contact chaining queries of BR metadata will begin with a RAS approved seed, and will return only that metadata within three "hops" of the seed.[23]

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

[19] (U//~~FOUO~~) The term "selection terms" includes but is not limited to "identifiers." The term "identifiers" means a telephone number, as that term is commonly understood and used; [redacted]

[20] ~~(TS//SI//NF)~~ Selection terms that are the subject of electronic surveillance authorized by the FISC based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by USPs, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. On 26 February 2014, NSA began sending selection terms to the FISC for RAS approval to comply with the President's directive of 17 January 2014. On 28 February 2014, the FISC approved RAS for the first two selection terms under this new process.

[21] (U) The First Amendment to the U.S. Constitution prohibits making any law abridging the freedom of speech, infringing on the freedom of the press, interferin g with the right to peaceably assemble, or prohibiting the petitioning for a government redress of grievances. The BR Order no longer requires that NSA's OGC perform a First Amendment review of selection terms used by USPs for non-emergency RAS requests; the FISC performs those reviews. This change was made following the President's directive on 17 January 2014, which requires that NSA submit selection terms to the FISC for RAS approval.

[22] ~~(TS//SI//NF)~~ The automated query process was initially approved by the FISC in the 7 November 2012 Order that amended docket number BR 12-178. Although approved, NSA never implemented and is no longer authorized to use the automated query process since it withdrew its request to do so in the renewal applications and declarations that support the BR Orders approved by the FISC (beginning with BR Order 14-67, dated 28 March 2014).

[23] (U//~~FOUO~~) The first hop from a seed returns results including all selection terms (and their associated metadata) with a contact and/or connection with the seed. The second hop returns results that include all selection terms (and their associated metadata) with a contact and/or connection with a selection term revealed by the first hop. The third hop returns results that include all selection terms (and their associated metadata) with a contact and/or connection with a selection term revealed by the second hop. On 29 January 2014, NSA's software system controls were modified to limit the number of hops from seed selection terms to two to comply with the President's directive of 17 January 2014.

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

Appropriately trained and authorized technical personnel may query BR metadata using selection terms that have not been RAS approved to perform processes needed to make the BR metadata usable for intelligence analysis and may share the results of those queries with other authorized personnel responsible for these purposes. However, the results of such queries may not be used for intelligence analysis purposes. NSA must ensure through adequate and appropriate technical and management controls that queries of BR metadata for intelligence analysis purposes will be initiated using only selection terms that have been RAS approved.

(U) Presidential directives affecting querying controls in 2014

(U) On 17 January 2014 and 27 March 2014, the President of the United States directed that NSA implement the following changes to the BR FISA program:

1. (U//~~FOUO~~) Submit selection terms to the FISC for RAS approval. Before 17 January 2014, selection terms were RAS approved by the S2I4 Chief or Deputy Chief or one of the twenty specially authorized HMCs as the BR Order required, and OGC performed First Amendment reviews for selection terms associated with U.S. persons.
2. (U//~~FOUO~~) Restrict contact chaining to two hops from seed selection terms. Before 17 January 2014, appropriately trained and authorized NSA analysts were authorized to query to three hops; however, NSA guidance restricted those analysts to query BR FISA repositories two hops from seed selection terms and one additional hop (three hops from seed selection terms) with S2 division management approval.
3. (U//~~FOUO~~) Store BR metadata in provider controlled repositories and not in NSA repositories. Once implemented, NSA will submit FISC-approved RAS selection terms to providers for them to query their repositories. Providers will provide to NSA only the results of those queries.

(U//~~FOUO~~) NSA implemented the first two directives by February 2014. The third directive, storing BR metadata in provider repositories and obtaining only those query results from providers, will require passage of a new statute for the production of business records, which had not been enacted when this report was issued.

(U//~~FOUO~~) The remainder of this section documents the control framework in place for querying BR metadata in 2013, including the changes implemented by the President's directives in 2014.

(U) Determining seed selection terms for requesting RAS approval

(U//~~FOUO~~) Analysts working CT missions focus on lead selection terms, which can be derived from multiple sources, [redacted] (b)(3)-P.L. 86-36 [redacted] Analysts apply a wide range of tradecraft in determining which selection terms to pursue RAS approval. [redacted]

[redacted]

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

(U//~~FOUO~~) Analysts making determinations whether selection terms are eligible to be used as seeds under the BR FISA authority must consider all the facts they know or reasonably can know before submitting requests for RAS approval. Looking at the totality of the circumstances, analysts evaluate whether there is a RAS that the selection terms are used by persons associated with one of the terrorist organizations in the BR Order. The level of proof demanded by the RAS standard is less than a preponderance of the evidence or probable cause.

(U//~~FOUO~~) Nonetheless, the RAS standard requires more than a mere hunch or uninformed guesswork. Analysts must have an "articulable reason," supported by at least one source, for suspecting that the person using the selection term is associated with one of the terrorist organizations in the BR Order. Sources used to justify RAS requests include, but are not limited to, [redacted][24] The RAS standard is the same for selection terms associated with USPs and foreign persons.

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

~~(TS//SI//NF)~~ Analysts electronically submit RAS requests in [redacted] – NSA's RAS selection term management system. [redacted] has required fields for analysts to enter justifications for RAS requests, user nationalities, and user ties to at least one of the terrorist organizations in the BR Order. Analysts save the supporting documentation for RAS requests in [redacted] for review by designated officials. As authorized by the BR Order, if selection terms are subject to ongoing FISC-authorized electronic surveillance [redacted] based on a finding of probable cause that the selection term is used or about to be used by persons associated with one of the identified foreign powers, NSA may use the selection terms to query the BR metadata without obtaining RAS because probable cause, a higher standard, has already been met. In these cases, entries are still submitted through [redacted] along with supporting documentation, and HMC and possible OGC review (if a selection term is associated with a USP) would also be required. According to [redacted] a majority of the selection terms submitted for RAS approval are derived from [redacted]

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

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

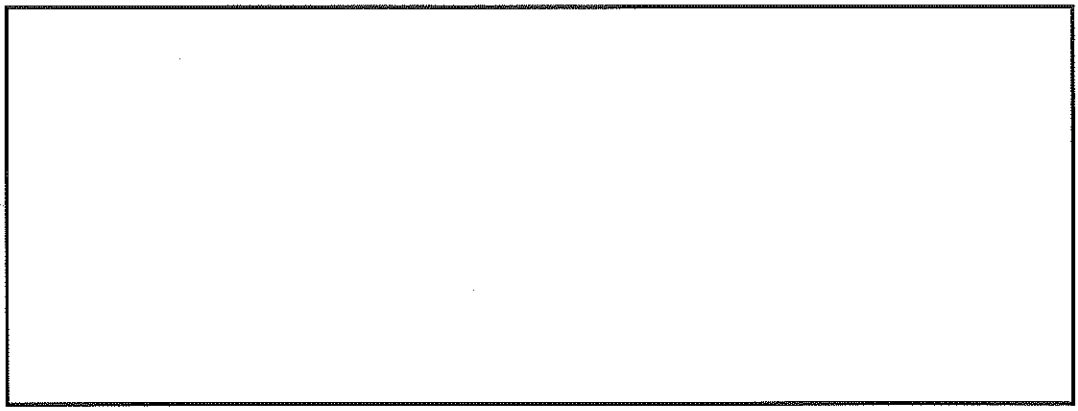
~~(TS//SI//NF)~~ **Maintaining the** [redacted] **list in** [redacted]

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

[redacted]

[24] (U//~~FOUO~~) If RAS requests are based in part or in whole on NSA SIGINT, NSA performs a purge verification check for the selection term when the request is submitted to ensure that the selection term had not been submitted for on-demand, retroactive, or reactionary removal of data from NSA SIGINT system repositories. The "purge verification" field must be filled out when creating a RAS request and must be conducted no more than 24 hours before submission.

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



~~(TS//SI//NF)~~ RAS can be met only on selection terms associated with the terrorist organizations listed in [redacted] Those would include organizations listed in the FISC-approved BR Order or based on IC reporting and determined by NSA's OGC and SV as [redacted] a terrorist organization in the FISC-approved BR Order.[25] [redacted]

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

Only individuals assigned the [redacted] role can maintain the terrorist organization list in [redacted] NSA personnel were assigned this role [redacted]

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

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

~~(TS//SI//NF)~~ [redacted] which NSA implemented in June 2010, provides the system control framework for nominating, justifying, reviewing, approving, and disapproving RAS for selection terms. [redacted] has built-in safeguards to ensure that RAS approved selection terms comply with requirements of the BR Order (e.g., required RAS approvals documented, only approved terrorist organizations used for RAS, maximum time limits not exceeded for RAS approvals). [redacted] also serves as the authoritative source for RAS approved selection terms and exports the selection terms to other systems in the BR control framework.

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

(U) RAS approval process—2013

(U//~~FOUO~~) In 2013, the RAS approval process included certain mechanisms NSA used to determine whether selection terms were associated with one of the terrorist organizations in [redacted] before BR authorized analysts could use the selection terms as seeds to query BR metadata. Consistent with the BR Order, all selection terms used as seeds for querying BR metadata were first approved by the S2I4 Chief

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

[25] ~~(TS//SI//NF)~~ In May 2012, DoJ NSD stated that it was generally acceptable for NSA's OGC to determine, based on IC reporting, [redacted] In addition, with the condition of RAS being met, NSA can include [redacted] DoJ NSD further stated that OGC must revisit those determinations every six months [redacted]

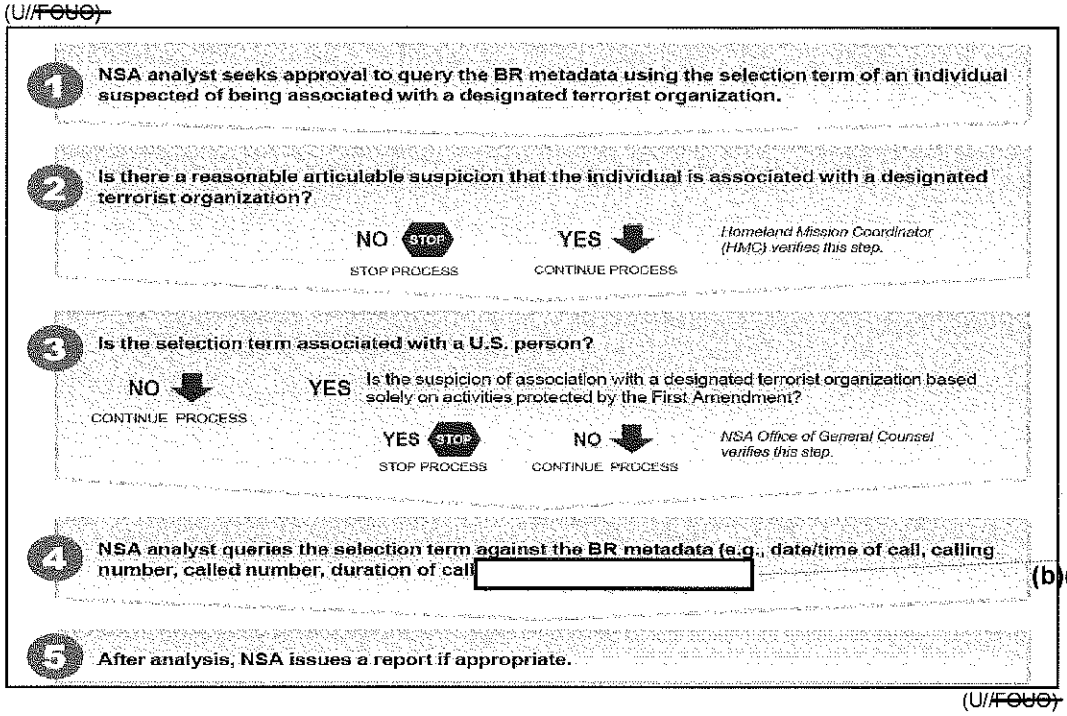
(b)(3)-P.L. 86-36

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

or Deputy Chief or one of the 20 specially authorized HMCs. If selection terms were reasonably believed to be used by USPs, NSA's OGC determined whether the USPs were regarded as associated with one of the terrorist organizations named in the BR Order solely on the basis of activities protected by the First Amendment. Figure 4 illustrates the RAS approval process in place during 2013.

(U) Figure 4. RAS Approvals Needed Before Querying BR Metadata in 2013

(U//~~FOUO~~)



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

(U//~~FOUO~~)

(U//~~FOUO~~) Table 15 summarizes the RAS selection terms approved in 2013.

(U) Table 15. 2013 RAS Approvals

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

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

Domestic Selection Terms		Foreign Selection Terms		Total Selection Terms RAS Approved *	Total Unique Selection Terms RAS Approved †
Approved	(% of total)	Approved	(% of total)		

* (U//~~FOUO~~) Data includes RAS selection terms that were approved more than once in 2013.

† (U//~~FOUO~~) Data only includes unique selection terms approved during 2013; it excludes multiple RAS approvals for the same selection terms in 2013.

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

(U) HMC review process—2013

(U//~~FOUO~~) After RAS approval requests are submitted in automatic e-mail notifications are sent to HMCs alerting them that requests are available for review. Depending on the ranking assigned to RAS approval requests in reminder e-mails are sent after for emergency requests, for urgent

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

requests, [redacted] for priority requests, and [redacted] for routine requests. HMCs verify that:

- (U//~~FOUO~~) Justifications sufficiently and accurately document user ties to the selection terms submitted for RAS approval;
- (U//~~FOUO~~) Justifications clearly support user ties to one of the terrorist organizations listed in [redacted]

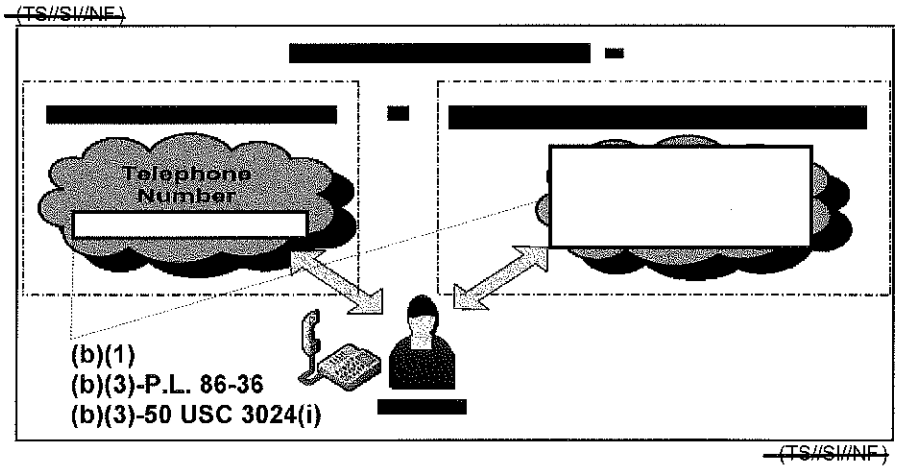
(b)(3)-P.L. 86-36

- (U//~~FOUO~~) RAS requests are supported by credible source documentation;
- (U//~~FOUO~~) Source documentation is current and has not been superseded by other intelligence; RAS requests contain time restrictions, if selection terms are or were associated with users for only a specific and limited time; and
- (U//~~FOUO~~) If SIGINT is used as justification for RAS approval requests, analysts performed purge verifications when requests are submitted.

(U//~~FOUO~~) If HMCs determine that the documentation requirements have not been met and the RAS standard has not been not satisfied, analysts are notified of deficiencies and asked to provide additional information. HMCs denote denied RAS requests as "Pending" until adequately documented in [redacted] If the documentation requirements are met and the RAS standard has been satisfied, HMCs change the status of requests from "Pending" to "Approved" in [redacted][26] Change logs in [redacted] document all status changes and edits of the original RAS approval requests by analysts and designated approvers. For oversight purposes, change log histories cannot be edited. [redacted] system controls require that OGC approve selection terms used by USPs before completing the RAS approval process. Figure 5 illustrates the RAS standard.

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

(U//~~FOUO~~) Figure 5. RAS Standard



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

[26] (U//~~FOUO~~) Some BR trained and authorized analysts can approve RAS requests and query BR metadata. However, [redacted] system controls prevent persons from submitting and approving their own RAS requests.

(U) OGC First Amendment review of seed selection terms associated with USPs—2013

(U//~~FOUO~~) NSA is prohibited from establishing RAS on a USP selection term based solely on activities protected by the First Amendment. In 2013, RAS requests containing selection terms associated with USPs were forwarded to the NSA OGC for a First Amendment review. [redacted] sent automated e-mail notifications to designated OGC attorneys until a First Amendment review was completed. OGC reviewed the RAS requests and source documentation, as well as the RAS decisions made by HMCs, and determined whether NSA intended to target individuals based solely on activities protected by the First Amendment. If there were indications that RAS requests were based solely on such activities, OGC would deny the RAS request (denoted as "Disapproved" in [redacted]. Once OGC has approved RAS requests in [redacted] the selection terms are authorized for use as seeds for querying. However, a series of system updates must be completed before analysts can query BR metadata using newly approved seed selection terms. [redacted]

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

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

(U) Controls for querying BR metadata using only RAS approved seed selection terms within the authorized number of hops

(U//~~FOUO~~) [redacted] tracks the status of selection terms and for an "Approved" status the expiration of the RAS approval. The BR Order specifies that RAS approvals shall be effective for 180 days for selection terms reasonably believed to be used by USPs and one year for all other selection terms. However, NSA, out of an abundance of caution, used a more restrictive RAS expiration policy in 2013: 90 days for selection terms used by USPs and 180 days for selection terms used by foreign persons.[27] [redacted] is configured to automatically change the status of RAS selection terms from "Approved" to "Expired" when expiration dates NSA set are exceeded.

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

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

(U//~~FOUO~~) [redacted] is the graphical user interface that analysts use to query data in [redacted] including BR metadata. When launching [redacted] analysts with

[27] (U//~~FOUO~~) [redacted] was reconfigured so that selection terms used by USPs expired in 173 days and 358 for all others. NSA made this change to avoid burdening the FISC, which began approving RAS for selection terms as the President had directed, with more frequent reauthorizations than the BR Order requires.

appropriate credentials have the option to include BR metadata in their queries. If analysts select the

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

~~(TS//SI//NF)~~ When in the mode of analysts may only use a RAS approved selection term to query BR metadata. The term used to initiate a query of BR metadata is referred to as a seed because it is used to produce a "chain" of metadata contacts, known as contact chaining. When analysts submit seed selection terms for querying using another part of middleware called the Emphatic Access Restriction (EAR) checks whether the selection terms appear as "Approved" in the tables.[28] The EAR, through internal software system controls, ensures that contact chaining is restricted to seeds that are RAS approved by preventing non RAS approved selection terms from being used as seeds for conducting call chaining analysis of BR metadata in (e.g., expired, decommissioned, disapproved selection terms, terms that have never been entered into . If selection terms submitted by analysts for querying of BR metadata appear as "Approved" in the tables, the EAR allows queries to perform. The EAR prevents queries from performing when the selection terms do not appear as "Approved."

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

(U//~~FOUO~~) In 2013, the EAR software system controls also restricted the number of hops to three from the seed for contact chaining, as the BR Order authorized.[29] However, if analysts, after reviewing the first two hops results wanted to perform contact chaining out to a third hop from the seed selection term, SID policy required that they first obtain S2 division management approval. NSA relied on analysts to comply with SID policy—no system control was in place to prevent analysts from querying out to three hops without S2 division management approval.

(U//~~FOUO~~) To understand how contact chaining was performed and the system controls implemented by the EAR to only allow querying using RAS approved seeds and within three hops of the seed selection term in 2013, it is helpful to review an example.

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

~~(S//SI//REL TO USA, FVEY)~~ Seed selection term A—reasonably believed to be used by a foreign person was RAS approved by an HMC. No First Amendment review was required because selection term A (the seed) was not used by a U.S. person. The analyst entered selection term A into to perform contact chaining analysis one hop from the seed. The EAR automatically checked the tables to determine whether

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

[28] ~~(TS//SI//NF)~~ NSA implemented the EAR Before then, NSA relied on analytic due diligence to query (BR metadata) with only RAS approved selection terms. After release in June 2010, the EAR was reconfigured to use data from to prevent queries in using selection terms that were not RAS approved, including USP selection terms that OGC had not reviewed.

[29] ~~(TS//SI//NF)~~ On 29 January 2014, NSA modified the EAR software system controls to reduce the number of hops from the seed to two to comply with the President's directive of 17 January 2014.

selection term A was RAS approved. Because it showed as RAS approved, the EAR allowed the query of BR metadata in [redacted] First hop queries returned all selection terms available in the BR repository (and associated metadata) that had a contact or connection with the seed. [redacted] If the analyst tried to query beyond the third hop or query using a selection term that had not been RAS approved, the EAR would have prevented the action.

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

(U) EAR bypass

~~(TS//SI//NF)~~ Because it can take [redacted] for system updates to complete before a RAS approved selection term can be used for querying BR metadata, an EAR bypass was implemented for emergency situations. If an analyst, with a RAS approved seed selection term and S2I4 management approval, determines that immediate querying of BR metadata using the RAS approved seed selection term is necessary to obtain time-sensitive results to respond to an emergency, S2I4 informs designated OGC, SV, and ODOC personnel of its intention to bypass the EAR software system controls. After this notification, S2I4 management contacts the [redacted] team requesting that designated analysts be temporarily added to the [redacted] user group in [redacted] This allows the analysts to select the bypass option in [redacted] thereby bypassing the EAR software system controls for hop restrictions and checks of RAS selection terms against the [redacted] tables. Analysts, with manual checks by direct on-site supervisor oversight, ensure that queries performed in the bypass mode do not exceed three hops (before 17 January 2014) or two hops (on and after 17 January 2014). The [redacted] team is notified when the analysts should be removed from the [redacted] user group in [redacted]—immediately following NSA's response to an emergency situation or after normal system updates have completed to allow querying using the RAS approved selection terms. No NSA personnel were included in the [redacted] user group [redacted]

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

(U) Querying by trained and authorized technical personnel for testing purposes only

~~(S//SI//NF)~~ The BR Order allows authorized NSA technical personnel to access the BR metadata, including through queries, to make it usable for intelligence analysis. This includes performing [redacted] and maintaining records to demonstrate compliance with the BR Order. However, technical personnel do not share the results of these queries with analysts. Tests of BR metadata are performed [redacted] as the BR Order allows. Only a limited number of technical personnel, who appear in the [redacted]

user group in [redacted], can query BR metadata using non RAS approved selection terms in operational databases. The [redacted] user group is used only by technical personnel. SV audits all queries performed using query tools by technical and mission personnel to ensure compliance with the BR Order. [redacted] authorized NSA technical personnel were in the [redacted] user group [redacted]

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

(U) RAS approval process—2014

~~(TS//SI//NF)~~ On 17 January 2014, the President directed that NSA implement changes in how it operates the BR FISA program: NSA must submit selection terms to the FISC for RAS approval and limit contact chaining to two hops from the seed selection terms. Before 17 January 2014, RAS selection terms were approved by the S2I4 Chief or Deputy Chief or one of the twenty authorized HMCs, as the BR Order required, and contact chaining was allowed out to three hops. [redacted] As an added measure, on 23 January 2014, all [redacted] RAS selection terms in an "Approved" status were changed to "Revalidate" in [redacted][30]

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

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

(U//~~FOUO~~) In the weeks following the President's directives, through a motion to amend BR Order 14-01 the FISC approved on 5 February 2014, the following:

> (U) The government may request, by motion and on a case-by-case basis, permission from the Court for NSA to use specific selection terms that satisfy the RAS standard as "seeds" to query the BR metadata to obtain contact chaining information, within two hops of an approved "seed," for purposes of obtaining foreign intelligence information. In addition, the Director or Acting Director of NSA may authorize the emergency querying of the BR metadata with a selection term for purposes of obtaining foreign intelligence information, within two hops of a "seed," if: (1) the Director or Acting Director of NSA reasonably determines that an emergency situation exists with respect to the conduct of such querying before an order authorizing such use of a selection term can with due diligence be obtained; and (2) the Director or Acting Director of NSA reasonably determines that the RAS standard has been met with respect to the selection term. In any case in which this emergency authority is exercised, the government shall make a motion in accordance with this amendment to the BR Primary Order to the Court as soon as practicable, but not later than seven days after the Director or Acting Director of NSA authorizes such query.

(U//~~FOUO~~) In response to these new requirements, the NSA BR control framework changed:

- (U//~~FOUO~~) **RAS approvals submitted to the FISC** NSA no longer approves RAS for selection terms, except in emergency situations. HMCs or the S2I4 Chief or Deputy Chief previously approved RAS. They now perform

[30] ~~(TS//SI//NF)~~ On 17 January 2014, [redacted] selection terms were in an "Approved" status in [redacted] RAS approvals for [redacted] selection terms had expired, and [redacted] automatically changed status from "Approved" to "Revalidate." [redacted] the remaining [redacted] selection terms still in an "Approved" status were changed to "Revalidate" in [redacted]

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

only first level reviews to determine whether RAS requests are adequately documented and supported by creditable source documentation in [redacted] Analysts follow the same preliminary procedures as before for determining whether selection terms are used by persons who are reasonably believed to be associated with one of the terrorist organizations listed in the BR Order and for documenting RAS requests in [redacted] After reviewing the supporting documentation, HMCs send RAS requests back to analysts to make additional changes (as needed), deny RAS requests, or formally endorse them. Only RAS requests endorsed by HMCs are submitted in [redacted] to OGC for second level review (regardless of whether selection terms are used by USPs or foreign persons).

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

(U//~~FOUO~~) OGC no longer officially performs First Amendment reviews of selection terms used by USPs for non-emergency RAS requests; the FISC performs those reviews. OGC now performs second level reviews of RAS requests, source documentation, and endorsement decisions by HMCs to provide greater assurance that the FISC will not reject RAS requests because of insufficient documentation or First Amendment concerns (for selection terms used by USPs). OGC reviews HMC endorsements during RAS verification meetings, at which HMCs present evidence supporting the RAS justifications for review by SV, OGC, and the S2 Declarant (usually the S2I4 Chief or Deputy Chief) who signs the eventual motions seeking FISC approval of the selection terms. This group (known as the "RAS verification panel"), chaired by SV, confirms that representations in RAS requests are accurate. If the RAS verification panel endorses the RAS requests, OGC submits them to DoJ NSD for review and submission to the FISC for approval. At each level of review by HMCs, OGC, the RAS verification panel, and DoJ NSD, all questions, concerns, and requests for additional information must be satisfied before DoJ NSD submits the requests to the FISC.

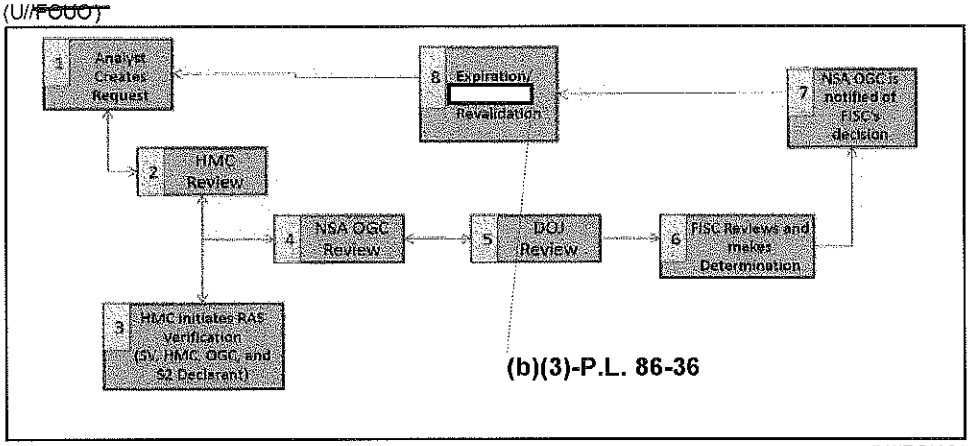
~~(TS//SI//NF)~~ The FISC makes the final determination of whether the RAS standard has been met for each request and notifies DoJ NSD of its decision to approve or disapprove requests. After OGC has been notified by the DoJ NSD of the FISC decision, OGC enters the date of the decision, saves the supporting court documentation, and updates the dispositions of RAS requests in [redacted] as "Approved" or "Disapproved."[31] FISC approvals are effective for 180 days for selection terms used by USPs and one year for all others. However, NSA established slightly more conservative expirations in [redacted] 173 days for selection terms used by USPs and 358 days for all others. Figure 6 illustrates the non-emergency RAS approval process.

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

[31] (U//~~FOUO~~) [redacted] is the system of record for storing documents relating to NSA authorities, including BR Orders for the BR FISA authority.

(U) Figure 6. Non-Emergency RAS Approval Process

(U//~~FOUO~~)



(U//~~FOUO~~)

- (U//~~FOUO~~) **Emergency RAS approvals** Under the BR Order, the NSA Director (DIRNSA) or Acting DIRNSA can approve RAS for selection terms for querying BR metadata within two hops of the seed selection term only after the RAS standard has been met and only when responding to emergencies. When submitting a RAS request for emergency approval, analysts document the request and justification for emergency approval in [redacted] An HMC performs a first-level review and requests additional information from the analysts (as needed) and denies or endorses the emergency RAS request. If the HMC endorses, the RAS verification panel is immediately convened to review the supporting documentation and justification for requesting emergency approval. If the RAS request contains a selection term used by a USP, OGC performs a First Amendment review to determine that the basis for seeking RAS is not solely based on activities protected by the First Amendment. If the RAS verification panel concurs with the HMC's endorsement and OGC concludes that there are no First Amendment concerns, the S2 Declarant, BR FISA Authority Lead, SV, and OGC will brief the DIRNSA or Acting DIRNSA, who determines whether an emergency situation exists, and the RAS standard has been met, and the RAS determination is not based solely on First Amendment protected activities.

  (U//~~FOUO~~) If the DIRNSA or Acting DIRNSA approves the emergency RAS request, OGC saves the approval documentation and changes the disposition of the RAS request to "Approved" in [redacted] and notifies DoJ NSD of the emergency RAS approval. If immediate querying is required, S2I4 coordinates adding the designated analysts to the [redacted] user group in [redacted] (see Querying section for EAR Bypass procedures). Otherwise, the designated analysts must wait [redacted] for a series of system updates to complete before querying BR metadata using the emergency-approved selection term.

  (U//~~FOUO~~) The BR Order requires that, within seven days of the emergency RAS approval, DoJ NSD file a motion with the FISC on behalf of NSA

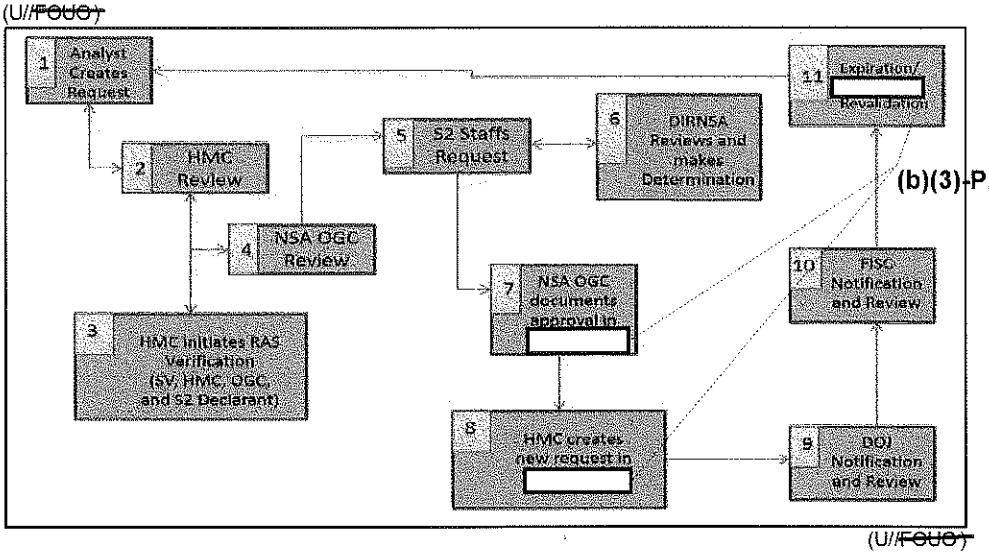
(b)(3)-P.L. 86-36

concerning the emergency authorization. If the FISC grants the motion, OGC enters the date the FISC approved the RAS request and records the supporting court documentation in [redacted] If the FISC denies the motion, NSA will take remedial action, including actions the FISC has directed. Figure 7 illustrates the emergency RAS approval process.

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

(U) Figure 7. Emergency RAS Approval Process

(U//~~FOUO~~)



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

(U//~~FOUO~~)

~~(C//REL TO USA, FVEY)~~ [redacted] the DIRNSA approved the first and only selection term for emergency querying since receiving this new mandate from the FISC on 5 February 2014. A motion was filed with the FISC within seven days of the DIRNSA's approval of the emergency RAS request. [redacted] the FISC approved RAS for the selection term.

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

- (U//~~FOUO~~) **Two-hop restriction for contact chaining** On 29 January 2014, NSA modified the EAR software system controls to restrict contact chaining to two hops from seed selection terms as the President had directed. Before 17 January 2014, authorized NSA analysts could query BR FISA repositories two hops from seed selection terms and one additional hop (three hops from seed selection terms) with S2 division management approval.

(U) Table 16 summarizes the provisions of BR Order 13-158 for querying BR metadata and the controls NSA implemented to maintain compliance.

(U) Table 16. Querying Provisions and Controls

(U//~~FOUO~~)

Provision	Control
Seed selection terms must be approved by a designated approving official and also reviewed by OGC, if the selection term is used by a USP, before querying BR metadata for intelligence analysis purposes.	In 2013, [redacted] controls ensured that one of the 22 designated approving officials approved RAS for selection terms and, if used by USPs, OGC performed a First Amendment review. Selection terms were added to the RAS Approved List only after the required approvals were documented in [redacted]*
Approvals shall be given only after the designated approving official has determined that there are facts giving rise to RAS that the selection term to be queried is associated with a Foreign Power.	[redacted] stores supporting documentation for justifying RAS; it also maintains the authoritative list of [redacted] foreign powers. (b)(3)-P.L. 86-36
NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS approved.	EAR restricts contact chaining to only those seeds that are RAS approved by preventing all non RAS approved selection terms (e.g., expired, disapproved) from being used as seeds for conducting contact chaining.†
RAS approvals must not exceed 180 days for selection terms reasonably believed to be used by a USP and 365 days for all other selection terms.	[redacted] automatically changes the status of RAS approved selection terms from "Approved" to "Expired" when expiration dates set by NSA are exceeded. In 2013, expiration dates were set for 90 days for selection terms associated with USPs and 180 days for all others.‡
Results of contact chaining queries must not exceed three hops from seed selection terms.	In 2013, the EAR limited the number of hops to three from the seed selection term for contact chaining.§
Technical personnel may query the BR metadata using selection terms that have not been RAS approved to perform processes needed to make it usable for intelligence analysis.	SV reviews all query records for compliance with the BR Order.

* (U//~~FOUO~~) On 26 February 2014, NSA began sending RAS requests to the FISC for approval to comply with the President's directive of 17 January 2014. On 28 February 2014, the FISC approved RAS for a selection term under this new process, and NSA began the process of manually entering into [redacted] the dates that the FISC approved RAS for selection terms. [redacted] was updated to require that FISC approval dates be inputted into it before adding selection terms to the RAS Approved List.

† (U//~~FOUO~~) The EAR relies on RAS approved selection terms to be accurately entered by authorized personnel manually into [redacted] In 2014, NSA discovered instances of RAS approved selection terms that were inaccurately entered into [redacted] by authorized personnel. In response, NSA implemented a two-person review for accuracy of RAS approved selection terms manually entered into [redacted]

‡ (U//~~FOUO~~) [redacted] the expiration dates in [redacted] were changed to 173 days for selection terms used by USPs and 358 days for all others.

§ (U//~~FOUO~~) [redacted] the EAR software system controls were modified to limit the number of hops from seed selection terms to two to comply with the President's directive from 17 January 2014.

(U//~~FOUO~~)

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

(U) Sharing and Dissemination

(U) Provisions of BR Order 13-158

(U//~~FOUO~~) **Sharing** Results of intelligence analysis queries of BR metadata may be shared, before minimization, for intelligence analysis among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures for handling and disseminating such information.

(U//~~FOUO~~) **Dissemination** NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of U.S. Signals Intelligence Directive (USSID) SP0018 to any results from queries of the BR metadata, in any form, before the information is disseminated outside NSA in any form. In addition, before disseminating USP information outside NSA, the DIRNSA, the Deputy Director, or one of the officials listed in Section 7.3(c) of USSID SP0018 (i.e., Director of SID, Deputy Director of SID, Chief of Information Sharing Services (S1S), Deputy Chief of S1S, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the USP is related to CT information and it is necessary to understand the CT information or assess its importance ("CT nexus"). Approximately every 30 days, NSA shall file with the Court a report that, among many things, includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain USP information, in any form, with anyone outside NSA.

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

(U) Sharing BR-unique information with authorized NSA personnel

~~(TS//SI//NF)~~ NSA refers to "sharing" as providing query results internally to appropriately trained and authorized NSA personnel. Sharing restrictions in the BR Order only apply to BR-unique query results of a USP. "BR unique" is a term used by NSA that refers to contacts [redacted] within a chain solely derived from BR metadata [redacted] Oral or written depictions, manipulations, and summaries are also query results. Unless already included in a disseminated report, BR-unique query results containing USP information are only shared with individuals who have the [redacted] credential. BR stakeholders manually check [redacted] to confirm that recipients have [redacted] before sharing BR-unique USP information, in any form. BR stakeholders also ensure that documents or files containing BR-unique USP information are only stored in access-controlled, personal or shared network locations accessible only to BR-cleared personnel and that BR-unique results containing USP information displayed in the workplace are not visible to analysts who do not have [redacted]

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

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

[redacted]

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

(U) Disseminating BR-unique information

(U) Dissemination is the sharing of information outside NSA. The BR Order includes two provisions for disseminating information: the CT nexus requirement and the dissemination tracking requirement.

- (U//~~FOUO~~) **CT Nexus Requirement** The CT nexus requirement applies only to disseminations of BR query results containing USP information. The dissemination provisions of Section 7.3(c) of USSID SP0018 must be followed. If query results include USP information unique to BR metadata and the analyst needs to disseminate that information to an external customer, such as the FBI, then the CT nexus requirement must be met before disseminating information in any form. However, if query results contain only foreign person information, the CT nexus requirement does not apply when disseminating BR information. The remainder of this section focuses on disseminating USP information derived from BR-unique metadata.

  ~~(TS//SI//NF)~~ In accordance with USSID SP0018, if unminimized USP information is to be disseminated, one of the designated approval authorities must determine that the information is necessary to understand the foreign intelligence in the report before the information is released. This applies to all disseminations of unminimized USP information under all NSA authorities. The BR Order further requires that one of the approving authorities confirm that the information identifying a USP also relates to CT information and is necessary to understand the CT information or assess its importance. S1S stated that most disseminations of USP information derived from BR metadata

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

(U//~~FOUO~~) There are two categories of BR disseminations: Published disseminations and other disseminations (e.g., oral briefings to recipients external to NSA, such as the FISC, who are not receiving the information as part of their lawful executive or legislative oversight function).

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

  - (U//~~FOUO~~) reports are used to disseminate SIGINT information that responds to special IC requirements reports are disseminated in a limited distribution to customers empowered to act on the information and to additional customers who have an operational need-to-know (e.g., FBI, NCTC, Central Intelligence Agency (CIA), Office of the Director of National Intelligence (ODNI)).

- (U//~~FOUO~~) **RFIs** are requests by customers (e.g., FBI) for information from NSA. RFIs are usually requests requiring one-time, specific responses.
- (U//~~FOUO~~) [redacted] are SIGINT reports that generally focus on one topic or event [redacted] (b)(3)-P.L. 86-36 [redacted] variety of collection authorities to a wide audience. However, [redacted] are not used to disseminate USP information unique to BR metadata [redacted]

(U//~~FOUO~~) After one of the approving authorities listed in Section 7.3(c) of USSID SP0018 has approved the dissemination, if USP information unique to BR metadata is included in an [redacted] it is usually combined with information from other collection authorities to provide a more complete intelligence summary. Otherwise, NSA masks the identities of (b)(3)-P.L. 86-36 USPs mentioned in [redacted] (e.g., USP1), so that the [redacted] can be distributed widely and sends separately an Identities Release Memorandum only to those parts of the IC that need to know the person's identity.[32] Only those recipients within the IC who receive both the [redacted] and Identities Release Memorandum can determine the USP identity, and then only after submitting a formal justified request that has been approved by one of the officials listed in Section 7.3(c) of USSID SP0018.

(U//~~FOUO~~) Dissemination of BR information occurs most often in [redacted] reports. S1S stated that, even when NSA disseminates information using RFIs, corresponding [redacted] reports follow to formally document the dissemination.[33] This allows the information requested by one IC customer, but important to other IC customers, to be released through a slightly wider, albeit highly controlled, distribution. Table 17 summarizes the BR reports disseminated in 2013.

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

[32] (U//~~FOUO~~) Masking is the process of using generic identification terms in place of USP names, titles, or contextual identifiers so that the person's identity is not revealed in written or oral disseminations.

[33] (U//~~FOUO~~) S2I4 confirmed that all RFIs containing BR-unique information have been followed up with [redacted] reports [redacted]

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

(U) Table 17. BR Reports Disseminated in 2013 (b)(1) (b)(3)-P.L. 86-36

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

		RFIs	Other	Total
BR Reports Disseminated*				
Total Selection Terms Reported (Derived from BR				
Total BR Unique Selection Terms Reported†				
Total U.S. Contacts Reported†				

* There were additional disseminations in oral presentations. The NSA Director briefed the SSCI and NSA made a presentation to the FISC

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

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

(U//~~FOUO~~) The S1S Chief or Deputy Chief, two of the approving authorities designated in USSID SP0018, reviews the majority of the requests for disseminating USP information for all NSA authorities, including those unique to BR. Dissemination requests are approved usually the day they are received. Senior Operations Officers (SOO) in the National Security Operations Center (NSOC) are also authorized approvers for disseminating USP information and typically review and approve dissemination requests submitted after hours or in emergency situations.

(U//~~FOUO~~)

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

(U//~~FOUO~~) S1S maintains disseminated reports signed in an access-controlled S1S network folder. Disseminations approved after hours by the SOOs are formally documented, normally the

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

[34] ~~(TS//SI//REL TO USA, FVEY)~~

[35] (U//~~FOUO~~)

following business day, by S1S. The NSOC Senior Reporting Officer notifies S1S of these disseminations.

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

(U//~~FOUO~~) Oral briefings that include USP information derived from BR-unique metadata to officials outside NSA occur less frequently. Normally, these briefings are provided by NSA leadership who are approving authorities for disseminating USP information under USSID SP0018. All other BR stakeholders coordinate approvals with one of the approving authorities before presenting information outside NSA. The CT division tracks oral briefings only, and S1S and S2I4 track all disseminations of USP information (published and oral), which are included in the 30-day reports filed with the FISC, as the BR Order requires.

- ~~(TS//SI//NF)~~ **Dissemination Tracking Requirement** The second provision of the BR Order that applies to USP information is the dissemination tracking requirement regarding BR-unique information. NSA tracks and reports to the FISC every instance in which NSA disseminates USP information derived from BR metadata.[36] Approximately every 30 days, OGC requests from S1S and S2I4 the number of disseminated reports containing USP information derived from BR-unique metadata for input into the 30-day reports filed with the FISC.

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

Although no longer required to track disseminations of foreign person information, S2I4 continues to track all disseminations of BR-unique information. Disseminations were tracked manually until NSA's corporate dissemination tracking tool, was implemented Since then, all disseminated reports containing BR-unique information have been tracked in completed the upload of current and past BR disseminations into

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

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

(U//~~FOUO~~) Table 18 summarizes the provisions of BR Order 13-158 for sharing and disseminating information derived from BR query results and the controls implemented by NSA to maintain compliance.

[36] ~~(TS//SI//NF)~~ Since 3 September 2009 (BR Order 09-13), NSA has been exempt from reporting in the 30-day reports to the FISC BR disseminations to the executive branch for oversight. On 3 January 2014 (the date the FISC approved BR Order 14-01), this reporting exemption was further extended to include BR disseminations to the legislative branch for oversight.

(U) Table 18. Sharing and Dissemination Provisions and Controls (b)(3)-P.L. 86-36

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

Provision	Control
(U) Results of intelligence analysis queries of the BR metadata may be shared, before minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for handling and disseminating such information. (b)(1) (b)(3)-P.L. 86-36	~~(TS//SI//NF)~~ BR stakeholders manually check [redacted] NSA's corporate authorization services tool, to confirm that recipients have [redacted] before sharing BR-unique query results of a USP, in any form. [redacted]
(U) Before disseminating USP information outside NSA, the NSA Director, the Deputy Director, or one of the officials listed in Section 7.3(c) of USSID SP0018 must determine that the information identifying the USP is related to CT information and that it is necessary to understand the CT information or assess its importance.	(U//~~FOUO~~) One of the designated approvers (usually the S1S Chief or Deputy Chief) verifies that the CT nexus has been met before disseminating USP information in any form. The approving documentation is independently maintained by S1S for internal recordkeeping and for external review by overseers.
(U) Approximately every thirty days, NSA shall file with the Court a report that among many things includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of BR metadata that contain USP information, in any form, with anyone outside NSA.	(U//~~FOUO~~) S1S and S2I4 independently track the number of disseminations since the preceding report in which NSA has shared, in any form, results from queries of BR metadata that contain USP information, in any form, with anyone outside NSA. ST tracks oral disseminations only. This data collectively is provided to OGC for input into the 30-day reports filed with the FISC.

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

(U) Retention

(U) Provisions of BR Order 13-158

(U) The BR Order requires that BR metadata be destroyed no later than five years (60 months) after its initial collection.

(U) NSA's BR age-off process (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ To remain compliant with the five year retention requirements, NSA completed its first BR age-off [redacted] May 2011. [redacted]

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

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

(U//~~FOUO~~) Based on guidance from OGC, BR retention compliance is determined using the date when records are received from providers, not the call communication date.

- (U//~~FOUO~~) **Record receipt date** is the date on which providers electronically deliver BR metadata to NSA.
- (U//~~FOUO~~) **Call communication date** is the date on which a telephone call is made from one selection term to another.[38]

(U) Timing differences with call communication dates and record receipt dates

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

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

Because of these differences, NSA tracks record receipt dates for BR metadata to document compliance with the BR Order.

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

(U) Quarantine process

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

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

[37] (U//~~FOUO~~) In September 2013, the DoJ Civil Division directed NSA to preserve all records relating to the collection of BR metadata under the BR FISA program as a result of civil lawsuits against NSA. To comply with the preservation order, NSA did not age-off data with record receipt dates exceeding 60 months in 2014. This data was saved in partitions within NSA system repositories inaccessible to analysts.

[38] (U) Selection terms also refer to identifiers used in dialed number recognition (e.g., telephone numbers).

(U) 2013 age-off

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

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

(U//~~FOUO~~) Table 19. 2013 BR Age-Off Procedures

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

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

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

(U) Changes that affected the 2014 age-off

(U//~~FOUO~~) In September 2013, DoJ's Civil Division directed NSA to preserve all records relating to the collection of BR metadata under the BR FISA program as a result of civil lawsuits against NSA. This affected the age-off performed during 2014: BR metadata that would have been aged off to comply with the BR Order was

retained to comply with the preservation obligation. This data was saved in partitions within NSA system repositor ies inaccessible to analysts.

(U//~~FOUO~~) On 12 March 2014, the FISC granted the government's motion for temporary relicf from the five year destruction requirement pending resolution of the preservation litigation filed by plaintiffs.[39] As permitted by the BR Order, analysts continue to access for intelligence purposes the repository that contains BR metadata received on or after the 2010 retention cutoff date using only RAS approved selection terms.

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

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

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

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

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

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

~~(C//REL TO USA, FVEY)~~ Table 20. [redacted] (b)(1) (b)(3)-P.L. 86-36

(before and after data comparison)

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

[redacted]

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

(U//~~FOUO~~) Table 21 summarizes the provision of BR Order 13-158 for retention and the control implemented by NSA to maintain compliance.

(U) Table 21. Retention Provision and Control

(U//~~FOUO~~)

Provision	Control
BR Metadata must be destroyed no later than five years after its initial collection.	See Table 19 for the procedures performed to age-off BR metadata to comply with the BR Order in 2013.

(U//~~FOUO~~)

(U) Oversight

(U) Provisions of BR Order 13-158

(U) NSA's OGC and ODOC will ensure that personnel with access to BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC will further ensure that all NSA personnel who receive query results in any form first

receive appropriate and adequate training and guidance regarding the procedures and restrictions for handling and disseminating such information. NSA will maintain records of all such training. OGC will provide DoJ NSD with copies of all formal briefing and/or training materials (including all revisions) used to brief/train NSA personnel concerning this authority.

(U) NSA's ODOC will monitor implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced in the previous paragraph.

(U) NSA will ensure that an auditable record is generated whenever BR metadata is accessed for foreign intelligence analysis or accessed using foreign intelligence analysis query tools.

(U) NSA's OGC will consult with DoJ NSD on all significant opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation will occur in advance; otherwise, DoJ NSD will be notified as soon as practicable.

(U) At least once during the authorization period, NSA's OGC, ODOC, DoJ NSD, and any other appropriate NSA representatives will meet for the purpose of assessing compliance with the Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority.

(U) At least once during the authorization period, DoJ NSD will meet with the NSA's OIG to discuss their oversight responsibilities and assess NSA's compliance with the Court's orders.

(U) At least once during the authorization period, NSA's OGC and DoJ NSD will review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.[40]

(U) NSA oversight

(U//~~FOUO~~) In addition to the oversight requirements listed in the BR Order, NSA performs additional oversight, not required in the Order, to ensure compliance. The organizations and the oversight performed are described next.

(U//~~FOUO~~) **BR FISA Authority Lead** is the focal point for the BR FISA program within SID, reporting to the CT Associate Deputy Director, who reports to the SID Director. The BR FISA Authority Lead's responsibilities include:

[40] (U//~~FOUO~~) As of 28 March 2014 (BR Order 14-67), the FISC no longer required OGC and DoJ NSD to conduct periodic reviews of RAS approved selection terms. The government sought this change as a result of the President's directive of 17 January 2014 that NSA submit selection terms to the FISC for RAS approval.

- (U//~~FOUO~~) Chairing weekly BMD meeting
- (U//~~FOUO~~) Ensuring appropriate program direction and proper program functioning
- (U//~~FOUO~~) Signing NSA's declarations to the FISC during renewal and
- (U//~~FOUO~~) Ensuring that the BR authority is used as described in the BR Order.

(U//~~FOUO~~) Weekly BMD meetings are held to discuss BR FISA program activities to ensure compliance with the BR Order. They include representatives from OGC, ODOC, TV, SV, GTO, DIAs, TD, Counterterrorism Production Center (S2I), OIG, and other organizations involved in the BR FISA program. Agendas and notes are maintained for each meeting.

(U//~~FOUO~~) **Authorities Integration Group (AIG)** reports directly to the Deputy DIRNSA. The AIG works directly with SID and Information Assurance Directorate authority leads, including the BR FISA Authority Lead, and holds weekly meetings with the authority leads and corporate process leads (e.g., TD, ODOC, OGC).

(U//~~FOUO~~) The AIG focuses on the activities for each authority, both internal and external, to ensure that they are coordinated and integrated across NSA. The AIG acts as a "forcing function" within NSA, facilitating discussion among the Directorates to promote a better understanding of how decisions affect the various authorities. The AIG updates the Deputy DIRNSA quarterly on each authority.

(U) **ODOC** In 2009, NSA created the position of Director of Compliance to improve the Agency's ability to keep NSA's activities consistent with the laws, policies, and procedures designed to protect USP privacy during SIGINT and information assurance missions. ODOC has specific functions with the BR FISA program outlined in the Order. The Assistant Director for Special Compliance Activities is ODOC's representative to the BR FISA program. Some of ODOC's responsibilities include:

- (U) Involvement in all decisions related to the program,
- (U) Participating in weekly BMD meetings,
- (U) Updating BR FISA program training material,
- (U) Participating in quarterly compliance meetings with DoJ NSD, and
- (U) Leading the verification of accuracy (VoA) process.

(U//~~FOUO~~) The BR FISA program has been designated a special compliance activity (SCA) since 2009, that is, an NSA mission activity determined to require additional tailored compliance safeguards to ensure the protection of USP privacy. When an activity is identified as an SCA, ODOC becomes active in all aspects of implementing the SCA until it is determined that it is sufficiently underpinned by the Comprehensive Mission Compliance Program and significant risks have been

mitigated. The Comprehensive Mission Compliance Program provides a framework and strategy to organize, govern, and resource compliance activities across NSA.

(U//~~FOUO~~) An activity may become an SCA when:

- (U//~~FOUO~~) NSA's external overseers (e.g., DoJ NSD, FISC, Congress) have a heightened sensitivity about an activity or the means by which NSA is executing an activity;
- (U//~~FOUO~~) NSA's legal, policy, compliance, or oversight elements determine that an activity requires attention to understand the application of compliance measures and potential risks; or
- (U//~~FOUO~~) NSA identifies an activity or process that may be out of sync with oversight and compliance regulations and policies, thus making NSA vulnerable to compliance incidents.

(U//~~FOUO~~) Recognizing the critical importance of the completeness and accuracy of documentation filed with external entities, ODOC developed line-by-line accuracy procedures, known as VoA. These procedures provide greater assurance that the representations NSA made to external overseers are accurate and based on a shared understanding among operational, technical, legal, policy, and compliance officials. NSA uses the VoA process during the application process to the Court when requesting renewal of the BR Order.

(U//~~FOUO~~) **OGC** has specific functions with the BR FISA program outlined in the Order. One requirement is that the OGC consult with DoJ NSD on all significant opinions that relate to the interpretation, scope, or implementation of the authority. The lead OGC BR attorney, assigned from January 2013 to September 2014, stated that OGC consults with DoJ NSD on all significant opinions. OGC saves all correspondence discussing significant legal opinions with DoJ NSD in an access-controlled network folder.

(U//~~FOUO~~) In 2013, NSA OGC met with DoJ NSD at least once during each BR authorization period to review a sample of the justifications for RAS approvals for selection terms used to query BR metadata. However, as of 28 March 2014 (BR Order 14-67), the FISC no longer required OGC and DoJ NSD to conduct periodic reviews of RAS approved selection terms. The government sought this change as a result of a January 2014 presidential directive under which NSA began submitting selection terms to the FISC for RAS approval.

(U//~~FOUO~~) In addition to the OGC's oversight requirements listed in the Order, the OGC defined its BR FISA program responsibilities as:

- (U//~~FOUO~~) Addressing all legal questions from BR FISA program stakeholders;
- (U//~~FOUO~~) Coordinating all interaction with DoJ NSD;

- (U//~~FOUO~~) Coordinating the filing of 30-day reports and renewal documents;
- (U//~~FOUO~~) Leading quarterly compliance reviews with DoJ NSD;
- (U//~~FOUO~~) Performing First Amendment reviews for USP RAS approval (before 17 January 2014);
- (U//~~FOUO~~) Coordinating RAS requests and submitting them to DoJ NSD for approval by the FISC (on and after 17 January 2014); and
- ~~(TS//SI//NF)~~ Approving, with SV, additions of [redacted] to the [redacted] List.

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

(U//~~FOUO~~) **SV** implements the SIGINT compliance program across NSA, particularly within SID, enabling the SIGINT mission to operate in compliance with laws, policies, and other guidance. SV provides guidance across the global SIGINT enterprise, manages compliance incidents, monitors compliance in high-risk areas, resolves problems, and verifies compliance through site visits, audits, and managing the SIGINT Intelligence Oversight Officer program.

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

~~(TS//SI//NF)~~ SV performs two main oversight functions for the BR FISA program: (1) managing access by verifying training requirements semi-weekly for persons who have the [redacted] credential and for persons included in the FISABR user group in [redacted] and (2) auditing all BR queries performed using query tools by mission and technical personnel to verify compliance with the requirements of the BR Order. SV's process for verifying training and managing access can be found in the Access and Training section.

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

~~(TS//SI//NF)~~ As the BR Order requires, whenever BR metadata is accessed for foreign intelligence analysis or accessed using foreign intelligence analysis query tools, an auditable record of activity is generated. Although not required by the BR Order, NSA audits all query records. SV verifies that only authorized personnel with the required credentials queried BR metadata, selection terms used to query BR metadata for intelligence analysis were RAS approved at the time of the query, and queries for intelligence analysis remained within the authorized number of hops from RAS approved seeds, as the BR Order requires. For the last two checks, SV verifies manually that the EAR software system controls are working as intended. SV stated that it has never found an instance of the EAR [redacted] allowing a non-compliant query to complete. In 2013, SV audited all [redacted] BR query records for that year.

(b)(3)-P.L.

(U) Additional SV responsibilities include:

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

- (U) Ensuring that SID incident reports are entered timely into NSA's corporate incident reporting database
- (U) Assisting in the development of oversight and compliance courses
- ~~(TS//SI//NF)~~ Providing BR query statistics and [redacted] credentialing data for monthly metrics reports provided to SID leadership

- (U//~~FOUO~~) Maintaining the content and access to the SV BR SharePoint site for storing BR FISA program documentation
- (U//~~FOUO~~) Performing VoA for statements assigned to SV in the BR Declarations and
- ~~(TS//SI//NF)~~ Approving, with OGC, additions of [redacted] to the [redacted] List.

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

(U//~~FOUO~~) In 2013, SV also assisted DoJ NSD in its periodic review of RAS approved selection terms used for querying BR metadata. SV provided DoJ NSD with RAS justifications and supporting documentation for each review. As previously mentioned in the OGC Oversight section, the periodic reviews of RAS approved selection terms were discontinued pursuant to BR Order 14-67, 28 March 2014.

(U//~~FOUO~~) **TV** is responsible for identifying, assessing, tracking, and mitigating compliance risks, including USP privacy concerns, in NSA mission systems across the extended enterprise, including systems that hold BR metadata. TV manages the system compliance certification process, continuous compliance monitoring, and technical compliance incident management and conducts training and awareness for technical personnel. TV attends the BMD weekly meetings and performs VoAs for areas assigned to it in the BR Declarations.

(U//~~FOUO~~) **OIG** conducts audits, special studies, inspections, investigations, and other reviews of programs and operations of NSA and its affiliates. OIG oversight includes:

- (U//~~FOUO~~) Performing audits and special studies of the BR FISA program;
- (U//~~FOUO~~) Meeting with DoJ NSD at least once during each BR authorization period to discuss oversight responsibilities, NSA's compliance with the BR Order, the status of OIG reviews, and important developments affecting the BR FISA program (notes from these meeting are documented in [redacted]; (b)(3)-P.L. 86-36
- (U//~~FOUO~~) Receiving notification of incident reports for all NSA authorities, including BR FISA, saved in the Agency's corporate incident reporting database;
- (U//~~FOUO~~) Reviewing Congressional Notifications and notices filed with the FISC of incidents of non-compliance with the BR Order;
- (U//~~FOUO~~) Preparing Intelligence Oversight Quarterly Reports, in coordination with the DIRNSA and OGC, that summarize compliance incidents for all authorities occurring during quarterly review periods and forwarding the reports to the President's Intelligence Oversight Board through

the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))[41];

- (U//~~FOUO~~) Performing IO reviews during OIG inspections of joint and field sites;
- (U//~~FOUO~~) Attending weekly BMD meetings for situational awareness;
- (U//~~FOUO~~) Maintaining the OIG Hotline and responding to complaints of violations of law, rule, or regulation (the OIG also investigates allegations of SIGINT misuse by NSA affiliates operating under the DIRNSA SIGINT authority); and
- (U//~~FOUO~~) Reporting immediately to the ATSD(IO) a development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the IC or otherwise call into question the propriety of an intelligence activity.

(U//~~FOUO~~) The OIG reviews management controls, maintains awareness of compliance incidents, and stays informed of changes affecting NSA authorities, including BR FISA. OIG reviews of the BR FISA program allow it to independently assess compliance with the BR Order. Since 24 May 2006, the date the original BR Order was signed, the OIG has completed five BR FISA program reviews. Table 22 summarizes OIG reviews of the program.

(U) Table 22. OIG Reviews of the BR FISA program

(U//~~FOUO~~)

Date Issued	OIG Review	Scope of the Review
09/05/06	Assessment of Management Controls for Implementing the FISC Order: Telephony BR (ST-06-0018)	Reviewed collection, processing, analysis, dissemination, and oversight controls.
05/12/10	NSA Controls for FISC BR Orders (ST-10-0004)	Reviewed querying and dissemination controls; summarized pilot test results for January through March 2010.
05/25/11	Audit of NSA Controls to Comply with the FISC Order Regarding BR (ST-10-0004L)*	Reviewed querying and dissemination controls; summarized the monthly test results for 2010.
10/20/11	Audit of NSA Controls to Comply with the FISC Order Regarding BR Retention (ST-11-0011)	Verified age-off of BR FISA metadata in 2011 to maintain compliance with the 60 month retention requirement of the BR Order.
08/01/12	NSA Controls to Comply with the FISC Order Regarding BR Collection (ST-12-0003)	Reviewed collection and sampling controls for ensuring that NSA receives only the BR FISA metadata authorized by the BR Order.
* (U//~~FOUO~~) This report summarized monthly test results of the BR querying and dissemination controls during 2010.		

(U//~~FOUO~~)

[41] (U//~~FOUO~~) In 2014, the ATSD(IO) was changed to the Office of the Senior DoD Intelligence Oversight Official.

(U) External oversight

(U) **DoJ NSD** is the liaison between NSA and the FISC for the BR FISA program. DoJ NSD oversight includes the following:

- (U) Coordinating 90-day renewal applications
- (U//~~FOUO~~) Providing guidance to NSA OGC on all significant legal opinions relating to the interpretation, scope, and implementation of the BR authority
- (U//~~FOUO~~) Reviewing NSA briefings and training transcripts to ensure that they accurately describe the requirements of the BR Order before NSA incorporates material into its training program (e.g., OVSC1205, OVSC1206)
- (U//~~FOUO~~) Meeting with NSA's OIG at least once during each BR authorization period to discuss oversight responsibilities and NSA compliance with the BR Order. Proposed initiatives and other important developments affecting the BR FISA program are discussed with the OIG
- (U) Meeting with NSA's OGC, ODOC, and other NSA stakeholders at least once during BR authorization periods to assess compliance. DoJ NSD meets with OGC, ODOC, and the BR FISA Authority Lead to review the Quarterly Compliance Report that summarizes the results of weekly tests NSA performed to ensure that NSA is receiving only authorized data. DoJ NSD submits summaries of these meetings in writing to the FISC as part of applications to renew the authority.

~~(TS//SI//NF)~~ In 2013, DoJ NSD met with NSA OGC and SV at least once each BR authorization period to review a sample of the justifications for RAS approvals for selection terms used to query BR metadata. For RAS selection terms approved in 2013, DoJ NSD sampled 100 percent of the USP RAS selection terms and 20 percent of the foreign RAS selection terms. As mentioned in the OGC Oversight section, DoJ NSD and OGC's periodic reviews of RAS selection terms were discontinued pursuant to BR Order 14-67, dated 28 March 2014. NSA now submits selection terms to the FISC for RAS approval to comply with the President's January 2014 directive. Table 23 summarizes DoJ NSD sampling of RAS selection terms approved in 2013.

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

(U//~~FOUO~~) Table 23. DoJ NSD Sample of RAS Selection Terms Approved in 2013

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

Domestic Selection Terms			Foreign Selection Terms			Total Approved by NSA in 2013†
NSA Approved	DoJ NSD Reviewed	% Reviewed	NSA Approved	DoJ NSD Reviewed*	% Reviewed	
		100%			20%	

* (U//~~FOUO~~) Estimate calculated using DoJ NSD sampling methodology (sample 20 percent of foreign selection terms for review).

† (U//~~FOUO~~) Data includes RAS selection terms that may have been approved more than once in 2013.

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

(U//~~FOUO~~) **ODNI** representatives attend DoJ NSD meetings with NSA's OGC, ODOC, and the BR FISA Authority Lead to review the Quarterly Compliance Report. Although ODNI does not have a formal role described in the BR Order, it participates in its general role as an overseer of IC activities.

~~(C//REL TO USA, FVEY)~~ **FISC** is the approving authority for all renewals, amendments, reinstatements of the BR authority, and, starting in February 2014, RAS for selection terms NSA submitted. The FISC approves the BR Primary Orders that authorize NSA to acquire bulk BR FISA metadata and the BR Secondary Orders that compel providers to provide daily bulk BR FISA metadata to NSA for the duration of the Order. The FISC performs oversight by receiving filings of Rule 13(a) Notices, Correction of Material Facts, and Rule 13(b) Notices, Disclosure of Non-Compliance, by DoJ NSD on behalf of NSA. The FISC also reviews the 90-day renewal applications and 30-day reports that NSA files. The 30-day reports document NSA application of the RAS standard (no longer applies after March 2014); NSA's implementation and operation of the automated query process (no longer applies after March 2014—NSA never implemented the process and withdrew its request to do so); NSA's description of significant changes in the way in which the BR metadata is received from providers and significant changes to the controls NSA has in place to receive, store, process, and disseminate BR metadata; and the number of instances since the preceding report that NSA disseminated, in any form, USP information outside NSA. The 30-day reports also include NSA's attestation that the CT nexus was completed and disseminations were approved by a designating approving authority before disseminating USP information derived from BR-unique metadata.

(U) Table 24 summarizes the provisions of BR Order 13-158 for oversight and the controls implemented by NSA to maintain compliance.

(U) Table 24. Oversight Provisions and Controls

(U//~~FOUO~~)

Provision	Control
NSA's OGC and ODOC will ensure that personnel with query access to BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata.	See Table 14 – Access and Training Provisions and Controls.
NSA's OGC and ODOC will ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.	
NSA will maintain records of all such training.	
OGC will provide DoJ NSD copies of all formal briefing and training materials (including all revisions) used to train NSA personnel concerning the authority.	

NSA's ODOC will monitor implementation and use of software and other controls (including user authentication services) and the logging of auditable information referenced above.	SV performs 100 percent audits of queries performed using query tools by mission and technical personnel to verify that only authorized personnel who have the required credentials queried BR metadata, selection terms used to query BR metadata for intelligence analysis purposes were RAS approved at the time of the query, and queries for intelligence analysis purposes remained within the number of authorized hops from RAS approved seeds.
NSA's OGC will consult with DoJ NSD on all significant opinions that relate to the interpretation, scope, and/or implementation of this authority.	NSA OGC confirmed that NSA has always consulted with and received advance approval from DoJ NSD and the FISC before implementing significant changes to the BR FISA program. NSA OGC saves all correspondence with DoJ NSD in an access-controlled network folder.
At least once during the authorization period, NSA's OGC, ODOC, DoJ NSD, and any other appropriate NSA representatives will meet to assess compliance with the Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is acquired. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority.	DoJ NSD meets with OGC, ODOC, and the BR Lead to review the Quarterly Compliance Report, which summarizes the results of weekly tests performed by NSA to ensure that it is receiving only the BR metadata authorized by the Order. DoJ NSD submits summaries of these meetings in writing to the FISC as part of the applications to renew the authority. **(b)(3)-P.L. 86-36**
At least once during the authorization period, DoJ NSD will meet with the NSA's OIG to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.	NSA OIG meets with DoJ NSD at least once during BR authorization periods to discuss oversight responsibilities and NSA's compliance with the requirements of the Order. Notes from these meeting are documented in [redacted]
At least once during the authorization period, NSA's OGC and DoJ NSD will review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.	In 2013, NSA OGC and SV met with DoJ NSD at least once during BR authorization periods and review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.*
* As of 28 March 2014 (BR Order 14-67), the FISC no longer required OGC and DoJ NSD to conduct periodic reviews of RAS approved selection terms. The government sought this change as a result of the President's January 2014 directive under which NSA began submitting selection terms to the FISC for RAS approval.	

(U//~~FOUO~~)

(U) BR FISA Program Incidents of Non-Compliance

(U//~~FOUO~~) FISC Rules of Procedure require that NSA report "corrections of material facts" and "disclosures of non-compliance" with FISC Orders. NSA also must determine whether Congressional notifications are required. Our review focused on the process for identifying and reporting incidents of non-compliance, the incidents reported in 2013 to the Court and other external overseers, and the controls NSA has instituted to mitigate recurrence of compliance incidents.

(U) FISC Rules of Procedure

(U) The FISC Rules of Procedure, 1 November 2010, adopted pursuant to 50 U.S.C. § 1803(g), govern FISC proceedings. Rule 13, *Correction of Misstatement or Omission; Disclosure of Non-Compliance*, is the procedure that NSA follows when notifying the Court, through DoJ NSD, of BR FISA misstatements and compliance incidents.

(U) **Rule 13(a) Correction of Material Facts** If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the governme nt must immediately, in writing, inform the Judge to whom the submission was made of:

(1) (U) the misstatement or omission;
(2) (U) necessary corrections;
(3) (U) the facts and circumstances relevant to the misstatement or omission;
(4) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
(5) (U) how the government proposes to dispose of or treat information obtained as a result of the misstatement or omission.

(U) **Rule 13(b) Disclosure of Non-Compliance** If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government must immediately, in writing, inform the Judge to whom the submission was made of:

(1) (U) the non-compliance;
(2) (U) the facts and circumstances relevant to the non-compliance;
(3) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
(4) (U) how the government proposes to dispose of or treat information obtained as a result of the non-compliance.

(U) Identifying and Reporting Incidents of Non-Compliance

(U) Identifying incidents of non-compliance

(U//~~FOUO~~) NSA typically discovers incidents of non-compliance with the BR Order during its operation of the BR FISA program. Because of the program's sensitivity, suspected anomalies are reported out of an abundance of caution. Training, a pillar of the compliance framework, provides a heightened sense of awareness for personnel to identify potential violations of the BR Order. A second pillar, monitoring and assessment, includes manual and technical controls to detect abnormalities. A weekly BMD meeting, attended by BR FISA program stakeholders, provides a forum for addressing potential problems.

(U//~~FOUO~~) When a possible incident is discovered, it is communicated to the BR FISA Authority Lead, OGC, ODOC, SV, and, if appropriate, TV and S2. BR FISA program stakeholders meet to discuss the facts and determine, with OGC's concurrence, whether a potential violation of the Order has occurred. If OGC believes an incident has or may have occurred, even if all the facts have not been

gathered, preliminary notification to DoJ NSD is made shortly after notice to the DIRNSA, other NSA leadership, BR FISA program stakeholders, and OIG. Upon receiving initial notification from OGC, DoJ NSD starts drafting a preliminary notification to the Court.

(U//~~FOUO~~) Once the facts have been gathered and OGC has made an initial determination that a violation of the BR Order has occurred, OGC finalizes a notification of non-compliance and forwards it to DoJ NSD, which makes the final determination as to whether there has been an incident of non-compliance that must be reported to the FISC. If DoJ NSD determines that an incident has occurred, it prepares a draft notification to the Court, coordinates the notification with NSA, finalizes the draft, and files the notification with the Court.

(U//~~FOUO~~) DoJ NSD often files a preliminary notification with the Court and, if needed, will follow up later with additional notifications. In some cases, the preliminary notification of an incident serves as the final notice. More than one notice to the Court to address an incident is typically required when at the time of the preliminary notification:

- (U//~~FOUO~~) NSA does not have all the facts the Court needs to fully understand or address the incident or
- (U//~~FOUO~~) Remedial follow-on action may be needed.

(U//~~FOUO~~) For the four incidents of non-compliance first reported to the Court in 2013, two required additional information; therefore, final notices were filed separately. One of the incidents included a notice of material misstatement because NSA had previously filed a declaration to the Court that contained inaccurate information.

(U) Congressional notifications

(U//~~FOUO~~) In addition to the requirement to notify the FISC, DIRNSA has a statutory obligation to keep the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence fully and currently informed of all significant intelligence activities.[42] NSA resolves doubts about notification in favor of notification. In addition to notifying Congress and the Director of National Intelligence (DNI), DIRNSA must notify the Undersecretary of Defense for Intelligence (USD(I)) and other USD(I) staff, as USD(I) guidance directs. For all BR FISA incidents of non-compliance reported by Congressional notifications to the intelligence committees, NSA also notifies the Senate and House Committees on the Judiciary.

(U//~~FOUO~~) NSA's Legislative Affairs Office (LAO) manages NSA's liaison with the Congress and DNI, DoD, the IC, and other U.S. government departments and agencies regarding matters of concern to the Congress. LAO is NSA's focal point for

[42] (U) See 50 U.S.C. §3091, as implemented by Intelligence Community Directive 112, *Congressional Notification*, 16 November 2011.

Congressional inquiries, correspondence, questions for the record, and RFIs directed to NSA.

(U//~~FOUO~~) NSA Policy 1-33, *Relations with the Congress*, 22 July 2005, provides guidelines for identifying matters that OGC and LAO must consider reporting to the Congressional intelligence committees under 50 U.S.C. §§3091 and 3092. The guidelines do not constitute a comprehensive list of what must be reported. Compliance incidents are assessed under a general guideline to consider for reporting matters that the intelligence committees have expressed a continuing interest in or which otherwise qualify as significant intelligence activities or failures.

(U//~~FOUO~~) NSA works to keep Congressional intelligence committees fully and currently informed about the Agency's activities, more than what is required under the guidelines outlined in NSA/CSS Policy 1-33.

(U//~~FOUO~~) OGC's analysis of the incidents of non-compliance that occurred in the BR FISA program in 2013 resulted in three of the four incidents reported as Congressional notifications.

(U) 2013 Incidents of Non-Compliance

(U//~~FOUO~~) In 2013, NSA reported four incidents of non-compliance to the Court. The following are NSA's reports of the incidents and the actions NSA took to mitigate recurrence.

~~(TS//SI//NF)~~ Notice of Compliance Incident, [redacted] **(b)(3)-P.L. 86-36**

~~(TS//SI//NF)~~ [redacted] *an NSA analyst conducted a query of the BR metadata with a RAS approved U.S. person selection term (the U.S. person is currently subject to Court-authorized electronic surveillance* [redacted] *The query yielded* [redacted] *new identifiers believed to be used by the same U.S. person as the selection term. The analyst then sent those* [redacted] *U.S. person identifiers, for further tasking, to an e-mail alias that included NSA personnel who had not completed the required BR metadata training to receive query results containing U.S. person information. The analyst also entered the* [redacted] *identifiers into certain analytic and tasking tools to which NSA personnel without the required BR metadata training have access.* **(b)(1) (b)(3)-P.L. 86-36**

~~(TS//SI//NF)~~ *The same day, the analyst's NSA supervisor realized that the* [redacted] *U.S. person identifiers had been shared, within NSA, with analysts who had not received the training required to receive them. The supervisor took steps to immediately detask the identifiers, delete them from the analytic tools, and recall the e-mail message, processes which had been successfully completed on or about March 22, 2013. The analytic and tasking tools had returned no collection or results, and a follow-up e-mail was sent to all addresses on the e-mail alias instructing that anyone without the required training should destroy all copies of the original e-mail sent to the alias.*

(U//~~FOUO~~) OGC determined that no Congressional notification was required for this incident.

~~(TS//SI//NF)~~ **Controls put in place to mitigate recurrence** The BR Order requires that results of queries of BR metadata may be shared among NSA analysts for intelligence analysis before minimization, subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for handling and disseminating such information. Analysts who run queries and obtain results on BR metadata receive annual OVSC1205 training regarding the rules and restrictions on sharing BR metadata query results. Before analysts share BR-derived query results containing USP information, they must confirm that the recipient has the [redacted] credential to receive BR metadata information. Analysts are reminded to verify recipient's credentials [redacted] To help mitigate recurrence, the analyst's supervisor reiterated to the analyst the requirements for sharing BR metadata query results and the portions of the OVCS1205 training related to sharing.

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

~~(TS//SI//NF)~~ Notice of Compliance Incident [redacted]

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

~~(TS//SI//NF)~~ [redacted] *NSA technical personnel discovered that NSA had inadvertently retained files containing call detail records that were more than five years old. Specifically, these call detail records, which had been produced pursuant to the Court's Primary Orders,* [redacted] *These call detail records were among those used in connection with a migration of call detail records to a new system* [redacted] *See Declaration, Docket Number BR 11-57 at 13 n.8 (describing migration of records to a replacement system). The call detail records could be accessed or used by only technical personnel who had received appropriate and adequate training to access call detail records.*

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

~~(TS//SI//NF)~~ [redacted] *NSA technical personnel destroyed the call detail records used in the migration of records that had been inadvertently retained past the retention limit of five years. As a result of the destruction, NSA is unable to provide an estimate regarding the volume of data destroyed. For recovery back-up purposes, NSA has retained those call detail records used in the migration of records that did not exceed the retention limit, and will use those records in accordance with the requirements of the Court's Primary Orders.*

~~(TS//SI//NF)~~ On 7 May 2013, NSA submitted a Congressional notification of the compliance incident to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary. Copies were also provided to Congressional affairs offices at the ODNI, USD(I), and DoJ. On 7 May 2013, the NSA OIG notified the ATSD(IO) of the incident and Congressional notification.

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

~~(TS//SI//NF)~~ **Controls put in place to mitigate recurrence** In response to this incident, technical personnel developed a script that searches for ingest and backup files in [redacted] servers containing BR metadata older than four years, 11 months. Before the preservation order, if such files were identified, the script would send automated reminders weekly for three weeks and then daily until the files had been

manually deleted.[43] No files matching the criteria have been identified since the script was developed. Before the preservation order, the [redacted] database, which ingests files from the [redacted] servers, automatically deleted files before they reached the five-year mark. NSA maintains location restrictions for machines and directories that hold BR metadata files.

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

~~(TS//SI//NF)~~ Notice of Compliance Incidents. [redacted]

~~(TS//SI//NF)~~ **Preliminary** [redacted] *NSA informed the NSD's Office of Intelligence (OI) that, in the course of reviewing its formal reporting to the FISC, it had identified BR metadata products containing U.S. person information that it had not reported in thirty-day reports to the Court. These disseminations* [redacted] *For each BR metadata product, an authorized official made the required CT determination prior to dissemination. NSA and OI continue to investigate the facts and circumstances concerning this matter and the DoJ will provide a thorough explanation of this matter to the Court.*

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

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

~~(TS//SI//NF)~~ **Final** [redacted] *final notice of Compliance Incidents,* [redacted] *was filed with the Court. The notice indicated that the disseminations* [redacted] *in total—were not included in the thirty-day reports because at the time the incidents occurred* [redacted] *NSA relied on a single individual to keep reports of disseminations that occurred during each reporting period and to provide information about those disseminations for inclusion in the thirty-day reports. Inadvertently, the disseminations described above were not recorded and, as result, information about them was not included in the thirty-day reports. Currently, as discussed in a notice in this matter filed with the Court* [redacted] *NSA's Information Sharing Services (ISS) office maintains records of the CT determinations for each disseminated BR metadata product containing U.S. person information. NSA's ISS now also verifies the accuracy of statements regarding disseminations that are included in each thirty day report by confirming that its records reflect the number of disseminations described in each report.*

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

~~(TS//SI//NF)~~ Along with the final notice, a supplemental report to the Court provided additional details and NSA's attestation that, before dissemination, the USP information was determined to be related to CT information and necessary to understand the CT information or to assess its importance.

~~(TS//SI//NF)~~ On 20 September 2013, NSA submitted a Congressional notification of the compliance incident to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary. Copies were also provided to the Congressional affairs offices at ODNI, USD(I), and DoJ. On 12 September 2013, the NSA OIG notified the ATSD(IO) about the incident and pending Congressional notification.

[43] (U//~~FOUO~~) On 21 March 2014, the U.S. District Court for the Northern District of California issued a preservation order against the destruction of BR metadata

~~(TS//SI//NF)~~ **Controls put in place to mitigate recurrence** In response to this incident, [redacted] NSA issued the "BR FISA Reporting Process SOP" that documents external reporting requirements and organizational responsibilities and defines a standardized, repeatable process for the creation, coordination, and release of mandatory FISC reports for the BR FISA program. The SOP states that, as part of incident remediation, the BR program committed to refine the manual report process and create a software tool, [redacted] to help automate accounting of BR FISA disseminations.

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

(U//~~FOUO~~) [redacted] NSA's corporate dissemination tracking tool, was implemented in December 2013. Before this, disseminations were tracked manually. Since then, all disseminated reports derived from BR metatada have been tracked in [redacted]

~~(TS//SI//NF)~~ Notice of Material Misstatement and Compliance Incident, [redacted]

(b)(3)-P.L. 8

~~(TS//SI//NF)~~ **Preliminary** [redacted] *NSA notified the NSD's OI that (1)* [redacted] *NSA received* [redacted] *a sample of* [redacted] *call detail records for testing purposes,* [redacted]

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

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

~~(TS//SI//NF)~~ *NSA deleted all* [redacted] *call detail records* [redacted] *Prior to its destruction, the* [redacted] *was stored at all times on servers accessible only to technical personnel and was not available for intelligence analysis. NSA and OI continue to investigate the facts and circumstances concerning this matter and the DoJ will provide a thorough explanation of the matter to the Court upon completion of the investigation.*

~~(TS//SI//NF)~~ **Final** [redacted] *final notice of Compliance Incident,* [redacted]

(b)(3)-P.L. 8

was filed with the Court. NSA identified [redacted] *in the sample* [redacted] *call detail records* [redacted]

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

~~(TS//SI//NF)~~ On 17 December 2013, NSA submitted a Congressional notification of the compliance incident to the House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary. Copies were also provided to the Congressional affairs offices at the ODNI and USD(I). On 2 December 2013, the NSA OIG notified the ATSD(IO) of the incident and pending Congressional notification.

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

~~(TS//SI//NF)~~ **Controls put in place to mitigate recurrence** NSA filed a "Notice of Material Misstatement" because in a previous declaration to the Court, NSA stated that it had expected to receive sample [redacted] records [redacted] for testing and that NSA had notified the providers that it did not want CSLI information. NSA was not able to verify [redacted] As an implementing control, NSA modified the way it performs the VoA on the declaration to the Court so that all organizations associated with the BR FISA program participate in the VoA process and review the entire document. The BR FISA Authority Lead initiated quarterly meetings with stakeholders to compare the previous final BR Order with the new declaration to identify changes and ensure that the new declaration is reviewed for accuracy. Since the incident, NSA has not received sample [redacted] records [redacted]

~~(TS//SI//NF)~~ As discussed in the Sampling section, DIAs test the [redacted] feed daily and weekly to verify that it does not contain CSLI data. The DIAs identified no CSLI data since the [redacted] feed became operational [redacted]

(U//~~FOUO~~) The four incidents of non-compliance were included in NSA's first, third, and fourth quarters 2013, *Report to the Intelligence Oversight Board on NSA Activities*.

(U//~~FOUO~~) For a list of the incidents of non-compliance from 2010 through 2012, see Appendix B.

(U) NSA Use of the BR FISA Authority

(U//~~FOUO~~) Although no formal process has been implemented to assess the effectiveness of the BR FISA authority, NSA asserts that the authority has made valuable contributions to the CT intelligence mission and that it plays an important role for NSA intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland and U.S. interests abroad.

(U) Methods Used to Assess Effectiveness

(U) NSA's BR FISA program was developed to assist the U.S. government in detecting communications between known or suspected terrorists operating outside the United States and others inside the United States, as well as communications among operatives within the United States. The 9/11 Commission identified that detecting and linking such communications as a critical intelligence gap in the aftermath of the attacks on 11 September 2001.

~~(TS//SI//NF)~~ Based on requests from the Senate Select Committee on Intelligence to determine the "value of the program," NSA and FBI personnel developed in February 2014 the "BR FISA Bulk Metadata NSA/FBI Process for FBI Feedback" plan that describes NSA's responsibility to deliver to the FBI spreadsheets with BR information and the FBI's responsibility to summarize use for NSA. The plan called for FBI's [redacted] to categorize selection terms in the BR FISA report as follows:

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

- (U//~~FOUO~~) Not of Interest—selection term is technically flawed or the characteristics make it worthless for research.
- (U//~~FOUO~~) Known to the FBI—FBI is aware of the selection term independently.
- (U//~~FOUO~~) Known to the FBI with additional information—FBI is aware of the selection term independently, but NSA reporting provides amplifying information to aid FBI investigations.
- (U//~~FOUO~~) Unknown to the FBI—the FBI was not aware of the selection term.

~~(TS//SI//NF)~~ Under the plan, [redacted] would send BR-unique leads to FBI field offices; [redacted]

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

[redacted]

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

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

[redacted]

(U//~~FOUO~~) BR FISA program leadership recognizes that there is no process to track program effectiveness. They agreed on the need to track effectiveness but were unable to determine how to do so. Feedback is difficult to obtain. One former BR FISA program leader asked, "How do you assess the effectiveness of an authority when we don't get feedback from the customer?"

~~(TS//SI//NF)~~ Another limitation on NSA's ability to determine the effectiveness of the BR FISA program [redacted]

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

[redacted]

(U) Table 25. Selection Terms in Approved Status as of 31 December 2013 by Target Office of Primary Interest

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

Target Office of Primary Interest	Selection Terms Approved	Percent of Total Selection Terms Approved

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

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

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

(U//~~FOUO~~)

NSA implemented the "BR FISA Bulk Metadata Monthly Internal Report for SID." The report includes:

- (U//~~FOUO~~) Program highlights,
- (U//~~FOUO~~) Number of disseminations,
- (U//~~FOUO~~) Number of approved RAS selection terms,
- (U//~~FOUO~~) Number of queries,
- (U//~~FOUO~~) BMD volume, and
- (U//~~FOUO~~) Number of personnel by organization and work role with program access, approved to disseminate USP information, and approved as HMCs.

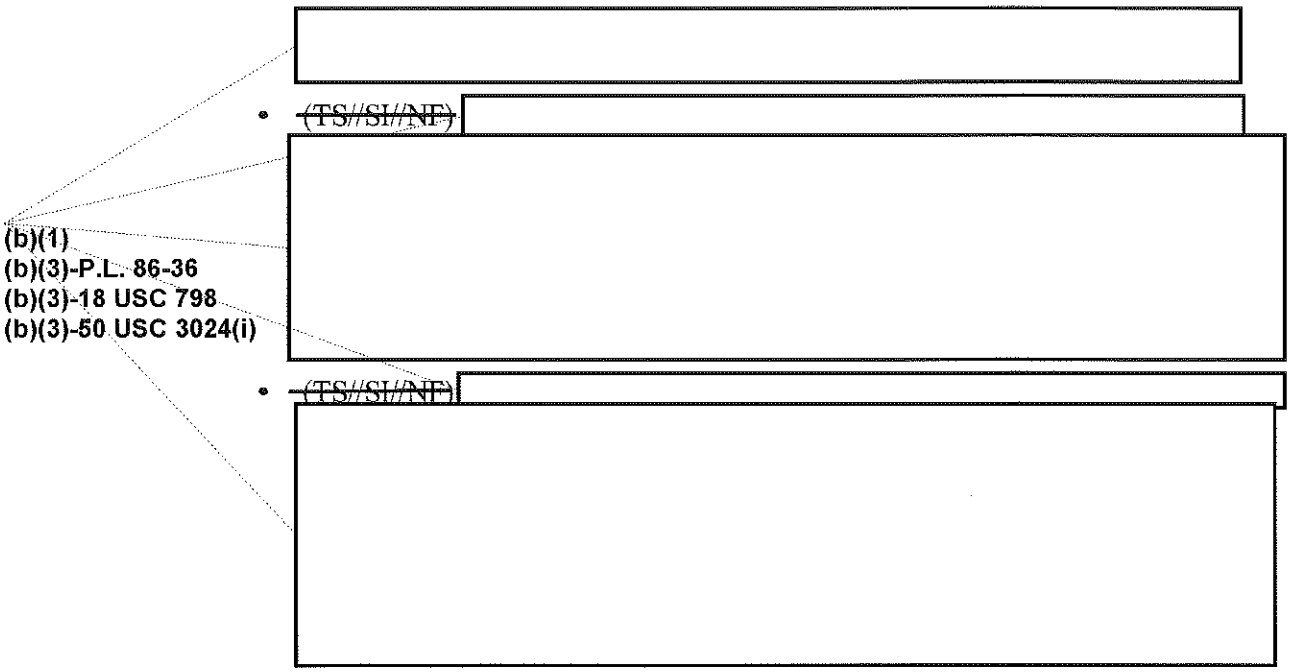
(U) Contributions from BR FISA Authority that Support the CT Intelligence Mission

(U) 2013 highlights

~~(TS//SI//NF)~~ NSA does not assert that information from the BR FISA program does, by itself, identify or thwart plots. Instead, information obtained through the program plays a complementary role within a larger body of intelligence and CT investigations. It is important to note that BR metadata may sometimes be the single source of intelligence. However, typically, acquisition and analysis of BR metadata are designed to fill gaps in information gathered under other collection authorities. By helping close those gaps, NSA personnel report that BR data contributes to comprehensive efforts to identify and address threats to the homeland. The following are highlights from the BR FISA program in 2013.

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

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



(U) On 21 June 2013, in response to a request from the House Permanent Select Committee on Intelligence after unauthorized public disclosures, NSA provided to that committee and the Senate Select Committee on Intelligence, the House and Senate Committees on the Judiciary, and the Defense subcommittees of the House and Senate Appropriations Committees a list of 54 events in which the BR FISA or FAA §702 authorities or both contributed to the production of SIGINT and to the IC's understanding of terrorism activities.

(U) Analyst Use of the Authority

(U//~~FOUO~~) NSA senior management believe that the BR FISA program is important to intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland, primarily in support of the FBI, by enhancing their ability to detect, prioritize, and track terrorist operatives and their support networks in the United States and abroad. By querying BR metadata, intelligence analysts are said to:

- (U//~~FOUO~~) Detect domestic and foreign selection terms in contact with domestic and foreign selection terms associated with foreign terrorist organizations,

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

[44] (U//~~FOUO~~)

- (U//~~FOUO~~) Discover selection terms with which the foreign and domestic selection terms associated with foreign terrorist organizations are in contact, and
- (U//~~FOUO~~) Detect possible terrorist-related communications between communicants inside the United States.

(U) Identifying threats

(U//~~FOUO~~) NSA has many sources of information that provide indications of potential terrorist activity against the United States and its interests abroad. The best analysis typically occurs when analysts evaluate information obtained from all those sources to disseminate to the FBI and the IC as complete a picture as possible of potential terrorist threats. Although BR metadata is not the sole source of information available to NSA CT personnel, it is a component of the information that analysts rely on to execute threat identification and characterization. BR metadata can add to the IC's and law enforcement community's understanding and evaluation of threat information and the need to take investigative action.

(U) Agility

(U) BMD, NSA personnel assert, enables the Agency to quickly analyze communications and contact chains. Unless the data is aggregated, it may not be feasible to detect communication chains that cross communication networks and authorities. The ability to query accumulated metadata from multiple authorities significantly increases NSA's ability to rapidly detect persons who are affiliated with foreign terrorist organizations and might otherwise go undetected.

(U) Hops

(U//~~FOUO~~) When NSA performs a contact-chaining query on a terrorist-associated selection term, analysts are able to detect not only the direct contacts made by that first tier of contacts but also the additional tiers of contacts, out to the maximum number of permitted hops from the seed selection term. [redacted] (b)(3)-P.L. 86-36

[redacted]

provides a more complete picture of those who associate with terrorists or are engaged in terrorist activities. The ability to look at a network beyond the first hop enables analysts to potentially identify the core of a network, focusing and prioritizing resources efficiently against threats.

(U) Historical data

~~(TS//SI//NF)~~ Another advantage that SID leadership ascribes to the BR FISA program is that the BR metadata is historical. [redacted] historical connections are critical to understanding newly identified targets, and metadata may contain links that are unique, pointing to potential targets of interest that may otherwise be missed.

(U) Tradecraft

(U//~~FOUO~~) Analysts report that BR metadata analysis enriches their understanding of the communications tradecraft of terrorist operatives who may be preparing to conduct attacks against the United States.

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

(U) Complementary

(U//~~FOUO~~) The BR FISA program, SID leadership asserts, complements information that NSA collects by other means, increasing the value to the Agency and linking possible terrorist-related telephone communications between communicants based solely inside the United States. As a complementary tool to other intelligence authorities, the NSA's access to BR metadata increases the likelihood of detecting terrorist cell contacts within the United States. The BR FISA program provides NSA the information necessary to perform call chaining that can enable analysts to obtain a much broader understanding of the target and, as a result, allow NSA to provide to the FBI and the IC a more complete picture of possible terrorist-related activity inside the United States.

(U) Prioritizing

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

(U//~~FOUO~~) The BR FISA program assists with applying limited analytic and linguistic resources available to the CT mission have the highest probability of connection to terrorist targets. Analysis of BR metadata can help analysts prioritize communications of non-USPs that it acquires under other authorities because such persons are of heightened interest if they are in a communication network with persons in the United States.

(U//~~FOUO~~) SID leadership asserts that, without the ability to obtain and analyze BR metadata, NSA would lose a tool for detecting communication chains that link to selection terms associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest. The BR FISA program allows efficient, potential terrorist activities. Any other means that might be used to conduct similar analyses would require multiple, time-consuming steps that would frustrate rapid analysis in emerging situations and could fail to capture some information available through BR metadata. If BR metadata is not aggregated and retained for a time, NSA could not detect

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

(U) Former DIRNSA General Alexander testified to the Senate Committee on the Judiciary in December 2013:

> (U) Measuring the value of the BR FISA authority by the number of plots exposed to date misses the point and presents us with a false choice. The BR FISA authority is similar to an insurance policy, designed to make sure that the gap exposed after 9/11 doesn't happen again, with perhaps even more catastrophic consequences. As with an insurance

policy on your house, you don't determine its value by asking how many times you've collected on the policy to date—you want to have it for the possible fire, or flood, or theft in the future. Combined with the limitations on the program, the potential benefit in allowing us to uncover the hidden terrorist in the U.S. still provides a unique value consistent with the protection of privacy rights.

III. (U) FAA §702

(U) Background

(U) The FAA §702 certifications

~~(S//NF)~~ Section 702 of FAA, *Procedures for Targeting Certain Persons Outside the United States other than United States Persons*, states that the Attorney General and the DNI may jointly authorize, for the period of up to one year, the targeting of persons who are not USPs and who are reasonably believed to be located outside the United States to acquire foreign intelligence information. This authority is granted on the basis of annual certifications made by the Attorney General and the DNI to the FISC. [redacted] certifications identify categories of foreign intelligence information sought through this acquisition:

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

[redacted]

~~(S//NF)~~ The NSA targeting and minimization procedures establish the processes that the Agency must follow and the requirements that it must satisfy to comply with the limits the statute and the Constitution impose on the use of this surveillance. The targeting procedures must be "reasonably designed" to limit acquisition under the [redacted] FAA §702 certifications to non-USPs reasonably believed to be located outside the United States to acquire foreign intelligence information and to prevent intentional acquisition of communications in which the sender and all intended recipients are known at the time of acquisition to be in the United States.[45] The purpose of the minimization procedures is to establish controls over the acquisition, retention, and dissemination of non-publicly available USP information.

(U//~~FOUO~~) In addition to targeting and minimization procedures, FAA §702 requires the Attorney General, in consultation with the DNI, to adopt guidelines to ensure compliance with the limitations in the Act on acquisition of communications. These are documented in *Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978*. Approved by the Attorney General in 2008, the guidelines reinforce the targeting procedures, establish

[45] (U//~~FOUO~~) Acquisition is the collection by NSA or the FBI through electronic means of non-public communications to which they are not intended parties.

requirements for application of the targeting procedures, and establish requirements for obtaining court orders.

(U//~~FOUO~~) The government's FAA §702 certifications, targeting procedures, and minimization procedures (but not the Attorney General Guidelines) require FISC approval. The FAA §702 certifications are accompanied by affidavits from the heads of elements of the IC, such as the DIRNSA, that describe the Agency's basis for assessing that acquisition will be consistent with statutory authorization and limits.

(U) Methodology and Scope

(U//~~FOUO~~) Our review of the FAA §702 control framework, incidents of non-compliance, and NSA's use of the authority to support its mission, was based largely on FAA §702 stakeholder interviews and reviews of policies, procedures, and other program documentation. The OIG's *Special Study: Assessment of Management Controls Over FAA §702,* revised and reissued 29 March 2013, was also used as a resource. That study examined the controls designed to ensure compliance with FAA §702 and the targeting and minimization procedures associated with the 2011 certifications. Given the time constraints for the current review and the agreement with staff of the Senate Committee on the Judiciary, we did not verify through testing that all controls were operating as described by FAA §702 program stakeholders.[46]

(U//~~FOUO~~) Our review focused on the processes and controls in place in 2013. Two documents filed annually with each FAA §702 certification delineate NSA's procedures for complying with the FISA Amendments Act of 2008:

- (U//~~FOUO~~) *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (FAA §702 Targeting Procedures) and
- (U) *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (the FAA §702 Minimization Procedures).

(U//~~FOUO~~) For calendar year 2013, the period under review, different versions of these documents were in effect because of changes made at the annual certification renewal and special amendments to the procedures.

- (U) Targeting Procedures
  - o ~~(S//NF)~~ Procedures approved with the 2012 renewal of the authority, effective 24 September 2012 through 10 September 2013.

[46] (U//~~FOUO~~) The NSA OIG has conducted several audits and special studies on the effectiveness of certain FAA §702 program controls.

- ~~(S//NF)~~ These procedures were not changed for the 2013 certification renewal and remained effective 10 September 2013 through 28 August 2014.

• (U) Minimization Procedures

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

- ~~(S//~~ [redacted] Procedures approved for the 2012 certification renewal, approved by the FISC 24 August 2012, were effective 24 September 2012 through 23 September 2013. [redacted]

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

[redacted]

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

- (U//~~FOUO~~) An amended version of the 2013 minimization procedures approved 13 November 2013, added special procedures for assessing NSA's ability to use collection received when NSA's [redacted] post-tasking checks were not functioning properly and procedures for handling data collected during a period in 2013 when these checks were not performing as intended.

(U) We also examined implementing procedures and controls for the Attorney General's targeting guidelines.

(U) FAA §702 Program Control Framework

(U//~~FOUO~~) The FAA §702 control framework describes how NSA targets, collects, retains, accesses, queries, disseminates, and purges FAA §702 data and the oversight mechanisms to comply with FAA §702 certifications, including FISC-approved targeting and minimization procedures. This section summarizes the provisions of the targeting and minimization procedures and the controls implemented for each phase of the FAA §702 production cycle.

(U) Targeting

(U) Provisions of FAA §702 certifications

~~(S//NF)~~ The FAA §702 targeting procedures set forth the measures that NSA uses to determine whether a prospective target is eligible for targeting under this authority. Each prospective target must meet three criteria. The individual must be a non-USP, reasonably believed to be located outside the United States, who possesses or is likely

[47] (U) A target is a person or entity against which intelligence operations are conducted. Foreign intelligence is obtained by tasking the target's selectors (e.g., e-mail addresses) to acquire information pursuant to one of NSA's authorities.

to communicate foreign intelligence information consistent with one of the [redacted] FAA §702 certifications.[48]

~~(S//NF)~~ The targeting procedures state that, when NSA proposes to direct surveillance at a prospective target, it does so only after it has learned something about the prospective target or the facilities the individual uses to communicate. For example, NSA personnel may examine lead information, obtained from a non-NSA element, such as tips from the CIA or FBI, [redacted][9]

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

~~(S//NF)~~ NSA personnel must also assess whether the prospective target possesses or is likely to communicate foreign intelligence information concerning a foreign power [redacted] and whether the proposed target is appropriate under one of the [redacted] FAA §702 certifications.

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

(U) Targeting process overview

(U//~~FOUO~~) To initiate targeting under FAA §702 authority, NSA personnel must research the prospective target to determine whether it meets the requirements of this authority and to identify selectors that will yield communications from the prospective target.[50] Mission analysts operate within an assigned mission team (see the Access and Training section) and follow targeting guidance established by SID Analysis and Production on the basis of the FAA §702 Targeting Procedures to complete the analysis that forms the basis for a targeting request (TR). The [redacted] is the vehicle for development and submission of TRs, [redacted] The TR documents information supporting the targeting decision and is subject to at least two levels of review before targeting. Additional reviews may be performed by the SID Data Acquisition (S3) office of Targeting Strategy and Mission Integration (TSMI) and SV.

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

(U//~~FOUO~~) Mission analysts are responsible for the initial research and identification of potential targets within their organization's assigned missions. Analysts must complete a training regimen involving general courses on legal authorities and annual courses on FAA §702 procedures to be eligible to submit TRs under this authority and access and handle FAA §702 data (see the Access and Training section).

(U) Provisions of FAA §702 certifications—eligibility for targeting

~~(S//NF)~~ **Foreignness determination** The targeting procedures require that NSA personnel examine, as appropriate under the circumstances, three categories of information to determine whether the intended target is a non-USP reasonably believed to be outside the United States (the foreignness determination). The

[48] (U) FAA does not define the term "reasonable belief," but the Act requires that NSA adopt targeting procedures to ensure that FAA §702 acquisition is limited to targets reasonably believed to be outside the United States.

[49] (U) Facilities are communication vehicles used by targets, including telephone numbers and e-mail addresses. NSA tasks these facilities or "selectors" to obtain foreign intelligence from approved targets.

[50] (U) Selectors are unique identifiers of targets (entities against which intelligence operations are conducted), such as telephone numbers and e-mail addresses, used for tasking (initiating SIGINT collection for the target's selectors).

determination is based on the totality of information available about the prospective target's location and status as a USP and may be obtained from any one or a combination of these sources:

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

- ~~(S//NF)~~
- ~~(S//NF)~~
- ~~(S//NF)~~

(U//~~FOUO~~) **Foreign intelligence purpose for targeting** In addition to the foreignness determination, NSA personnel must assess whether the prospective target possesses, is expected to receive, and/or is likely to communicate foreign intelligence pursuant to one of the FAA §702 certifications.[51] Each certification identifies categories of foreign intelligence (see Background at the beginning of FAA §702 section) and specifies activities for which foreign intelligence collection is approved.

~~(S//NF)~~ Targeting must also comply with the Attorney General's *Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978*, which reiterates the five targeting activities prohibited by FAA §702:

- (U) Intentionally targeting a person known at the time of acquisition to be in the United States;
- (U) Reverse targeting, that is, targeting a non-USP outside the United States for the purpose of targeting a particular, known person reasonably believed to be in the United States;
- ~~(S//NF)~~ Intentionally targeting a USP reasonably believed to be outside the United States;
- (U) Intentionally acquiring communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States; and
- (U) Targeting inconsistent with the Fourth Amendment to the Constitution of the United States.

[51] (U) Foreign intelligence information is defined in FISA as (1) information that relates to, and if concerning a USP is necessary to, the ability of the United States to protect against- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to – (A) the national defense or the security of the United States or; (B) the conduct of the foreign affairs of the United States.

(U) Targeting control procedures

~~(S//NF)~~ **Target research—foreignness**

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

(U//~~FOUO~~) **Target research—foreign intelligence determination** NSA mission analysts task targets that are aligned with the National Intelligence Priorities Framework, can be linked to one of the foreign intelligence purposes specified in the appropriate FAA §702 certification and, generally, are within the analysts' assigned mission area.[53]

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

(U//~~FOUO~~) **Targeting request** Once mission analysts complete the research for the proposed target, they must develop and submit a TR identified for an eligible target. The TR documents the analyst's determinations that the prospective targets meet the standards in the targeting procedures. Once the TR has been reviewed and approved (see Targeting Authorization), the selector identified in the TR is used to initiate collection. To complete a valid TR, mission analysts must compile specific information to demonstrate that, based on the totality of the circumstances determined from the research performed, there is a reasonable belief that the proposed target is foreign (not a USP and not within the United States) and is likely to produce foreign intelligence consistent with one of the FAA §702 certifications. The TR must include:

[52] (U//~~FOUO~~) Raw data is data that has not been evaluated for foreign intelligence or processed to handle USP identities pursuant to the minimization procedures. Metadata is dialing, routing, addressing, or signaling information associated with a communication but does not include information concerning the substance of the communication.

[53] (U) The National Intelligence Priorities Framework translates national foreign intelligence objectives and priorities approved by the President into specific prioritization guidance for the IC. It serves as guidance for U.S. foreign intelligence analysis and collection.

- (U//~~FOUO~~)

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

- (U//~~FOUO~~)
- (U) Sources supporting the determination of foreignness. [54]

(U//~~FOUO~~) Mission analysts must create permanent documentation of the information sources used to establish foreignness. Copies of the source information are saved in a restricted access SharePoint site SV maintains. This repository facilitates approval of the TR, as well as internal and external oversight.

U//~~FOUO~~) The system supports targeting compliance as the mission analyst creates the TR. The system requires:

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

- ~~(S//SI//REL TO USA, FVEY)~~ Detailed information establishing the foreignness of the selector,

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

- (U//~~FOUO~~) Target information, including the TAR,
- (U//~~FOUO~~) Completion of key fields to document information about the prospective target (e.g., authorized targeting purpose, how the individual was determined to be outside the United States, basis for expectation that targeting the individual will produce foreign intelligence), and
- (U) Identification of the appropriate FAA §702 certification.

(U//~~FOUO~~) The system also:

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

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

- (U) Identifies conflicting data within the TR,
- (U) Captures references to supporting documentation,
- ~~(S//REL TO USA, FVEY)~~
- ~~(S//REL TO USA, FVEY)~~

[54] (U) Targeting Rationale is a brief justification for targeting a selector, intended to explain the connection between the proposed target and a foreign intelligence purpose.

[55] ~~(S//REL TO USA, FVEY)~~

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

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

~~(S//NF)~~

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

~~(S//NF)~~

~~(TS//SI//REL TO USA, FVEY)~~

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

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

[56] ~~(S//SI//NF)~~

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

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

- (U//~~FOUO~~) (b)(3)-P.L. 86-36
- (U//~~FOUO~~)
- ~~(S//NF)~~ (b)(1) (b)(3)-P.L. 86-36

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

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

~~(TS//SI//REL TO USA, FVEY)~~

(U) Provisions of FAA §702 certifications—authorization to target

(U//~~FOUO~~) Approval to task a prospective target's selectors requires that the TR entry for that tasking be reviewed to verify that it contains the necessary citations to source information that led the analyst to reasonably believe that the individual is a

[57] ~~(TS//SI//NF)~~ (b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)

non-USP outside the United States and is linked to the appropriate FAA §702 certification.

(U) Targeting authorization—c ontrols

(U//~~FOUO~~) NSA has implemented a multi-level review process to approve all proposed targeting.

(U//~~FOUO~~) **Releaser review** Submitted TRs are first reviewed by the mission releaser. Normally, the releaser is in the same organization as the mission analyst. Releasers must complete the same training courses as mission analysts. They examine the TRs for completeness and compliance with the FAA §702 Targeting Review Guidance developed and maintained by the Mission and Compliance staff, part of the Directorate for Analysis and Production, within NSA's Signals Intelligence Directorate.[58]

(U//~~FOUO~~) **Adjudication** [redacted] the final approval of the TR, known as adjudication, is a critical control point in tasking selectors under FAA §702 authority and is performed by personnel designated as mission adjudicators. TRs were initially subject to adjudication by SV but, [redacted] (b)(3)-P.L. 86-36 [redacted] the responsibility was moved to the mission groups within the SIGINT Analysis and Production organization, where specially trained and experienced analysts, usually from the same organization as the targeting analyst, perform adjudication.[59] Adjudicators must complete the same courses as other mission personnel as a prerequisite for access to FAA §702 data (see the Access and Training section). They must also complete a specific course on adjudication and receive on-the-job training in their mission office before they are permitted to adjudicate independently. Adjudicators receive advice and updated information from the staff of the SIGINT Analysis and Production organization, SV, and OGC on developments affecting the application of the FAA §702 authority. The majority of adjudicators have two or more years experience in adjudication. Adjudicator performance is monitored by the Mission and Compliance staff in SID's Directorate for Analysis and Production.

~~(C//REL TO USA, FVEY)~~ Adjudicators review TRs for accuracy, evaluate the evidence in the TR supporting the foreignness of the proposed target, examine the TAR statement for the individual's foreign intelligence value, and verify that the TR supports eligibility for targeting under the specified FAA §702 certification. As part of their TR reviews, adjudicators recreate the steps taken by the mission analyst to independently confirm that the supporting data is accurate and that the most current information available is used to support a reasonable belief that the prospective target

---

[58] (U//~~FOUO~~) As part of the Operations Staff for the S2, the staff includes teams who provide support and oversight of SID's use of FAA §702, such as [redacted] (S203A1) and [redacted] (S203A7).

[59] (U//~~FOUO~~) Mission Groups are primarily in S2; [redacted] S2 (if appropriate), SV, and the NSA OGC.

is foreign. Following the same procedure as mission analysts, adjudicators [redacted] to determine whether there is supporting or contrary information regarding the foreignness of the individual. Adjudicators must complete a series of checks manually or assisted by technology:

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

- (U//~~FOUO~~) [redacted] for an initial foreignness determination.[60]
- ~~(TS//SI//REL TO USA, FVEY)~~ Reviewing the database of selectors [redacted] whether there was information indicating that the individual was not foreign.

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

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

- (U//~~FOUO~~) Accessing the SV4 SharePoint Site to determine whether there is information that would preclude the current tasking request from being approved [redacted]
- (U//~~FOUO~~) [redacted]

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

(U//~~FOUO~~) If adjudicators are able to confirm that the prospective target meets the FAA §702 requirements for tasking, they approve the target's selector for tasking [redacted] However, if there is an error or required information is absent in the TR, adjudicators must ensure that corrective action is taken before approving the TR.

~~(TS//SI//NF)~~ In most instances, if adjudicators identify updated foreignness information, they substitute that information in the TR to ensure that the TR is current. If adjudicators find an error, such as inaccurate foreignness information, insufficient evidence to support foreignness, or an incomplete TAR statement, adjudicators may deny the TR and return it to mission analysts for correction. When the TR is corrected, the TR goes back to the mission releaser and the mission adjudicator. As part of the approval process, adjudicators upload documentation of the sources supporting the targeting decision to the SharePoint site that SV maintains. [redacted]

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

[60] ~~(C//REL TO USA, FVEY)~~ [redacted]

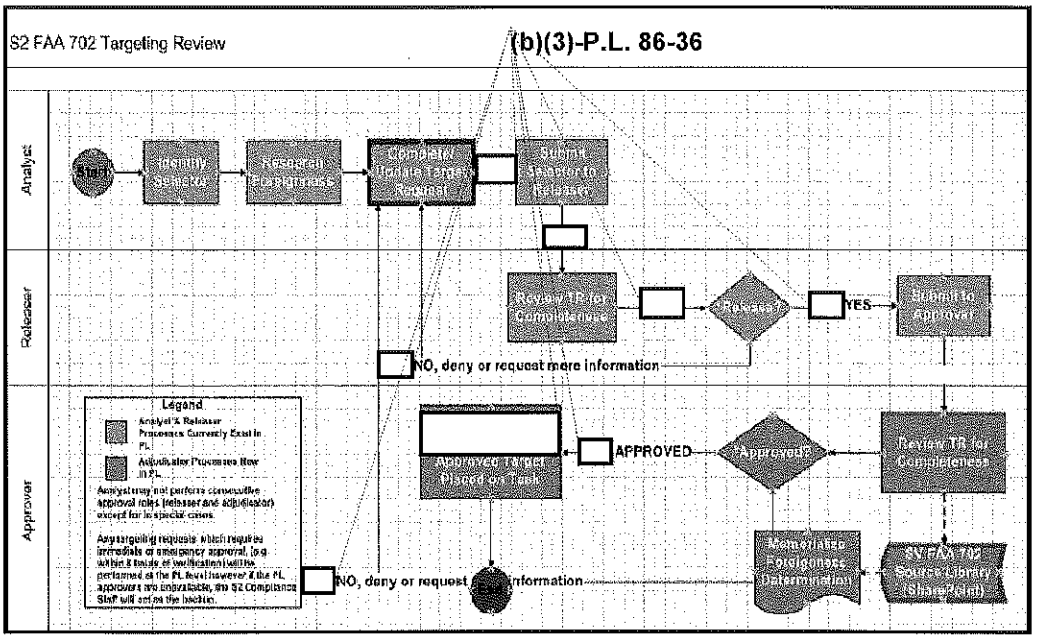
[61] ~~(C//REL TO USA, FVEY)~~ [redacted]

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

(U//~~FOUO~~) The targeting review process is summarized in Figure 8.

(U) Figure 8. FAA §702 Targeting Review Process

~~(S//NF)~~



~~(S//NF)~~

(U) Provisions of FAA §702 certifications—approval of TRs from other agencies

(U//~~FOUO~~) The FAA §702 minimization procedures set forth processes NSA uses for the acquisition, retention, use, and dissemination of information acquired under FAA §702.

(U//~~FOUO~~) In accordance with Section 6(c) of the minimization procedures, NSA provides the CIA and the FBI unminimized communications acquired pursuant to FAA §702 for targets nominated by the respective agencies and approved for tasking in accordance with NSA's targeting procedures. Both the CIA and the FBI must handle unminimized communications received from NSA in accordance with their FISC-approved minimization procedures adopted by the Attorney General in consultation with the ODNI.

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

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

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

(U//~~FOUO~~) Controls over approval of CIA and FBI TRs

~~(S//REL TO USA, FVEY)~~ The CIA and the FBI submit requests for tasking selectors of prospective targets to NSA, which reviews the foreignness information and the foreignness justification for the prospective target and approves the selectors for tasking upon an assessment that there is a reasonable belief that the prospective target is a non-USP outside the United States and that collection will produce foreign intelligence information pursuant to one of the approved certifications.

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

~~(S//NF)~~ Targets proposed by the CIA or FBI that are not currently tasked by NSA are vetted through reviews performed by NSA personnel

(U//~~FOUO~~) Table 26 summarizes the targeting provisions of the FAA §702 targeting procedures and the controls NSA has implemented to maintain compliance.

(U) Table 26. Targeting Provisions and Controls

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

Provision	Control
(U) Foreignness - Acquisition targets only non-USPs reasonably believed to be outside the United States	(U//~~FOUO~~) The TR documents the support for NSA's determination of the prospective target's foreignness. ~~(TS//SI//REL TO USA, FVEY)~~ The targeting system enforces completion of required fields (including foreignness information), identifies conflicting data, flags selectors ineligible for tasking and captures source information supporting targeting. (U//~~FOUO~~) All TRs are subject to at least two levels of review prior to targeting. Additional reviews may be performed by TSMI or SV. Reviewers examine available information to validate accuracy of the foreignness determination and that conflicting information has been resolved.

(b)(3)-P.L.

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

[63] (U) An MCT is an Internet "transaction" that contains more than one discrete communication within it. If one of the communications within an MCT references a tasked selector and one end of the transaction is foreign, the entire MCT transaction will be acquired through upstream Internet collection techniques. Since this can include discrete communications that do not contain the tasked selector, use of such information must meet specific requirements.

(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)	~~(TS//SI//REL TO USA, FVEY)~~ ~~(TS//SI//REL TO USA, FVEY)~~ ~~(TS//SI//REL TO USA, FVEY)~~
(b)(1) (b)(3)-P.L. 86-36 ~~(S//SI//NF)~~ NSA will maintain records of selectors to support compliant tasking. New TRs will be compared with these records before targeting.	~~(S//SI//NF)~~ NSA maintains these records in a database of selectors. This tool is used in target research by analysts and interfaces with to identify ineligible selectors proposed for targeting. The information generated is reviewed by the adjudicators and any conflicts should be resolved before the TRs are approved. (b)(3)-P.L. 86-36
(U) Foreign Intelligence Purpose of Targeting - NSA will assess whether the target possesses or is likely to communicate foreign intelligence pursuant to one of the approved certifications.	(U//~~FOUO~~) The TAR Statement documents why targeting is requested and indicates the tie to a foreign intelligence purpose specific to the FAA Certification under which targeting is requested. This is subject to adjudication.
(U) NSA may provide unminimized communications acquired pursuant to FAA §702 to the CIA and FBI.	~~(S//REL TO USA, FVEY)~~ The CIA and FBI may nominate targets and selectors for acquisition, subject to NSA's targeting procedures. (b)(1) (b)(3)-P.L. 86-36 The CIA and FBI have their own minimization procedures for processing the unminimized data that they receive.
(U//~~FOUO~~) Tasking requests must be supported by citations to the information that led to the analyst's reasonable belief of the foreignness of the target. Approval of the TR will include review of the citation.	(U//~~FOUO~~) The adjudication review includes examination of the citations supporting the foreignness determination maintained in the SV SharePoint site.

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

(U) Provisions of FAA §702 Certifications and other Guidance—Post-Targeting Review

~~(S//NF)~~ In accordance with the targeting procedures set forth in each FAA §702 certification, NSA analysts are required to conduct post-targeting reviews of all selectors tasked under FAA §702 authority. The targeting procedures state that "Such analysis is designed to detect those occasions when a person who when targeted, was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States."

(U) Post-targeting

~~(S//NF)~~ NSA has implemented four procedures to ensure that targeted persons continue to meet the criteria specified in the FAA §702 targeting procedures.

~~(S//REL TO USA, FVEY)~~ **Post-targeting controls—obligation to review** NSA has implemented a process called Obligation to Review (OtR) that has two provisions. The first requires that, upon tasking a selector, the mission team that initiated tasking must review collection from that tasking within 5 business days of the receipt of the initial piece of traffic from FAA §702 collection. An e-mail notification is sent to mission team members notifying them of the receipt and the 5 day review requirement. The mission analyst must review a sample of the content of the collection to determine that:

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

- (U) The selector is being used by the intended target,
- (U) The target is valid under the requested FAA §702 certification, and
- ~~(S//REL TO USA, FVEY)~~ [redacted]

(U//~~FOUO~~) If the reviewing analyst determines that all three requirements have been satisfied, thus making the tasking valid under FAA §702 authority, no further action is required. If any of the three requirements is not satisfied, the selector must be immediately detasked in the [redacted] system (removed from collection). The selector cannot be resubmitted for tasking until all requirements have been satisfied. (Detasking is discussed further in Monitoring Collection section.)

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

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

(U//~~FOUO~~) The second provision of the OtR process requires the mission office to conduct an ongoing review of at least a sample of the content from ongoing collection to ensure that the target continues to meet the criteria for targeting under FAA §702. After the initial review has been completed, a sample of collection is reviewed [redacted]

~~(S//REL TO USA, FVEY)~~ [redacted]

~~(S//REL TO USA, FVEY)~~ [redacted]

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

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

~~(TS//SI//REL TO USA, FVEY)~~

(U//~~FOUO~~) **Post-targeting controls—monitoring collection** Mission analysts must monitor collection for indications that the target no longer meets the foreignness requirements, is not associated with the tasked selector, or is not linked to a valid foreign intelligence purpose tied to an FAA §702 certification. If it is determined that the target or the selector is no longer appropriate for tasking under this authority, NSA will have to take actions that might include detasking the selector, reporting a compliance incident, recalling intelligence reports, and purging collected communications.

(U//~~FOUO~~) If collection indicates user of a tasked selector is an individual who is not the intended target and is not of foreign intelligence value or is or may be a USP or is in the United States, the mission office must immediately remove from collection all selectors and identify collection ineligible for retention. Additional research may be performed before detasking, if there is evidence that the information on the user's USP status or location is not correct. Unless there is a strong reason to doubt this information from collection, it is presumed valid and detasking should occur immediately. If review of collection identifies communications in which the sender and all intended recipients are determined to have been within the United States at the time of collection (domestic communications), those communications must be destroyed with limited exceptions.[64]

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

(U) If analysis of the collection finds that the selector is no longer used by the target, the selector must be removed from tasking.[65]

(U//~~FOUO~~) Attorney-client privileged communications are subject to special procedures designed to prevent privileged information from being used in prosecution. Should review of collection identify communications between persons known to be under criminal indictment in the United States and their attorneys, review of the communication must be discontinued and OGC notified for guidance on handling the communication.[66]

---

[64] (U//~~FOUO~~) If the domestic communication collected is not related to an incident (see Incident Reporting), DIRNSA may approve a destruction waiver to allow retention of the collection.

[65] ~~(S//SI//REL TO USA, FVEY)~~

[66] (U//~~FOUO~~) Monitoring communications between a person known to be under criminal indictment in the United States and an attorney representing that individual in the matter under indictment must cease once the relationship has been identified. The acquired communications must be logged and NSD notified so that measures may be taken to protect such communications from review or use in criminal prosecutions.

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

(U//~~FOUO~~) If authorized collection incidentally acquires a foreign communication of or concerning a USP (e.g., an FAA §702 target is communicating with a USP or about a USP), the communication may in general only be retained if the USP information qualifies as foreign intelligence or the information is evidence of a crime and is provided to appropriate federal law enforcement authorities. Domestic communications, including communications of a target who has entered the United States, must in general, be destroyed upon recognition, unless DIRNSA or the Acting DIRNSA approves retention of the communication for one of the limited reasons listed in Section 5 of NSA's FAA §702 minimization procedures.

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

(U//~~FOUO~~) For intelligence collected from upstream Internet collection [redacted] subject to MCTs, NSA mission analysts must identify and carefully review collection containing MCTs made available for analytic review. While NSA automatically segregates certain MCTs and does not pass them to repositories accessible to analysts, there may still be information in some MCTs that is not eligible for retention. If a discrete communication within an MCT is not to, from, or about a tasked selector but otherwise contains foreign intelligence information and the discrete communication is not to or from an identifiable USP or a person reasonably believed to be in the United States, the MCT may be retained to the same degree that a discrete communication could be retained. If any portion of the MCT contains a domestic communication, the entire MCT must be purged, unless there is no underlying compliance incident and DIRNSA approves a destruction waiver.

(U) For selectors removed from tasking, all communications collected after the target no longer meets the requirements of FAA §702 must be identified for purging through incident reporting and the purge adjudication process (see the Purge section).

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

~~(TS//SI//NF)~~ **Post-targeting controls—detection of targets that may have entered the United States** [redacted] In addition to analyst review of selector communications, NSA has implemented [redacted] for indications that the user of a tasked selector has entered the United States. [redacted] immediately detasks the roaming selector, and [redacted] sends a message to mission analysts notifying them that the selector has been detasked. It is the analysts' responsibility to identify and detask additional selectors for the target and develop the information necessary to produce an incident report. Though NSA may not have had prior notice of the target's intention to travel, FAA §702 may not be used to target individuals in the United States (see the Incident Reporting section).

(b)(3)-P.L. 8

~~(S//REL TO USA, FVEY)~~ [redacted]

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

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

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

(U//~~FOUO~~) **Post-targeting controls—periodic selector review** As discussed earlier, NSA is required to regularly confirm that all selectors tasked under FAA §702 continue to meet targeting requirements. In addition to these ongoing reviews, defaults all FAA §702 targeting to a one year review. To maintain acquisition for the target, mission analysts must confirm that continued tasking of the selector is expected to acquire foreign intelligence relevant to the FAA §702 certification under which the targeting was executed.

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

(U//~~FOUO~~) Table 27 summarizes the post-targeting provisions of the FAA §702 targeting procedures and the controls implemented by NSA to maintain compliance.

(U) Table 27. Post-Targeting Provisions and Controls

~~(S//SI//NF)~~

Provision	Control
(U//~~FOUO~~) Post-targeting analysis is performed to detect when a person, reasonably believed to be outside the United States when targeted, has since entered the United States. This will allow NSA to take steps designed to prevent acquisition of domestic communications or the targeting of a USP.	(U) Analysts are required to monitor collection to determine whether the target continues to meet targeting criteria, including foreignness. (U) Analysts receive "obligation to review" notices upon first receipt of collection for newly tasked Internet selectors and every thirty days commencing with the date of first collection after the last review. The notice is repeated until collection has been reviewed. (U) Annual reviews confirm that a target remains eligible for targeting and continues to be expected to produce foreign intelligence relevant to the FAA §702 certification under which it was approved.
~~(S//SI//REL TO USA, FVEY)~~ NSA will routinely compare tasked selectors with information collected from	~~(S//REL TO USA, FVEY)~~

[67] ~~(TS//SI//REL TO USA, FVEY)~~

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

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

	or detasking of the selector and purge of any non-compliant communications.
~~(S//SI//NF)~~ NSA will routinely compare selectors tasked	~~(S//REL TO USA, FVEY)~~ See Table 26 – second control.
~~(S//SI//NF)~~ NSA will for indications that a foreign target has entered or intends to enter the United States.	(U) Automated notices are sent to mission teams upon first receipt of collection for newly tasked Internet selectors and every thirty days commencing with the date of first collection after the last review. The notice is repeated until collection has been reviewed.
(U) If NSA determines that a target has entered the United States, it will take the necessary steps to assess whether the incident represents non-compliance with the targeting procedures and report such occurrences to DoJ and ODNI and purge related communications from NSA databases as required.	(U) See the Incident Recognition and Reporting section. (U) If NSA determines that a target has entered the United States and the target's selectors were not detasked before entry, it is reported to DoJ and ODNI as an incident. DoJ assesses which incidents represent non-compliance with the targeting procedures and reports such occurrences to the FISC. NSA purges related communications from NSA databases as required. In some cases, DIRNSA may grant a destruction waiver so NSA can retain collection that is otherwise subject to purge.
(U) If NSA determines that a target who at the time of targeting, was believed to be a non-USP is in fact a USP, it will terminate collection without delay and report the incident to DoJ and ODNI and purge such collection from its databases.	(U) See the Incident Recognition and Reporting section.
(U//~~FOUO~~) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment, monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose.	(U//~~FOUO~~) Annual FAA training requires that such communications be brought immediately to OGC's attention for further instruction. OGC maintains e-mail records of such communications, DoJ has agreed that the process used to quarantine these communications is a sufficient process for documenting the information.

(b)(3)-P.L. 8

(b)(3)-P.L. 8

~~(S//SI//NF)~~

(U) Incident Recognition and Reporting

(U) Provisions of FAA §702 certifications—incident reporting

(U//~~FOUO~~) The targeting procedures state that NSA will conduct ongoing oversight and report incidents of non-compliance to the NSA OIG and OGC and ensure that corrective actions are taken to address deficiencies. Reporting is required for incidents of non-compliance "that result in the intentional targeting of a person

reasonably believed to be located in the United States, the intentional targeting of a USP, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States." NSA must report these incidents within five business days of learning about them. The Agency must purge from its databases information acquired by intentionally targeting a USP or a person not reasonably believed to be outside the United States at the time of targeting. If post-targeting analysis shows that the target is inside the United States or a USP, acquisition must be terminated without delay. Inadvertent acquisition of domestic communications is addressed in the minimization procedures see the Purge section). NSA also reports incidents of non-compliance with the FAA §702 minimization procedures. Some examples include incomplete minimization of USP information, improper queries of raw data, and technical errors that affect systems controls over the data, such as retention beyond the required destruction date.

(U) Incident reporting controls

(U//~~FOUO~~) Training and management communications emphasize the fact that incidents can occur at any point in the collection, targeting, dissemination, access, and retention of SIGINT communications and stress the importance of immediate reporting of instances of non-compliance. Individuals do not have to prove that the activity is noncompliant to report an incident. SV works with the mission team that reports the matter to develop an incident report with complete and accurate information. If the incident involves a system or a system's performance, TV involves all appropriate subject matter experts (including SID, SV, TD, and OGC) to assess the situation and evaluate its effect on compliance under the authority. OGC informs DoJ and ODNI of incidents that may indicate non-compliance with FAA §702. DoJ, in coordination with ODNI, makes the final determination whether an incident is reportable to the FISC.

(U//~~FOUO~~) The OIG receives internal incident reports from SV and TV. Notices of non-compliance (13b notices) that DoJ files with the FISC are made available to the OIG. The OIG uses this information to develop the Intelligence Oversight Quarterly Report, which is prepared with OGC and sent to the President's Intelligence Oversight Board through DoD. The incidents and notices of non-compliance are also used as input to OIG inspections and intelligence oversight reviews.

(U//~~FOUO~~) The annual FAA §702 training required of all individuals handling information obtained under this authority addresses incident recognition, reporting, and processing. It defines two types of reportable events: incidents of non-compliance and changes in the target's status.

(U//~~FOUO~~) **Reportable compliance incident** An FAA §702 compliance incident occurs when NSA violates FAA §702 statutory requirements or targeting and minimization procedures or has made materially inaccurate representations to the FISC or has otherwise not performed in a manner consistent with previous representations to the FISC. For example, if NSA tasked a foreign intelligence target reasonably believed to be outside the United States at the time of tasking and later

learned that the target planned to travel to the United States but did not detask the selector before the target's entry into the United States, this would be reported as a compliance incident.

(U//~~FOUO~~) Reportable compliance incidents may also result from actions taken by communication service providers. For example, provider error could cause distribution to NSA of communications for selectors not tasked under FAA §702.

(U//~~FOUO~~) **Change in target status** After tasking selectors associated with a target that meets all requirements of the targeting procedures, NSA may identify information about the target that was not available when the targeting decision was made. This information may show that the target is a USP or is located in the United States, making the target ineligible for targeting. These changes in target status, though not incidents of non-compliance, must be reported.

(U//~~FOUO~~) **Incident reporting and documentation** SV has a significant role in reporting incidents of non-compliance with FAA §702. SV developed an operating procedure that addresses the multiple means of incident discovery and the actions SV personnel follow for each. There are three primary sources from which SV may identify incidents:

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

- (U//~~FOUO~~) Detask notifications—produced by [redacted] when mission personnel remove selectors from collection. A detargeting reason is associated with each notification, some of which may indicate an incident, e.g., the user of the tasked selector has been identified as a USP,
- (U//~~FOUO~~) [redacted] targets that appear to have roamed into the United States, and
- (U//~~FOUO~~) Communications of incidents reported by analysts, query reviewers, and others involved in processing or monitoring collection. This may include errors by communication service providers.

~~(S//SI//REL TO USA, FVEY)~~ For each incident, SV works with personnel familiar with the occurrence to create a permanent record including significant detail about the incident and its resolution, for example, the selector, the intended target, [redacted] method of incident discovery, detasking information, and dates of collection to be purged. SV creates an entry in the database of selectors associated with targets that have roamed into the United States or have been identified as USPs to identify selectors associated with targets identified as meeting certain criteria. [redacted] generates a notice to analysts entering TRs. This entry is required when incidents identify a target located in the United States, [redacted] or a target identified as a USP.

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

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

(U//~~FOUO~~) TV is responsible for overseeing the reporting and mitigation of incidents that affect TD personnel and systems. For each incident, information regarding the incident's root cause and mitigation is gathered and documented. There are four primary ways in which incidents in TD are discovered:

- (U//~~FOUO~~) Technical personnel or analysts find data that is not protected, labeled, or transferred as expected,
- (U//~~FOUO~~) Audits of queries submitted by TD personnel are reported when they do not comply with the minimization procedures,
- (U//~~FOUO~~) Upon analysis of a system for TV certification, instances of potential non-compliance are reported, and
- (U//~~FOUO~~) Technical personnel self report incidents.

(U//~~FOUO~~) SV and TV provide the incident reports to OGC to assess whether the incident is a matter of non-compliance with the FAA §702 certifications and targeting and minimization procedures and is reportable to NSA's overseers (see the Oversight section).

(U//~~FOUO~~) **Incident remediation** Several types of activities may be necessary to resolve compliance incidents or changes in status, for example, detasking selectors, purging communications ineligible for retention, recalling disseminated reports based upon communications subject to purge, correcting system errors, and training. The actions taken are documented in the incident report and, if appropriate, the notice of non-compliance filed with the FISC. Depending on the magnitude of an incident of non-compliance (e.g., a system error affecting the functioning of targeting controls), the FISC may require supplemental reports on progress in correcting the matter. SV and OGC coordinate such reports with DoJ and ODNI.

(U//~~FOUO~~) Table 28 summarizes the incident reporting provisions of the FAA §702 targeting procedures and the controls implemented by NSA to maintain compliance. The provisions are documented in the oversight and compliance requirements in the targeting procedures.

(U) Table 28. Incident Reporting Provisions and Controls

(U//~~FOUO~~)

Provision	Control
(U) NSA will conduct ongoing oversight activities and will make necessary reports, including those relating to incidents of non-compliance, to the NSA OIG and OGC.	(U) FAA §702 training addresses incident identification, documentation, and the process for self-reporting. (U//~~FOUO~~) SV and TV document the incident with assistance of the individuals who identified the matter and provide the information to OGC for review. OGC, in turn, forwards the incident to DoJ and ODNI.
(U) NSA will ensure that necessary corrective actions are taken to address identified deficiencies.	(U) The incident report documents measures taken to remediate the incident (e.g., detasking and purge of communications).
(U//~~FOUO~~) NSA will report to DoJ NSD and ODNI incidents of non-compliance (including over collection) by electronic communications service providers within five business days after determining non-compliance.	(U//~~FOUO~~) SV, TV, and OGC manage the incident reporting process to assure that initial reporting is performed within five business days of the identification of non-compliance.

(U//~~FOUO~~)

(U) Collection

(U) NSA's FAA §702 minimization procedures require that collection of information by targeting non-USPs reasonably believed to be outside the United States be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant for the purpose under which the collection was authorized. Steps to assure that acquisition meets this requirement start with target research and approval and the determination that the proposed target meets the criteria for eligibility under FAA §702. NSA has incorporated additional measures in its collection process to comply with this limitation.

(U) Collection mechanisms for FAA §702 communications

(U) NSA has two collection mechanisms for FAA §702. [redacted] (b)(3)-P.L. 86-36 communications are obtained by the FBI through compelled collection from ISPs and include only communications to which a tasked selector is a party. For upstream Internet collection and telephony collection, the communication service providers who control the telecommunications infrastructure over which the communications travel are legally compelled to make available to NSA communications related to tasked selectors. Upstream collection of Internet-based selectors may include communications to or from the tasked selector, as well as communications in which the selector is referenced within an Internet transaction. The latter is called "abouts" collection because the communication is neither to nor from the tasked selector, but "about" the selector, i.e. the selector is contained within the communication. Communications acquired from telephony selectors are only to or from the tasked telephone number (i.e., "abouts" collection is not a factor).

(U) Provisions of FAA §702 certifications—filters

~~(S//SI//NF)~~ NSA's FAA §702 targeting procedures state that, [redacted] (b)(1) (b)(3)-P.L. 86-36 NSA will [redacted] employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located in a foreign country, [redacted]

(U) Collection controls for telephony and upstream Internet communications—communications not to or from the target

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

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

[redacted]

The providers should deliver only communications meeting these criteria to NSA.

(U) Provisions of FAA §702 certifications—analysis of selector targeting status

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

~~(S//REL TO USA, FVEY)~~ NSA's FAA §702 targeting proceedures set forth criteria for initiating collection on a target. Once a target's selector has been placed on collection, the Agency continues to evaluate collection and use other tools to identify changes in the status or location of the target (e.g., change in USP status, such as information that the individual has been granted permanent resident status in the United States or information that the target is entering the United States). If these changes occur or it is determined that the target is no longer producing foreign intelligence, the selector is removed from collection. Changes in targeting status may be processed immediately upon identification in NSA systems [redacted] This requires NSA to employ measures [redacted]

(U) Collection controls—verification that collection is for currently tasked targets

~~(S//NF)~~ For each source of collection, NSA employs processes to determine whether [redacted] are sending communications only for selectors currently tasked and authorized for collection. [redacted]

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

(U//~~FOUO~~) **Collection for telephony selectors** [redacted]

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

[redacted]

~~(TS//SI//NF)~~ **Upstream collection for Internet-based selectors** [redacted]

[redacted]

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

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

~~(TS//SI//NF)~~ A situation known as [redacted] can result in the unintended acquisition of non-target communications [redacted] NSA implemented a verification process to address this situation that is another check performed before upstream Internet communications are forwarded to analyst-accessible repositories for processing. [redacted]

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

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

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

(U) Provisions of FAA §702 certifications—upstream Internet transactions

(U) **Background** Upstream Internet collection includes acquisition of two types of communications not present in downstream collection: "abouts" communications and "multiple communications transactions" (MCTs). "Abouts" communications are those that are not to or from the target selector but whose contents include the selector. For example, if a target's e-mail address is within the body of the Internet communication between other individuals, the communication is "about" the selector. An MCT is an Internet "transaction" that contains more than one discrete communication. If one of those discrete communications is to, from or about a tasked selector and if the active end of the transaction is foreign, the entire MCT transaction will be acquired through upstream Internet collection. This can include other discrete communications that do not contain the tasked selector. If the targeted selector is not the active user in the transaction, the MCT can include other discrete communications that do not contain the tasked selector.

(U) **Provisions** NSA's FAA §702 minimization procedures require NSA to:

take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

(U//~~FOUO~~) Internet transactions that cannot be identified as meeting the above definition must be segregated and retained in an access-controlled repository from which transactions may not be moved, except for processing to render them intelligible, unless they are determined not to contain discrete communications for which the sender and all intended recipients are reasonably believed to be in the United States. Any such transactions moved to data repositories accessible by analysts are required to be identified as having been previously segregated.[68] NSA's FAA §702 minimization procedures also specify that Internet transactions acquired through NSA's upstream Internet collection techniques on or before 31 October 2011 be destroyed upon recognition.

(U) Upstream Internet collection controls—multiple communication transactions

~~(TS//SI//NF)~~ Effective January 2012, NSA implemented a process for analyzing and processing upstream Internet collection to ensure that only MCTs devoid of wholly domestic communications will be forwarded for further analysis. This process applied to all upstream data that had been sequestered starting 1 November 2011.[69] Three criteria are used to sort these communications and determine whether they would be withheld from use by analysts (sequestered in a collection store) or sent to data stores accessible by analysts: the type of communication (discrete or MCT), the active user of the selector, and the location of the active user. The minimization procedures require that sequestered communications be accessible only to specially trained personnel to determine whether they may be authorized for use. [redacted] As NSA reported to the FISC, all FAA §702 upstream Internet transactions acquired before November 2011, whether or not they were MCTs, were deleted. Additional controls are required when MCTs available to analysts are used, for example, to support reporting of foreign intelligence (see the Sharing and Dissemination section).

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

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

[68] ~~(TS//SI//NF)~~ Though the minimization procedures permit NSA to pass previously segregated communication to repositories accessible to analysts, NSA has not done so.

[69] ~~(S//SI//REL TO USA, FVEY)~~ [redacted] the only FAA §702 data forwarded to analyst-accessible repositories was data [redacted] or where the target was the active user. The remainder was sequestered pending development of decision logic to assess MCTs. The data was also excluded from [redacted]

(U) Table 29 summarizes the collection provisions of the FAA §702 minimization procedures and the controls implemented by NSA to maintain compliance.

(U) Table 29. Collection Provisions and Controls

~~(S//SI//NF)~~ (U//~~FOUO~~)

Provision	Control
(U) Acquisition of information by targeting non-USPs reasonably believed to be outside the United States will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the purpose for which it was authorized.	(U//~~FOUO~~) Targeting controls (see Table 26) are the first measures employed to limit collection to communications of targets that meet the requirements of the targeting procedures. The foreignness requirements and the post-targeting analysis of communications serve to minimize collection of communications not authorized for acquisition (e.g., domestic communications). ~~(S//NF)~~ (U//~~FOUO~~) (b)(3)-P.L. 86-36
~~(S//SI//NF)~~ Acquisition of communications not to or from the target will employ an Internet protocol filter on	(U//~~FOUO~~) Internet protocol filtering is performed on collection to verify that at least one end of each transaction is foreign. Only transactions meeting this criterion should be delivered to NSA. ~~(S//SI//NF)~~
(U) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where the active user of the transaction is reasonably believed to be located in the United States or the location of the active user is unknown.	(U//~~FOUO~~) NSA has implemented procedures to analyze upstream Internet collection. Only discrete transactions and MCTs meeting certain criteria are made accessible to analysts.

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

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

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

(U//~~FOUO~~)

~~(S//SI//NF)~~

(U) Repositories

(U) Provisions of FAA §702 certifications—repositories

(U//~~FOUO~~) NSA's FAA §702 targeting procedures require that NSA establish processes for ensuring that raw traffic is labeled and stored only in authorized repositories and is accessible only to those who have had proper training (see the Access and Training section).

(U) Control framework for access to FAA §702 repositories

(U//~~FOUO~~) Several control procedures are employed to ensure that FAA §702 data is stored in repositories that meet standards for security and compliance and that access to the data is properly controlled. From the time of collection, data is processed through interim systems before it reaches the [redacted] approved source systems for FAA §702 reporting.[70] The remainder of this section describes four types of controls, focusing on their application to the [redacted]

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

- (U//~~FOUO~~) System security accreditation,
- (U//~~FOUO~~) System certification,
- (U//~~FOUO~~) Data flow management, and
- (U//~~FOUO~~) Data tagging.

(U//~~FOUO~~) Approval for NSA systems to store and process FAA §702 data

(U//~~FOUO~~) **Accreditation** TS is responsible for managing the risk on all NSA networks and the computer systems and devices connected to those networks. TS's responsibilities include:

- (U//~~FOUO~~) Guiding, prioritizing, and overseeing the development of information assurance programs necessary to ensure protection of information systems and networks by managing the NSA Information Security Program,
- (U//~~FOUO~~) Serving as the Director NSA Authorizing Official to accredit all NSA information systems,
- (U//~~FOUO~~) Conducting information systems security and accreditation and risk management programs, and
- (U//~~FOUO~~) Establishing, maintaining, and enforcing NSA information systems security policies and implementation guidelines.

(U) Accreditation is the official management decision to permit operation of information systems in specific environments at acceptable levels of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

(U//~~FOUO~~) When accrediting systems, TS uses the National Institute of Standards and Technology (NIST) Risk Management Framework to determine the appropriate level of risk mitigation to protect systems, information, and infrastructure. NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010, describes the six steps in the framework.

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

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

- (U//~~FOUO~~) Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis (risk assessment),
- (U//~~FOUO~~) Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions,
- (U//~~FOUO~~) Implement the security controls and describe how the controls are employed within the information system and its environment of operation (system developers),
- (U//~~FOUO~~) Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (independent testing by TS),
- (U//~~FOUO~~) Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the information system and the decision that this risk is acceptable, and
- (U//~~FOUO~~) Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

(U//~~FOUO~~) Before a system is authorized to be put on a network, it must go through the accreditation process and be approved by TS. Once implemented, systems are subject to reaccreditation every three years or when significant changes occur that may affect the risk assessment. The dates through which the FAA §702 repositories are accredited are listed in Table 30. (b)(3)-P.L. 86-36

(U//~~FOUO~~) Table 30. Accreditation Status of NSA [redacted]

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

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

System named in the System Security Plan (SSP)	Content	SSP Accredited Through

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

(U//~~FOUO~~) **Certification** In addition to system accreditation, all systems containing FISA data must be certified by TV4, the NSA authority for certifying automated systems to ensure they are compliant with the legal and policy regulations protecting USP privacy. DoJ and the FISC are notified when NSA designates a new [redacted]

(U//~~FOUO~~) In 2010, NSA began certifying FISA systems as part of an effort to ensure that they comply with the legal and policy regulations protecting USP privacy. This included the repositories that contain FAA §702 metadata. Personnel from various organizations within SID and TD performed the initial certifications. TV subsequently assumed responsibility for system certification and developed the NSA corporate database for registering NSA systems, their compliance certification, and data flows. It is NSA's authoritative source for all compliance certifications.

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

(U//~~FOUO~~) The Agency's certification process currently evaluates system controls for compliance with purge, data retention and age-off, data access, querying, dissemination, data tagging, targeting, and analytical processes. These mission functional areas are defined by the Comprehensive Mission Compliance Program ODOC administers. Through this program, compliance certification requirements are developed to address required compliance controls. The compliance requirements, administered by the TV2 requirements team, form the basis for the criteria against which systems are certified for compliance.

(U//~~FOUO~~) To be certified to handle FISA data, systems must receive TV certification through the Compliance Certification process. The TV4 certification dates for the [redacted] that contain FAA §702 data and which can be used as sources to support dissemination are listed in Table 31.

(U//~~FOUO~~) Table 31. Compliance Certification Status of NSA [redacted] (b)(3)-P.L. 86-36

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

System	Content	Certification Date

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

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

(U//~~FOUO~~) TV provided new compliance certification guidance in May 2014. Systems other than those being decommissioned within twelve months, which meet the following criteria, should be recertified by TV: (b)(3)-P.L. 86-36

- (U//~~FOUO~~) Systems with two significant system-related incidents in a twelve month period or three total,
- (U//~~FOUO~~) FISA systems that have not been certified within two years,

- (U//~~FOUO~~) Systems with a major upgrade affecting compliance functionality, or
- (U//~~FOUO~~) Systems planning to process under a new authority (e.g., addition of FISA data).

(U//~~FOUO~~) Owners of all affected FISA systems were notified in June 2014 that they should complete recertification, if their systems met these guidelines, within six months. [redacted] of the repositories [redacted] are scheduled to be decommissioned and were exempted from this requirement. (b)(3)-P.L. 86-36

(U) Data flow management

~~(C//REL TO USA, FVEY)~~ USSIDs define a set of controls and operating procedures for the United States SIGINT System. USSID DA3511, *Data Acquisition Directorate Targeting and Data Flow Management*, defines a process intended to assure that only desired SIGINT is delivered to intended users in the time frame and format required.

~~(S//SI//REL TO USA, FVEY)~~ [redacted] is responsible for governing end-to-end management of Internet and telephony data collection. [redacted] houses the access data managers responsible for testing and setting up new data flow paths that traverse the SID processing infrastructure. The [redacted] Data Governance Team governs the processing and distribution of data collected within NSA's SIGINT system, oversees the documentation and review of all new dataflow requests, and implements processes designed to ensure that NSA compliance standards are maintained throughout the development of new data flows. (b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ The Data Governance Team manages the data flow process. Customers must complete Dataflow Management Requests (DMR) to initiate or modify data flows. DMRs require detailed information, including the status of system certifications, system accreditation plans, types of data to be processed [redacted] authorities for collection, and documentation of data flows. DMRs are evaluated and approved by a triage team [redacted] Upon triage team concurrence, the DMR is given to the [redacted] Targeting and Tasking and [redacted] Data Delivery organizations for testing and implementation. DMRs are complete once all required approvals are obtained and data flows become operational. (b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

(U) Data tagging

(U//~~FOUO~~) Historically, NSA has managed data access by implementing restrictions on data storage, including the use of logical database partitions. Data flows were designed to place data in these partitions, for example, according to the FAA §702 certification under which the communications were acquired. To access the data, personnel had to have appropriate training and be given access to certain systems and missions matching the data partitions where the data was stored.

(U//~~FOUO~~) As NSA [redacted] new mechanisms for storing and accessing data are being developed. Data tags are created for each collection record, identifying the authority under which the data was collected, as well as several other pieces of information used in managing the data over its life cycle.[71] [redacted] Thus, to access raw data acquired under the [redacted] certification for FAA §702, analysts must be approved for access to such collection as part of an authorized mission and fulfill the training requirements for the authority. (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36

(U//~~FOUO~~) Data tags also serve to maintain compliance with limitations on the scope of queries, as well as age-off and purge requirements.

(U//~~FOUO~~) Table 32 summarizes the repository provisions of the FAA §702 targeting and minimization procedures and the controls NSA implemented to maintain compliance.

(U) Table 32. FAA §702 Repository Provision and Controls

(U//~~FOUO~~)

Provision	Control
(U//~~FOUO~~) NSA has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories.	(U) All systems processing FAA §702 data must complete a security accreditation process. (U) All FAA §702 repositories are certified compliant with the legal and policy regulation protecting USP privacy. (U//~~FOUO~~) Data flows must be approved by [redacted] and SV to ensure compliance. (U//~~FOUO~~) Data tags are applied to identify the authority under which the information was acquired. The tags also serve to manage access to and retention of the data. [redacted]

(U//~~FOUO~~)

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

(U) Access and Training

(U) Provisions of FAA §702 certifications

(U) The FAA §702 targeting procedures state that NSA will develop and deliver training to ensure that intelligence personnel responsible for approving the targeting of persons under that authority, as well as analysts with access to the raw data acquired pursuant to FAA §702, understand their responsibilities and the procedures that apply to this acquisition.

[71] ~~(C//REL TO USA, FVEY)~~ [redacted]

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

(U) **Control framework for restricting access to FAA §702 collection to authorized personnel**

~~(TS//SI//NF)~~ NSA requires that users having access to FAA §702 data have one or more credentials, be current on the required training, and be assigned to approved missions.

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

~~(TS//SI//NF)~~ **Required credential** One [redacted] credentials is needed to access FAA §702 data: [redacted] is required to access data collected under the [redacted] FAA §702 certifications. [redacted][72]

~~(C//REL TO USA, FVEY)~~ **Obtaining the credential** To obtain any of the [redacted] credentials, a request must be submitted in [redacted] Only individuals who hold the requested credential may submit someone for the credential. The request is first reviewed by the Associate Directorate for Security and Counterintelligence (Q) to determine whether the applicant has satisfied certain security criteria. If approved by Q, the request is forwarded to SV for final adjudication. SV reviews the request, verifying that the individual is current on required training and that the request includes a valid mission justification. If all requirements are met, SV approves the credential in [redacted] for entry to NSA's security database. [redacted] retrieves information from [redacted] and several other corporate authoritative source systems that provide the status of individuals' approved missions, training, and clearances. Using this information, [redacted] calculates daily a list of individuals who qualify for FAA §702 access. NSA systems use the information from [redacted] to determine what data the individuals are authorized to access. SID maintains the authority rules, which determine what [redacted] verifies for individuals to access data.

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

(U//~~FOUO~~) **Obtaining access to mission resources** SID policy designates [redacted] as NSA's tool for the proper administration and implementation of access to SIGINT data in NSA repositories; it facilitates the administrative process of acquiring access to tools and databases. Access sponsors submit individuals for access. The sponsors determine the appropriate SIGINT authority for users, assigning them to a mission documented in the mission correlation table, a master list of all analytic production elements that have been approved for SIGINT missions. The table facilitates database access by providing a record of databases needed to perform SIGINT missions. The access sponsor nominates a user for access to raw SIGINT databases, sources, and tools in support of a stipulated mission. The sponsor ensures that auditors are assigned to the mission to review queries of mission auditable data. [redacted] feeds user access information to [redacted]

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

[72] (U//~~FOUO~~) The [redacted] credential was originally established for FISA data and requires training in NSA's Standard Minimization Procedures for FISA information. Later, different versions of [redacted] were established for particular categories of FISA. [redacted] permits access to FAA §702 data acquired before the establishment of the [redacted] credential in [redacted]

(U//~~FOUO~~) **Maintaining access** Automated and manual procedures provide assurance of continuing eligibility to access FAA §702 data. Users and access sponsors are responsible for removing users' access when they no longer qualify for a mission. Each [redacted] mission is also required to have an intelligence oversight officer who performs periodic reviews to ensure that individuals assigned to missions are still eligible for access.

(U//~~FOUO~~) Enforcement of required training is supported by the production of automated notices to individuals well in advance of their training expiration date. Notices are produced at regular intervals until the training is completed. If training expires, the individual is automatically removed from access to FAA §702 data.[73]

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

~~(C//REL TO USA, FVEY)~~ [redacted] calculates daily a list of individuals who qualify for FAA §702 access. [redacted] interfaces with several corporate authoritative source systems that provide the status of individual's approved missions, training, and clearances. For systems that use data tags, user information in [redacted] is compared with the data tags applied to the communications before giving the individuals access to the data. If the user does not possess the combination of requirements identified in the data tag, access to that data is denied.

(U//~~FOUO~~) **Appropriate and adequate training** NSA/CSS Policy 1-23 requires that Agency personnel complete IO training annually.

(U//~~FOUO~~) To qualify for access to data acquired under an FAA §702 certification, persons must have completed specific training courses within the last 12 months. All courses are developed by NSA's ADET in conjunction with the OGC, mission subject matter experts, and mission compliance professionals. All NSA analysts who perform targeting functions must take the first three courses listed next; the last is mandatory only for personnel requiring access to FAA §702 data.

- (U//~~FOUO~~) OVSC1000 - NSA/CSS Intelligence Oversight Training - the Agency's core IO course, provided to the workforce to maintain a high degree of sensitivity to and understanding of intelligence laws, regulations, and policies associated with the protection of U.S. person privacy rights. Personnel are familiarized with the major tenets of the four core IO documents: Executive Order 12333, as amended, Department of Defense Regulation 5240.1-R, Directive Type Memorandum 08-052, and NSA/CSS Policy 1-23. OVSC1000 is web-based and includes knowledge checks for proficiency.[74]
- (U//~~FOUO~~) OVSC1100 - Overview of Signals Intelligence Authorities - the SIGINT core IO course, provides an introduction to various legal authorities

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

[73] (U//~~FOUO~~) [redacted] does not verify the individuals' FAA §702 training status. [redacted]

[74] (U//~~FOUO~~) E.O. 12333, *United States Intelligence Activities*; DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons*; DTM-08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*.

governing NSA operations. Upon completion, personnel should be able to identify applicable surveillance authorities at a high level, define the basic provisions of the authorities, and identify situations requiring additional authority. OVSC1100 is web-based and includes knowledge checks for proficiency. All personnel in the U.S. SIGINT System (USSS) working under NSA SIGINT authority with access to raw SIGINT are required to complete OVSC1100.

- (U//~~FOUO~~) OVSC1800 - *Legal Compliance and Minimization Procedures* - an advanced SIGINT intelligence oversight course which explains policies, procedures, and responsibilities within missions and the obligations of the USSS to protect U.S. person and foreign partner privacy rights. OVSC1800 is web-based and includes competency exams [redacted] Personnel who do not pass the test after [redacted] attempts must complete remedial training. All analysts in the USSS working under DIRNSA SIGINT authority with access to raw SIGINT are required to complete OVSC1800 annually. (b)(3)-P.L. 86-36
- (U//~~FOUO~~) OVSC1203, FISA Amendments Act (FAA) Section 702, explains the legal policies and targeting and minimization procedures FAA mandates. The course is web based and includes a competency exam [redacted] Personnel who do not pass the test after [redacted] attempts must complete remedial training. All analysts who require access to FAA §702 data must take this course annually.

(U//~~FOUO~~) Other courses are also required before analysts can access NSA targeting tools. The first four of these are required for all NSA analysts who perform targeting functions, while the last is mandatory only for those analysts targeting under FAA §702.

- (U//~~FOUO~~) CRSK1300, Foundations of Smart Targeting, a web-based course that covers targeting policy, processes and concepts, available assistance, targeting tools, research, and collection.
- (U//~~FOUO~~) CRSK1301, Foundations of Smart Targeting: Research, available in web-based format beginning January 2015, the course focuses on elements of the targeting process requiring research, the research process, and the tools and databases used in research.
- (U//~~FOUO~~) CRSK1302, Foundations of Smart Targeting: Targeting, a web-based course that includes collection source considerations, the target workflow process, creating TRs, finding and assessing collection results, and documenting sources.
- (U//~~FOUO~~) CRSK1303, Foundations of Smart Targeting: Targeting Maintenance, a web-based course that focuses on resolving compliance problems, managing traffic, and maximizing the intelligence value of tasked selectors.

- (U//~~FOUO~~) CRSK1304, FAA Section 702 Practical Applications, a web-based course required for all NSA analysts who conduct targeting under FAA §702. It is scenario-based and addresses compliant TRs, targeting maintenance, and incident reporting.

(U//~~FOUO~~) **Adjudicator training** In addition to the above courses, mission personnel who grant final approval of FAA §702 TRs must take a course on the approval process, be approved by their FAA §702 mission lead, receive hands-on training by personnel with adjudication experience, and be approved by S2 Mission and Compliance staff. Upon approval, elements in SID will upgrade the individual's access role in [redacted] to allow adjudication of TRs. (b)(3)-P.L. 86-36

- (U//~~FOUO~~) CRSK1305 - FAA Section 702 Targeting Adjudication – a course that explains NSA resources for validating selectors and foreignness explanations in [redacted] TRs, determining whether submitted TRs should be approved, and follow-up actions after a TR has been approved or denied.

(U) **Access requirements for technical personnel to FAA §702 repositories**

(U//~~FOUO~~) Technology Directorate personnel who directly support repositories and systems that contain raw SIGINT data or activities that utilize raw SIGINT must complete OVSC1000, OVSC1100, and OVSC1806 training annually. OVSC 1806 is the same course as OVSC1800 (see above) but has an additional lesson on the system compliance certification process. Technical personnel who support FISA systems and whose responsibilities may include direct access to FISA data are also required to attend a briefing administered by OGC and TV. Upon completion of the briefing, SV updates [redacted] recording the user's attendance at the briefing and their authorization for access.

(U) Identification of access vulnerability in [redacted]

(U//~~FOUO~~) [redacted] is one of the [redacted] scheduled to be decommissioned in 2017. [redacted] relies on a combination of [redacted] to protect access to data.[75] [redacted] does interface with [redacted] however, it does not verify that an individual is current on training as part of its access control.[76] (b)(3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~ [redacted] an individual with authorized access to FISA data discovered that FAA §702 data had been included in the results of a query of [redacted] data. The individual had received FAA §702 training when she was

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

[76] (U//~~FOUO~~) [redacted] is NSA's Corporate Authorization Service. See the Obtaining the Credential section for more information on [redacted] (b)(3)-P.L. 86-36

assigned to a different mission so her access to the data was not in violation of the FAA §702 targeting and minimization procedures. However, the access did violate SID policy because the mission to which the individual was assigned was not authorized for FAA §702.[77] Investigation of the occurrence led to the discovery that personnel without the required FAA §702 training could access FAA §702 data in [redacted] if they have the [redacted] credential.[78] To date, no incidents have been identified of individuals who have not received FAA §702 training querying [redacted] and receiving FAA §702 data.[79]

(U//~~FOUO~~) When SV personnel discovered this vulnerability, they worked with TD to initiate corrective measures. [redacted] was updated to add new COIs to FAA §702 data collected on or after that date. The new COIs emulate the access controls required for other FAA §702 systems, including controlling access based upon the authority under which it was obtained. [redacted] a similar process will be implemented to address access controls for data obtained [redacted] A review is currently underway regarding action to take for data [redacted]

(U//~~FOUO~~) Table 33 summarizes the access and training provisions of the FAA §702 targeting procedures and the controls implemented by NSA to maintain compliance.

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

(U) Table 33. Access and Training Provisions and Controls

(U//~~FOUO~~)

Provision	Control
(U) NSA will develop and deliver training regarding the applicable procedures to ensure that intelligence personnel responsible for approving the targeting of persons under FAA §702, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition.	(U//~~FOUO~~) NSA has a list of courses required annually for analysts to qualify for access to data acquired under FAA §702. This includes OVSC1203, a course specific to FAA §702. (U//~~FOUO~~) To access NSA targeting tools, all analysts must complete four courses on targeting. Analysts targeting under FAA §702 must also take a course on application of the authority. (U//~~FOUO~~) Adjudicators (who grant the final approval of TRs under FAA §702) must also complete a course on adjudication specific to the authority. (U//~~FOUO~~) Technology Directorate personnel who support FISA systems must complete OVSC1000, 1100 and 1806 annually and attend a briefing administered by OGC and TV.

[77] ~~(C//REL TO USA, FVEY)~~ SID Management Directive 421 states that FISA access is based on current mission need and does not follow individual analysts when they move to new missions or locations unless specified in the document authorizing the assignment. Persons changing missions, jobs, or locations must provide re-justification to SV through their management chains for FISA access or access to unminimized, unevaluated content in the new positions.

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

[78] (U//~~FOUO~~) Without a [redacted] credential, analysts cannot access FAA §702 data and most other types of FISA data. The [redacted] credential was originally established for FISA data and requires training in NSA's standard minimization procedures for FISA information.

[79] ~~(TS//SI//NF)~~ Of NSA's [redacted] SIGINT missions authorized for FISA access, [redacted] are also authorized to access FAA §702 data.

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

(U) NSA has established processes to ensure that raw traffic is accessible in authorized repositories only to those who have had the proper training.	(U//~~FOUO~~) Access to FAA §702 foreign intelligence and the ability to submit and approve targeting under the authority require certain credentials and access to mission resources (databases, sources and tools). The approval is not granted unless the required training has been completed. (See above information regarding [redacted] access.)

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

(U//~~FOUO~~)

(U) Querying Repositories of Collected FAA §702 Data

(U) Provisions of FAA §702 certifications—q ueries

(U) Minimization procedures permit use of computer selection terms to scan storage media containing communications acquired pursuant to FAA §702 and to select communications for analysis with certain limitations. Query selection terms (e.g., telephone numbers and key words and phrases) must be formed in a manner reasonably likely to return foreign intelligence information. Collection obtained through NSA upstream Internet collection techniques may not be queried using selection terms of an identifiable USP.

(U) Compliance controls—query compliance

(U//~~FOUO~~) Queries of raw SIGINT databases are subject to USSID CR1610, *SIGINT Production and Raw SIGINT Access*, revised 12 February 2013, which requires that:

- (U//~~FOUO~~) All user organizations designate two auditors to review daily those queries presented for their review,[80]
- (U//~~FOUO~~) Auditors be familiar with the targets and types of queries executed within their missions,
- (U//~~FOUO~~) SV provide training for new auditors on their responsibilities and certify them as compliant before conducting audits,[81]
- (U//~~FOUO~~) SV conducts periodic super audits of interactive raw SIGINT database queries, verifying that selectors were foreign on the date the super audit is performed and examining the query terms to determine compliance with NSA policy,[82]
- (U//~~FOUO~~) NSA maintain a non-editable file of all such database queries for a minimum of one year,

---

[80] (U//~~FOUO~~) [redacted] NSA implemented an approach to query review that uses stratified sampling based upon historical rates of queries identified as "reportable" to determine the queries from each database to be presented for auditor review. The [redacted] system passively logs queries, but the queries are not subject to audit. NSA is developing a process to provide additional oversight for queries against this system.

[81] (U//~~FOUO~~) Auditors are now required to take *NSA Raw Traffic Database Auditor Training* (OVSC3101) every two years and must be cleared to the security level required for the authority under which the analyst performed the query subject to audit.

[82] (U//~~FOUO~~) The system used to test foreignness [redacted] does not maintain an historical record of foreignness of the tasked selector.

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

- (U//~~FOUO~~) All queries be driven by a foreign intelligence purpose, and
- (U//~~FOUO~~) An audit record of the selection terms be created and reviewed per NSA policy by the originating organization.

(U//~~FOUO~~) Mission auditors are assigned to each mission using the [redacted] tool described in the access section. The tool requires that missions have designated auditors before new personnel can be approved for the missions. Auditor qualifications include target knowledge expertise in the mission area, familiarity with the type of queries to be reviewed, ability to mentor analysts to improve query execution, attainment of all credentials required for the data reviewed, and completion of all required training. Queries presented to auditors are required to be audited within 24 hours of receipt or on the next normal duty day.

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

(U//~~FOUO~~) SV developed OVSC3101, *NSA Raw Traffic Database Auditor Training*, to prepare auditors for post-query review. The course provides instruction on use of the corporate query audit system, incident identification, incident reporting, and maintenance of records of audits (to support SV super audits and DoJ/ODNI reviews).

~~(S//SI//REL TO USA, FVEY)~~ The [redacted] system, a legacy system which predates USSID CR1610 and is scheduled to be decommissioned, does maintain a log of queries for five years. The system has not yet been modified to provide these query logs to the corporate logging and auditing system. [redacted] SV is developing a procedure to perform audits of these queries.

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

(U//~~FOUO~~) Queries not using USP selection terms

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

(U//~~FOUO~~) FAA §702 systems provide records of queries to the corporate logging and auditing system for user generated queries of raw SIGINT content.[83] These records are the source for daily post-query reviews by auditors and SV query oversight. These systems also maintain records of query reviews.

(U//~~FOUO~~) Auditors examine queries to determine whether they have a valid foreign intelligence purpose. Auditors also evaluate query selection terms to determine whether they were constructed so as to avoid obtaining information on USPs. The review is intended to balance the pursuit of foreign intelligence and protection of USPs' Fourth Amendment rights. When a tasked FAA §702 selector is used as a query term and the selector is foreign, the corporate query logging and auditing system does not present the query for review by an auditor because the term has been reviewed by a releaser and an adjudicator as part of the TR approval for tasking during the targeting process.[84] If a tasked selector is used as a query term and the

[83] (U//~~FOUO~~) One of the [redacted] does not send query records to the NSA corporate logging and auditing system. This system is scheduled to be decommissioned.

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

[84] (U//~~FOUO~~) The query auditing and logging system obtains current tasked selectors from [redacted] and verifies their foreignness against NSA SIGINT databases.

selector is not foreign, it is subject to review by an auditor. Queries using selection terms that are not approved selectors are subject to auditor review.

(U//~~FOUO~~) Provisions of FAA §702—queries using USP selection terms

(U//~~FOUO~~) A 3 October 2011 FISC Order approved the use of modified minimization procedures that permit queries of data collected under the authority only for foreign intelligence purposes, using USP query terms subject to specific NSA review procedures and external oversight. Such queries can only be performed using FAA §702 telephony communications and Internet communications obtained from downstream collection. Use of USP identifiers to query FAA §702 collection must be approved in accordance with NSA procedures. NSA is required to maintain records of all USP identifiers approved for use as selection terms. These query procedures are subject to oversight by DoJ and ODNI.

(U//~~FOUO~~) Compliance controls—queries with USP selection terms

(U//~~FOUO~~) NSA adopted internal procedures governing use of USP identifiers for queries of communications collected under FAA §702. Upstream Internet collection is not approved for such queries. DoJ and ODNI reviewed and approved these procedures. The Senate and House Intelligence Committees were informed of these changes. There are three sets of procedures for approval of these queries:

- (U//~~FOUO~~) Queries of metadata,
- (U//~~FOUO~~) Emergency queries of content, and
- (U//~~FOUO~~) Non-emergency queries of content.

(U//~~FOUO~~) NSA's annually required course on FAA §702, OVSC1203, includes training on the use of USP identifiers to query raw data collected under the authority. The NSA FAA web page also contains the documented and approved procedures for these queries. Although metadata queries are not subject to pre-approval, the query and a foreign intelligence justification must be recorded to support external oversight. The justification must document the analytic knowledge linking the selector to a foreign target or foreign intelligence purpose. Content queries using USP identifiers are subject to pre-approval by S2, SV, and OGC. SV maintains records of all queries using USP identifiers and includes such queries in its query oversight.

(U) Table 34 summarizes the query provisions of NSA's FAA §702 minimization procedures and the controls implemented by NSA to maintain compliance.

(U) Table 34. Query Provisions and Controls

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

Provision	Control
(U) Storage media (data repositories) containing communications acquired pursuant to FAA §702 may be queried to identify and select communications for analysis. Query terms, such as telephone numbers and key words or phrases, will be limited to those selection terms reasonably likely to return foreign intelligence information.	(U) Queries of FAA §702 databases may only be conducted for foreign intelligence purposes and are subject to review by mission auditors who must have target knowledge expertise in the mission area and have completed training on raw traffic database auditing. The review evaluates whether the query was for a valid foreign intelligence purpose. (U//~~FOUO~~) SV conducts periodic super audits of these queries. ~~(S//SI//REL TO USA, FVEY)~~ NSA maintains a file of all database queries for at least one year in the corporate logging and auditing system for user generated queries of raw SIGINT content. [redacted]
(U) Identifiers of an identifiable USP may not be used as terms to query any Internet communication acquired through upstream Internet collection. Use of USP identifiers as terms to query communications must be approved in accordance with NSA procedures. NSA will maintain records of all USP identifiers approved for use as selection terms.	(U//~~FOUO~~) All personnel receive annual training on USP query procedures which can only be performed for foreign intelligence purposes against FAA §702 telephony communications and Internet communications [redacted] The SV web page provides instructions for requesting approval of such queries, using a process that DoJ and ODNI approved. (U//~~FOUO~~) Queries of upstream Internet collection using USP terms are prohibited. (U//~~FOUO~~) Queries of metadata are not subject to pre-approval, but the query and foreign intelligence justification must be documented. (U//~~FOUO~~) Content queries using USP terms follow request and documentation procedures and are subject to pre-approval by SV and OGC. (U//~~FOUO~~) SV maintains records of all queries using USP identifiers and includes these queries in its oversight of query review.
(U//~~FOUO~~) DoJ and ODNI will conduct oversight of NSA's queries using USP identifiers.	(U) See the Oversight section.

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

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

(U) Sharing and Dissemination

(U) Sharing

(U//~~FOUO~~) As stated in the Access and Training section, targeting procedures require that all personnel accessing or otherwise handling raw data acquired pursuant to FAA §702 must be current on training for the authority. This imposes restrictions even within NSA on the use of information obtained under this authority.

(U) Unminimized communications acquired pursuant to FAA §702 may be provided to the CIA and FBI for targets each has identified to NSA. Each agency has minimization procedures for handling data collected under this authority and must

handle communications provided by NSA in accordance with those procedures. Currently, unminimized data shared with the CIA and FBI is limited to communications derived from downstream collection.

(U) Dissemination

(U) The NSA minimization procedures apply to dissemination of all information acquired under FAA §702, including non-publicly available information concerning USPs acquired by targeting non-USPs approved under the NSA targeting procedures. There are several restrictions on dissemination of information acquired under this authority.

- (U//~~FOUO~~) **Discrete Communications within an MCT** Analysts seeking to disseminate information obtained from a discrete communication within an MCT must assess whether the communication is eligible for dissemination (e.g., not a domestic communication) and document that assessment in the comments field of the reporting tool in a manner that supports internal and external oversight.
- (U//~~FOUO~~) **Attorney-Client Communications** Dissemination of USP attorney-client privileged communications must be reviewed by the NSA OGC. NSA must cease review of communications between a person known to be under criminal indictment in the United States and an attorney representing that individual in that matter, segregate such communications, maintain a record of the identified attorney-client communications, and notify DoJ so that appropriate procedures may be established to protect such communications from review or use in a criminal prosecution, while preserving foreign intelligence information in the communication.
- (U//~~FOUO~~) **Domestic Communications** A domestic communication may only be disseminated if DIRNSA has approved a destruction waiver for that communication, documenting its eligibility for retention and dissemination. Such communications must contain information that meets one of four criteria: significant foreign intelligence, technical database information necessary to assess a communication's vulnerability, evidence of a crime, or information concerning a threat of serious harm to life or property. Communications acquired when there was no reasonable belief at the time of tasking that a target was a non-USP located outside the United States are not eligible for destruction waivers. If a waiver has been obtained, NSA may share domestic communications that do not have foreign intelligence value but are believed to contain evidence of a crime with appropriate federal law enforcement authorities in accordance with applicable laws and regulations.[85] Without a destruction waiver, NSA is authorized to notify the FBI if information in a domestic communication indicates that a target has entered the United States. The Agency may also provide information to the CIA and

[85] (U) 50 U.S.C. §§1806(b) and 1825(c) require that the communications be released with a statement that the Attorney General must approve use of the information in a criminal proceeding. USC §1806(b) is not limited to FAA §702 domestic communications; it applies to all disseminations to law enforcement.

FBI for collection avoidance purposes. NSA may retain domestic communications shared with the CIA and FBI for six months and must restrict further use or dissemination of communications whose destruction has been waived by placing the identifiers for these communications on the MPL.

- (U) **Foreign Communications of or Concerning USPs** These communications may be disseminated, if the identity of the USP is deleted and a generic term substituted so that the information cannot reasonably be connected with an identifiable USP. This process is referred to as "masking." Otherwise, dissemination of intelligence based on such communications may only be made to recipients requiring the identity of the USP to perform their official duties and only if at least one of eight additional requirements is met:
  - (U) The USP consented to dissemination or the information is publicly available,
  - (U) The USP identity is necessary to understand the foreign intelligence information or assess its importance,
  - (U) The communication or information indicates that the USP may be a foreign power, an agent of a foreign power, residing outside the United States and holding an official position in the government or military forces of a foreign power, a corporation or other entity owned or controlled directly or indirectly by a foreign power, or acting in collaboration with an intelligence or security service of a foreign power and the USP has or has had access to classified national security information or material,
  - (U) The USP may be the target of intelligence activities of a foreign power,
  - (U) The USP is engaged in unauthorized disclosure of classified national security information (only if the originating agency has verified that the information has been properly classified),
  - (U) The USP communication was authorized by a court order and the communication may relate to the foreign intelligence purpose of the surveillance,
  - (U) The USP may be engaging in international terrorist activities, or
  - (U) There is evidence that the USP is engaging in a criminal activity.
- (U) **Foreign Communication of or Concerning a Non-USP** may be disseminated in accordance with other laws, regulations, and policies, provided that the communications are eligible for retention under FAA §702.
- (U) **Collaboration with Foreign Governments** Consistent with the authority accorded NSA by E.O. 12333, the Agency maintains cryptologic liaison relationships with certain foreign governments. Information derived from FAA §702 collection that has been evaluated for foreign intelligence and minimized for USP information may be disseminated to these foreign

governments. [86] Dissemination of information of or concerning a USP must comply with the restrictions described in Foreign Communications of or Concerning USPs above, as well as with those described for MCTs above. NSA is permitted to disseminate unminimized communications to foreign partners to obtain technical or linguistic assistance to determine the meaning or significance of the information. [87]

(U) Sharing FAA §702 with authorized NSA personnel

(U//~~FOUO~~) Analysts authorized to access FAA §702 communications are trained to ensure that individuals with whom they wish to discuss such communications have appropriate credentials. [redacted] permits review of an individual's training and clearances. The training also addresses NSA policy which states that e-mailing unminimized and unpublished data to anyone, even other NSA personnel, violates compliance controls, such as effective auditing.

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

(U) Provision of unminimized communications to CIA and FBI

(U//~~FOUO~~) As described in the Targeting section, NSA must approve selectors nominated by these agencies based upon compliance with NSA targeting procedures. For approved selectors, Internet communications [redacted] are routed to the requesting agency [redacted] based upon information in the TR. NSA policy states that analysts should not share unminimized and unevaluated communications received pursuant to this collection with the CIA and FBI for selectors tasked on behalf of those agencies; collaboration on such collection is permitted when analysts from the CIA or FBI access the unminimized communications from their own agencies' FAA §702 data repositories. The required annual FAA §702 course, OVSC1203, provides training on these restrictions which are designed to assure accountability of dissemination if recall or purge becomes necessary.

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

(U) General dissemination requirements

(U//~~FOUO~~) **Limits on use of reported FAA §702 communications** Analyst training (OVSC1203) instructs that "use or disclosure of information derived from FAA §702 communications in any criminal proceeding, immigration proceeding, or any other legal or administrative proceeding is prohibited without the advance authorization of the Attorney General of the United States." To prevent such use, NSA internal procedures require that disseminations of FAA §702 derived information include the "Intelligence Purposes Only" caveat that prohibits use of the information without approval. This is included in the FAA §702 training.

---

[86] (U//~~FOUO~~) Collected traffic that has been evaluated to determine whether it contains foreign intelligence and has been subject to minimization to protect USP identities is referred to as evaluated minimized traffic or EMT.

[87] (U) Dissemination for technical or linguistic assistance is subject to specific restrictions limiting the use of the information by the foreign government to translation or analysis of the communications, allowing dissemination only to the individuals performing the analysis or translation, restricting the foreign government from making a permanent record of the information, and requiring destruction or return to NSA of the information disseminated.

(U//~~FOUO~~) **Reporting documentation** Consistent with the purge requirements in the minimization procedures, NSA is required to account for and must be able to trace its disseminations based on FAA §702 communications. The annual training addresses the documentation that analysts must complete to fulfill this requirement:

- ~~(S//NF)~~ The collection authority (specific FAA §702 certification [redacted] for each piece of traffic used in the report, and (b)(3)-P.L. 86-36
- (U) A source verification statement documenting an identifier for each piece of traffic and confirming that the source was not ineligible for retention or subject to purge. A new reporting tool, first introduced in 2013, performs the source verification automatically. Successful completion of this process with no flags confirms the traffic may be used as a source for reporting.

~~(S//SI//REL TO USA, FVEY)~~ An NSA reporting policy document, *Sourcing Requirement and Verification Guidance,* ISS-054-10, revised 8 May 2012, provides reporting and dissemination guidance. The policy requires that individuals releasing reports verify that the reports do not contain information that should have been purged from raw SIGINT databases. This must be performed within 24 hours of the report release using the Master Purge List. SIGINT reporters are also required to include traffic source identifiers for all reports and enter source verification statements in the reporting tool to confirm that this review has been performed.

~~(S//SI//REL TO USA, FVEY)~~ The primary analyst reporting tools used in 2013 performed automated verification of sources against NSA's [redacted] at the time of report release. If none of the source records for the report matched records in the purge system, the report would be released. If a match to the identifier for a purged record was found, the release would be stopped and the individual releasing the report would be notified. The policy requires that a manual source verification check be performed for reports released through means without automated source verification. In 2014, a new analyst reporting tool was implemented that also includes automated source verification (see the Purge section).

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

(U) Disseminating communications involving MCTs

(U//~~FOUO~~) The FAA §702 annual training course, OVSC1203, addresses procedures that analysts must perform for upstream Internet collection containing MCTs to comply with the minimization procedures. The training identifies the requirements for disseminating single discrete communications within MCTs. The course also explains requirements for documenting the analysis that supports the decision that communications are eligible for reporting. An NSA reporting policy document, *Source Record Entries for Reporting from FAA 702 Multiple Communications Transaction,* ISS-185-11, requires that compliance be documented in NSA reporting tools. SV performs oversight of the documentation supporting use of certain MCTs for reporting (see the Oversight section).

(U) Disseminating attorney-client communications

(U//~~FOUO~~) In OVSC1203, analysts are trained on the requirement that NSA OGC personnel pre-approve disseminations of information involving USP attorney-client privileged communications.

(U//~~FOUO~~) **Disseminating domestic communications** Dissemination of domestic communications is limited to those communications for which DIRNSA has approved a destruction waiver documenting their eligibility for retention.[88] Such communications must contain information that meets at least one of five criteria: significant foreign intelligence, technical database information, information necessary to assess communications vulnerabilities, evidence of a crime, or information concerning a threat of serious harm to life or property. (Destruction waivers are discussed in the Oversight and Purge sections.) Training on retention and use of domestic communications is included in OVSC1203.

(U//~~FOUO~~) Disseminating foreign communications of or concerning USPs

(U//~~FOUO~~) OVSC1203 addresses the requirement to exclude information from reporting that would allow a reader to determine a USP's identity unless the identity qualifies for dissemination under the terms of the FAA §702 minimization procedures. NSA's Information Sharing Services Group (ISS) reviews exceptions to this "masking" requirement. ISS handles requests for release of USP identities.

(U) **Disseminating foreign communications of or concerning a non-USP** Foreign communications of non-USPs that contain foreign intelligence are eligible for dissemination subject to other applicable laws and policies.

(U) **Dissemination to foreign governments** Information obtained under FAA §702 may be disseminated to foreign governments in three ways (addressed in OVSC1203):

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] (b)(3)-P.L. 86-36
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] These records are provided to SV and are subject to review by DoJ and ODNI.

[88] (U//~~FOUO~~) A destruction waiver is not required for dissemination of domestic communications to notify the FBI of the target's presence in the United States or to notify the FBI or CIA for collection-avoidance purposes.

- (U//~~FOUO~~) [redacted] (b)(3)-P.L. 86-36 [redacted] Such dissemination must be performed in accordance with special handling procedures and requires the approval of SV and OGC, who maintain records and report this activity to DoJ and ODNI.

~~(S//REL TO USA, FVEY)~~ **Dissemination of collection acquired when post-tasking technical checks are not functioning properly** In 2013, NSA identified and reported an incident in which a system modification caused incomplete production of [redacted] (see the Post-Targeting section). Amended (b)(3)-P.L. 86 minimization procedures approved in November 2013 required application of procedures that NSA developed in response to the incident. These procedures included additional verification of target location before FAA communications acquired during a period when [redacted] post-tasking technical checks are not functioning as intended are used for targeting and dissemination. These procedures were the subject of several communications across SID, as well as training sessions, and are documented on NSA's FAA §702 web page.

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

(U//~~FOUO~~) Table 35 summarizes the sharing and dissemination provisions of the FAA §702 targeting and minimization procedures and the controls implemented by NSA to maintain compliance.

(U) Table 35. Sharing and Dissemination Provisions and Controls

~~(S//NF)~~

Provision	Control
(U) NSA has established processes to ensure that raw traffic is accessible in authorized repositories only to those who have had the proper training.	(U) Annual FAA §702 training addresses analyst responsibility for ensuring that individuals with whom they wish to discuss FAA §702 communications have the necessary credentials and training.
(U) NSA may provide to the CIA and FBI unminimized communications acquired pursuant to FAA §702. These communications will be based upon targets that each agency identifies to NSA.	~~(S//NF)~~ SV adjudicates TRs from CIA and FBI. If approved, the agencies will receive unminimized communications [redacted] For requested targets whose selectors are already tasked by NSA, SID personnel will dual-route [redacted] to provide Internet communications to the requesting agency. (b)(1) (b)(3)-P.L. 86-36
(U) Minimization procedures require NSA be able to purge communications that meet specific requirements.	(U) To account for and trace dissemination based on FAA §702 communications and to comply with purge requirements, analysts must document certain information for the data sources in each report, including the certification under which data was collected and a statement verifying that each piece of traffic used was confirmed as eligible for retention. This is addressed in annual analyst training and NSA reporting policy. (U//~~FOUO~~) A new reporting tool, first introduced in 2013, performs the source verification automatically. Successful completion of this

	process with no flags confirms the traffic is not subject to purge and may be used as a source for reporting.
(U) A dissemination based on communications of or concerning a USP that are eligible for retention may be made, if the identity of the USP is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable USP. Otherwise, dissemination of intelligence based on communications of or concerning a USP may only be made to a recipient requiring the identity of such person for the performance of official duties and only if at least one of eight criteria is met.	(U) This requirement is consistent with NSA reporting policy for all reporting based on communications of USPs.
(U) NSA analysts seeking to use a discrete communication within an MCT for reporting must document that specified analysis has been performed.	(U//~~FOUO~~) Annual FAA §702 training includes the requirements for reporting based upon discrete communications within an MCT and the documentation required. SV reviews this documentation for certain MCTs. (See Oversight - SID Oversight and Compliance .)
(U) All proposed disseminations of information constituting USP attorney-client privileged communications must be reviewed by the NSA OGC before dissemination. (U) Monitoring of attorney-client communications between a person known to be under criminal indictment in the United States and an attorney representing that individual in the matter under indictment must cease once the relationship has been identified. Acquired communications must be logged and the National Security Division of the DoJ notified so that appropriate procedures may be established to protect such communications from review or use in criminal prosecutions, while preserving foreign intelligence information contained therein.	(U) Annual FAA §702 training addresses procedures analysts must perform to disseminate this data. OGC notifies DoJ NSD of such communications and advises mission personnel on dissemination.
(U//~~FOUO~~) Minimization procedures require that domestic communications be promptly destroyed upon recognition, unless DIRNSA approves the communication for a destruction waiver. Domestic communications for which a destruction waiver is approved may be disseminated. If a waiver has been obtained, NSA may share domestic communications believed to contain evidence of a crime with appropriate federal law enforcement authorities in accordance with applicable laws and regulations. Without a destruction waiver, NSA is authorized to notify the FBI if information in a domestic communication indicates that a target has entered the United States and may provide information to both the CIA and FBI for collection avoidance purposes.	(U) Annual FAA §702 training addresses this requirement.

~~(S//REL TO USA, FVEY)~~ NSA is permitted to disseminate evaluated minimized information to foreign partners.	~~(S//REL TO USA, FVEY)~~ NSA policy requires that dissemination of EMT acquired pursuant to FAA §702, other than as serialized product, must be approved by the SIGINT Director and a record of the dissemination provided to SV.
(U) NSA may disseminate raw data to a foreign government for technical or linguistic assistance.	(U) Annual FAA §702 training addresses the requirement that such dissemination must be approved by SV and OGC, who will manage the restrictions on this dissemination, keep the required records, and report to DoJ and ODNI.
~~(S//NF)~~ If NSA seeks to use information acquired pursuant to FAA §702 when there is uncertainty about the location of the target of the acquisition because [redacted] post tasking checks described in NSA's FAA §702 targeting procedures were not functioning properly, NSA will follow internal procedures for determining whether such information may be used.	~~(S//NF)~~ Procedures addressing the requirements for use of data acquired when post-tasking [redacted] checks are not functioning as intended were communicated to mission personnel and are documented on the FAA §702 web page.

~~(S//NF)~~

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

(U) Purge

(U) Background

~~(S//REL TO USA, FVEY)~~ The Post-Targeting section documents the requirements for destruction of communications and the processes that may identify a change in the target's location or USP status. These processes include analyst review of communications, [redacted] and receipt of information from other agencies. If the circumstances result in unauthorized collection, the non-compliant data will be identified and purged.[89] The period of the unauthorized collection is included in an incident report documented by SV and is used by the purge adjudicator, who initiates the purge process.

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

(U//~~FOUO~~) **Compliance controls—purge of FAA §702 communications**[90] Manual and automated controls support the purge process. SID's Mission Support-Systems and Data Compliance Group, within the Directorate for Analysis and Production, developed a purge information web page to guide analysts. This page includes instructions to purge communications collected under FAA §702 authority. The directions call for analysts to contact SV, if they believe that purge of FAA §702 data is required, because nearly all cases requiring purges also require incident reports.

~~(S//SI//REL TO USA, FVEY)~~ The purge web page describes two types of purges: 1) incident or parametric purges which are necessary when the reason for the purge affects all collection for a target or selector over a period of time (SID's Mission Support-Systems and Data Compliance Group performs these); and 2) purge upon

[89] (U) "Purge" refers to the deletion of communications from systems that were acquired as a result of unauthorized collection or otherwise are not authorized for retention pursuant to the minimization procedures.

[90] ~~(TS//SI//NF)~~ From the time of collection, [redacted] The following description focuses on the [redacted]

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

recognition or analyst-driven purges. A parametric purge is applied, for example, to remove communications collected after a target is determined to be in the United States. Purge upon recognition for FAA §702 is, for example, required when: 1) NSA identifies a discrete domestic communication within an MCT, requiring the entire MCT to be purged or 2) a legally acquired foreign communication between a foreign target and a USP or a communication in which the subject is a USP found to have no foreign intelligence value.

(U//~~FOUO~~) NSA has implemented a mission compliance standard for purges which states that, consistent with NSA's FAA §702 minimization procedures and absent a destruction waiver, some or all communications data acquired under the authority must be purged if any of the following criteria are satisfied:

- (U) The targeted person is confirmed or believed to be a USP, regardless of location (purge all communications),
- (U) The targeted person was confirmed or believed to be in the United States at the time of collection (roamer) (purge collection acquired during period of U.S. travel),
- (U) A person was incorrectly targeted (purge all collection),
- (U) The tasked selector is known or suspected to be used by a USP (purge all communications from known date of use by the USP),[91]
- (U) The tasked selector was known or suspected to be accessed from within the United States (purge communications from date of access),
- (U) The tasked selector was tasked before being approved for tasking, remained tasked for any reason after collection was no longer authorized, or was tasked under the wrong authority (purge all collection),
- (U) An incorrect selector was tasked (purge all collection),
- (U) The communication is one in which the sender and all intended recipients were in the United States at the time of acquisition of the communication (purge affected communications), or
- (U//~~FOUO~~) The communication otherwise qualifies as a "domestic communication" as defined in the FAA §702 minimization procedures and DIRNSA or the Acting DIRNSA has not executed a destruction waiver to authorize continued retention of the communication (purge affected communications).

(U//~~FOUO~~) **Purge processes** Purging involves four processes: nominate data to purge, adjudicate purge nominations, execute purge actions, and verify purge actions. Other systems are certified to hold certain data copied or derived from [redacted] data

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

[91] ~~(S//NF)~~ [redacted]

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

objects. These systems have their own purge processes. The following description focuses on the [redacted] (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Nomination for purge** Nomination involves identification of the selectors and time period for which communications must be destroyed. For FAA §702, most are identified in incident reports, and SV determines whether purge is required and documents the date range for purge in the incident report. Purges of specific data objects are also initiated by analysts recognizing content that meets minimization criteria, but which is not an indicator of a compliance incident. This process is known as "purge upon recognition." For this type of purge, the identifiers of the affected communications are placed on the MPL in "discover state" before a modified version of the process described below is followed.

(U//~~FOUO~~) **Adjudicating purge nominations** Purge adjudication is the process whereby the purge adjudication authority, SID's Mission Support-Systems and Data Compliance Group, determines the validity and accuracy of a nominated purge request, locates the data required for destruction, and places the data objects on the master purge list (MPL). The goal of adjudication is to ensure compliance with purge criteria without over-purging communications at the expense of mission. The adjudicator:

- (U//~~FOUO~~) Evaluates the nomination against the purge criteria (unless a determination was made during incident processing),
- (U//~~FOUO~~) Using logical parameters provided in the nomination, determines and issues search criteria for discovery of potentially affected communications in the [redacted][92]
- (U//~~FOUO~~) Reviews and collates the results of purge discovery searches [redacted] (b)(3)-P.L. 86-36
- (U//~~FOUO~~) Enters identifiers of affected data objects in the MPL in "discover state" to prevent use as a source for new SIGINT reporting or other controlled uses and to initiate checks to determine if the objects were used in prior SIGINT reporting,
- (U//~~FOUO~~) Manages the impact of pending or approved destruction waivers that may exclude specific objects from purge,
- (U//~~FOUO~~) For data objects requiring purge, changes MPL state of their identifiers to "purge" and issues purge execute orders to the [redacted] to delete those objects, and
- (U//~~FOUO~~) Records the decision to purge, release, or quarantine the data objects in the corporate purge tracking system, [redacted] which retains (b)(3)-P.L. 86-36

[92] (U//~~FOUO~~) The discovery process is performed by a limited number of individuals with special access for each [redacted]

submitted data identifiers with historical records of actions taken and cross-references to original compliance incidents and/or purge nominations that caused them to enter the purge process.

(U//~~FOUO~~) For purges stemming from system or technical errors, collection and/or technical subject matter experts are typically relied upon to conduct or assist with purge discovery. Some aspects of the adjudication process may be modified based on the details of the specific incident.

(U//~~FOUO~~) **Executing purge actions** The purge executor receives purge decisions from the adjudication authority, issues execute orders to [redacted] system owners (b)(3)-P.L. 86-36 containing the unique identifiers of the data to be purged, confirms receipt of the orders, changes the MPL state for those identifiers to "purge," and retains records of the purge action for five years. [redacted] system owners are responsible for processing the orders, rendering the specified data unrecoverable, and confirming completion of purge execute orders.

(U//~~FOUO~~) **Verifying purge actions** Procedures are performed to provide additional assurance that system owners have purged required SIGINT data from NSA [redacted] SV obtains random samples of data from the master purge list and determines whether the data objects have been removed from the systems selected for review.

(U//~~FOUO~~) **Automation to support purge processing** Much of the purge process is performed manually. NSA is developing a system to automate more of the purge process in phases between [redacted] (b)(3)-P.L. 86

(U//~~FOUO~~) **Reports affected by purge actions** SIGINT reporting procedures require MPL checks to prevent publication of new reports with sources that were subject to purge. Additional measures are taken to detect and adjudicate already-disseminated SIGINT products affected by a compliance incident or specific data identified during purge discovery. Incident reports include information SV obtained from the mission team on reports issued related to the target or collection referenced in the incident. Another source of information is a daily query run by NSA's management information systems for SIGINT production against the MPL to identify reports sourced from communications listed on the MPL, whether because of an incident or purge-upon-recognition.

(U//~~FOUO~~) When SIGINT products with potentially "tainted" sources are identified, the Reports under Review (RUR) team coordinates with the mission team that issued the report, the purge adjudication authority, SV, and OGC, as necessary, to determine and complete appropriate actions. This may include requesting a destruction waiver to permit retention of the traffic and allow the report to stand, removing the MPL-listed traffic completely from the report and revising and reissuing the report, or recalling the report. The RUR team maintains a list of affected reports and their status that is updated when the report analysis is complete. The purge adjudication

authority makes necessary changes to the status of the communication identifiers on the MPL, depending on the action taken.

(U//~~FOUO~~) Table 36 summarizes the purge provisions of the FAA §702 targeting and minimization procedures and the controls NSA has implemented to maintain compliance.

(U) Table 36. Purge Provisions and Controls

~~(S//NF)~~

Provision	Control
(U//~~FOUO~~) Telephony communications and Internet communications acquired with the assistance of the FBI from Internet service providers that are not approved for retention under the standards set forth in the minimization procedures and that are known to contain communications of or concerning USPs will be destroyed upon recognition.	(U//~~FOUO~~) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.
(U//~~FOUO~~) Internet transactions acquired through NSA's upstream collection techniques that do not contain information that meets the retention standards set forth in the minimization procedures and that are known to contain communications of or concerning USPs will be destroyed upon recognition.	(U//~~FOUO~~) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.
(U) Internet transactions that are identified and segregated pursuant to the requirements for processing MCTs and are subsequently determined to contain a discrete communication in which the sender and all intended recipients are reasonably believed to be in the United States will be handled as domestic communications.	(U//~~FOUO~~) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.
(U//~~FOUO~~) A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition, unless DIRNSA or the Acting DIRNSA approves a destruction waiver after determining the communication meets one or more of four specific conditions.	(U//~~FOUO~~) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.
(U//~~FOUO~~) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be outside the United States but is in fact inside the United States at the time such communications were acquired and any communications acquired by targeting a person who at the time of targeting was believed to be a non-USP but was in fact a USP at the time such communications were acquired will be treated as domestic communications under these procedures.	(U//~~FOUO~~) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report. ~~(S//REL TO USA, FVEY)~~ In addition to analyst review of communications, investigation of [redacted] notices from others involved in processing FAA §702 information, and receipt of information from other agencies may identify an incident. If the circumstances of the collection require an incident report, analysts and SV work together to determine the extent of the communications affected. This is used to document the purge parameters in an

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

	incident report, which becomes the source for the purge adjudication process. (U//~~FOUO~~) Communications identified for purge are subject to adjudication to determine whether the nominated data objects are consistent with the purge criteria, communications affected by the incident have been properly identified, destruction waivers (pending or approved) may affect the purge. (b)(3)-P.L. 86-36 The adjudicator adds the relevant data to the Master Purge List (MPL) to prevent its use in targeting and reporting and issues purge execute orders to appropriate systems. (U//~~FOUO~~) Owners of the FAA §702 execute the purge orders, remove data matching the included identifiers, and acknowledge completion of each order. (U//~~FOUO~~) NSA's management information system for SIGINT reporting queries the MPL daily to identify data objects added to the list that may be associated with issued reports. The Reports under Review team uses this information and incident report data concerning reporting associated with the affected communications to follow up with mission personnel for recall or reissuance of the reports. (U//~~FOUO~~) SV randomly samples records from the MPL, comparing them to the FAA §702 repositories to assure completeness of purge.
~~(S//NF)~~ For information acquired pursuant to FAA §702 during a period when post-tasking checks were not functioning properly, resulting in uncertainty about the location of the target of the acquisition, if NSA determines that the target is reasonably believed to have been inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.	~~(S//NF)~~ SID guidance, *NSA Procedures for the Use of FAA 702, 704 or 705(b) Collection,* last revised 15 November 2013, was updated to provide manual procedures for evaluating data when NSA's post-tasking checks are not properly functioning. (b)(1) (b)(3)-P.L. 86-36

~~(S//NF)~~

(U) Retention of Data

(U) Provisions of FAA §702 certifications

(U//~~FOUO~~) The retention criteria in the minimization procedures apply only to communications not subject to purge based upon other minimization requirements (see the Post-Targeting section).

(U//~~FOUO~~) NSA minimization procedures state that telephony communications will be retained no longer than five years from the expiration date of the certification authorizing collection, unless NSA analysts have determined that the communications meet the retention standards set forth in the minimization procedures, for example, communications necessary to understand foreign intelligence information. Communications for which SIDDIR has approved longer retention and for which a purge was not otherwise required, may also be retained.

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

Communications for which DIRNSA has waived destruction may also be retained in accordance with the terms of the destruction waiver.

(U) In general, NSA may not retain Internet transactions obtained through upstream collection techniques longer than two years from the expiration date of the certification authorizing collection. However, NSA may be able to retain certain Internet transactions longer, if at least one discrete communication within the upstream Internet transaction would otherwise meet the retention standards and each discrete communication within the transaction is to, from, or about a tasked selector or not to, from, or about a tasked selector and is also not to or from a USP or person reasonably believed to be in the United States. The minimization procedures also required destruction of all upstream Internet transactions acquired before November 2011.

(U) Retention control procedures

(U//~~FOUO~~) **System certification** The NSA system certification process implemented in 2010 (see the Repositories section) includes the Agency's requirements for compliance with the FAA §702 retention limits established in the minimization procedures. To be certified, FAA §702 systems must: 1) limit retention of unminimized data records to the authorization and retention periods of the certification under which they were collected, 2) retain data with an approved age-off waiver beyond the normal age-off period (SID Director waiver), and 3) provide a means to identify data records to be retained beyond the maximum retention period specified by the collection authority under which it was obtained.[93]

(U//~~FOUO~~) **Data tagging** Data tags are now associated with most collection before it is made available to data stores accessible to analysts. The tags include the certification under which the communications were obtained, further supporting NSA's ability to identify records that meet the criteria for removal from system repositories based upon age-off requirements associated with each certification. In 2014, new data tags were implemented to distinguish among the retention periods for upstream Internet transactions (two years), downstream collection (five years) and telephony data (five years).

(U//~~FOUO~~) **Implementation and monitoring of age-off** Processes have been implemented to age-off data in FAA §702 [redacted] Though the minimization procedures require data be aged-off within two or five years of expiration of the certification, depending upon the source of collection, the processes NSA uses for determining age-off result in earlier removal of data (see Table 37).[94] (b)(3)-P.L. 86-36

[93] (U//~~FOUO~~) NSA's FAA §702 minimization procedures provide no maximum retention period for foreign communications determined to contain foreign intelligence information. The age-off requirements apply to communications for which such a determination has not been made.

[94] (U//~~FOUO~~) The FAA 702 certifications are renewed annually. Expiration of the certification in effect for any collection would occur somewhere between 1 and 365 days of that collection. NSA applies age-off criteria to time of collection or recording date, not the expiration of the certification.

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

(U) Table 37. System Age-Off Procedures

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

	Upstream Procedure for Data Age-Off	Telephony and Downstream Internet Collection Procedure for Data Age-Off	Monitoring for Compliance with Age-Off Criteria

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

* (U//~~FOUO~~) Enterprise data header (EDH) is a small set of metadata tags applied to a piece of mission data so that it can be identified, protected, tracked, and handled throughout its life cycle. will only accept data with an EDH.

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

† (U//~~FOUO~~) Systems scheduled to be decommissioned.

‡ (U//~~FOUO~~) DTOI, date and time of intercept.

§ ~~(TS//SI//NF)~~

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

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

(U//~~FOUO~~) Table 38 summarizes the retention provisions of the FAA §702 targeting and minimization procedures and the controls NSA implemented to maintain compliance.

(U) Table 38. Retention Provisions and Controls

(U//~~FOUO~~)

Provision	Control
(U) Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA determines that each communication meets the retention standards in these procedures.	(U) System certification, required of all FAA §702 systems, includes retention standards consistent with minimization procedures. (U) Data tags are now associated with most collection before it is made available to data stores accessible to analysts. Data tags support identification of records for age-off.
(U) Internet transactions acquired through NSA's upstream collection may not be retained longer than two years from the expiration date of the certification authorizing the collection, unless NSA determines that each communication meets the retention standards in these procedures. [Additional requirement regarding MCTs are addressed in the Purge section.]	(U//~~FOUO~~) [redacted] utilizes a software tool to search for data beyond the required age-off procedure. A similar tool is being developed for [redacted] (b)(3)-P.L. 86-36
(U) Internet transactions that are identified and segregated pursuant to the procedures for MCTs will be retained in an access-controlled repository. (U) Any information contained in a segregated Internet transaction may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States.	(U//~~FOUO~~) NSA has implemented a segregation process and sequestered MCT data is maintained in a collection store where it is not available for analytic use. None of the data subject to sequestration has been transferred to repositories accessible to analysts. (U//~~FOUO~~) NSA has deleted all identified upstream Internet collection acquired before November 2011. If additional data is identified that was subject to this purge requirement, NSA deletes it upon recognition. (U) These controls are documented in the Collection section.
(U) Any Internet transactions acquired through NSA's upstream collection techniques prior to 31 October 2011 will be destroyed upon recognition.	

(U//~~FOUO~~)

(U) Oversight

(U) Provisions of FAA §702 certifications—internal and external oversight

(U//~~FOUO~~) The FAA §702 targeting and minimization procedures provide that NSA will conduct the following oversight:

- (U) Implement a compliance program with ongoing oversight of its exercise of FAA §702 authority, including the associated targeting and minimization procedures
- (U) Develop and deliver training regarding procedures to ensure that intelligence personnel responsible for approving targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition

- (U) Establish processes for ensuring that raw traffic is labeled and stored only in authorized repositories and is accessible only to those who have had the proper training
- (U//~~FOUO~~) Conduct ongoing oversight activities and make necessary reports to the NSA OIG and OGC, including reports of non-compliance
- (U) Ensure that corrective actions are taken to address identified deficiencies
- (U) Conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures and conduct periodic checks of queries in data repositories
- ~~(S//NF)~~ Report incidents of non-compliance with the targeting and minimization procedures within five business days of discovery to the DoJ NSD and ODNI's oversight team.[95]

(U) DoJ NSD and ODNI oversight requirements include:

- (U) Oversee NSA's exercise of the FAA §702 authority, including bi-monthly reviews to evaluate the implementation of the procedures
- (U) Oversee NSA's activities with respect to use of USP identifiers to query communications collected under FAA §702.

(U) NSA oversight

(U//~~FOUO~~) NSA operates a comprehensive oversight framework to maintain compliance with the FAA §702 targeting and minimization procedures. The NSA organizations that perform oversight are described below.

(U//~~FOUO~~) **FAA §702 Authority Lead** is responsible for the implementation and operation of the FAA §702 authority for NSA. The FAA §702 Authority Lead serves on NSA's corporate Authorities Integration Group and works with other NSA mission Authority Leads and corporate, legal, policy, compliance, and technology personnel to coordinate implementation of NSA mission authorities. The FAA §702 Authority Lead addresses the tactical and strategic elements of the program; interacts regularly with NSA's OGC, ODOC, TD, LAO, and SID; routinely interacts with DoJ NSD, ODNI, FBI, and CIA; provides direction regarding daily operational and technical questions; and coordinates input to reports to Congress and the FISA Court.

(U//~~FOUO~~) **Authorities Integration Group (AIG)** is administratively assigned to ODOC and reports to the NSA Deputy Director. The AIG works directly with SID and Information Assurance Directorate authority leads, including the FAA §702 Authority Lead, and holds weekly meetings with the authority leads and corporate process leads (e.g., TD, ODOC, OGC) to bring legal, policy, compliance, technology, and mission areas together to provide recommendations on the implementation of the

[95] (U) ODNI's oversight team is comprised of ODNI's Office of General Counsel, ODNI's Civil Liberties and Privacy Office, and ODNI's Office of the Deputy Director of National Intelligence for Intelligence Integration/Mission Integration Division.

authorities. The AIG focuses on the activities of each authority, internal and external, to ensure that they are coordinated and integrated across NSA. The AIG acts as a "forcing function" within NSA, facilitating discussion among the Directorates to promote better understanding of how decisions affect the various authorities. The AIG updates the NSA Deputy Director quarterly on each authority.

(U//~~FOUO~~) **Office of the Director of Compliance (ODOC)** is responsible for developing and directing the execution of compliance strategies and activities focused on protecting USP privacy during the conduct of authorized NSA missions. ODOC has the authority to develop, implement, and monitor a Comprehensive Mission Compliance Program for the Agency, which addresses: (1) integration of compliance strategies and activities across NSA mission, technology, and policy organizations; (2) a training and education program for compliance; and (3) maintenance of and reporting on the status of mission compliance. The CMCP's focus is on mission compliance, particularly in Signals Intelligence and Information Assurance operations, including the technology base on which they function. The key objective of the CMCP is to provide reasonable assurance that the legal authorities and policies affecting USP privacy are reliably and verifiably followed by NSA. The CMCP includes activities and funding to support compliance with FAA §702, such as compliance target validation and query tools.

(U//~~FOUO~~) ODOC's monitoring activities provide continuous assessment to determine whether internal controls are operating as intended. Its assessments help management evaluate the effectiveness of the compliance program and its components. For example, ODOC reviews compliance activities associated with queries in NSA repositories, including those related to FAA §702:

- (U//~~FOUO~~) ODOC analyzes [redacted] queries forwarded to the query audit database that could indicate a problem in communicating with the repositories queried, (b)(3)-P.L. 86-36
- (U//~~FOUO~~) It verifies that all queries requiring post-query review are assigned to reviewers,
- (U//~~FOUO~~) It monitors the number of queries selected for review and the timeliness of review, and
- (U//~~FOUO~~) It tracks the super audits performed by SV (see the Oversight section).

(U//~~FOUO~~) In addition, ODOC performs Compliance Vulnerability Discovery (CVD) reviews that focus on high-risk areas within the CMCP to discover compliance weaknesses. In 2013, ODOC completed two CVDs focused on mission compliance with SIGINT authorities. Table 39 summarizes these CVDs.

(U) Table 39. Compliance Vulnerability Discovery Reviews

(U//~~FOUO~~)

Date Issued	SIGINT Authority	CVD Review	Scope of the Review
05/03/13	FISA/ FAA §702	Multiple Communications Transactions	Reviewed implementation of controls to segregate unauthorized data from NSA's FAA §702 Upstream Multiple Communications Transactions
07/17/13	All	Data Tagging	Reviewed data from NSA systems for proper tagging to support designation of these systems as

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

(U//~~FOUO~~)

(U//~~FOUO~~) ODOC has also implemented processes to ensure that NSA representations to external overseers are accurate and NSA personnel have a consistent understanding of program activities. VoA and verification of implementation reviews are performed on written NSA representations that describe the Agency's acquisition, processing, retention, analysis, and dissemination and form the basis for legal opinions, FISC Orders, and Executive Branch decisions. In 2013, ODOC conducted VoAs with FAA §702 stakeholders for the affidavits and targeting and minimization procedures supporting renewals of FAA §702 certifications. One verification of implementation was conducted in June 2013 with NSA external partners (DoJ NSD and ODNI) on procedures for implementing the FAA §702 targeting procedures.

(U//~~FOUO~~) **SV** implements the SIGINT compliance program across NSA. SV establishes SIGINT compliance standards and provides guidance across the global SIGINT enterprise, manages incidents of non-compliance, monitors compliance in high risk areas, resolves problems, and verifies compliance through audits and by managing the SIGINT Intelligence Oversight Officer program. SV manages resources to ensure that NSA corporate systems and capabilities align with CMCP solutions.

~~(C//REL TO USA, FVEY)~~ To maintain NSA's compliance with the FAA §702 targeting and minimization procedures, SV:

- ~~(S//NF)~~
- (U//~~FOUO~~) Adjudicates TRs for selectors nominated by the CIA and FBI, utilizing the same process used for NSA TRs
- ~~(TS//SI//NF)~~ Reviews tasking requests for completeness.
- ~~(S//REL TO USA, FVEY)~~ Performs post-tasking analysis for FAA §702 selectors suspected of being accessed within the United States

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

- (U//~~FOUO~~) Investigates all incidents of non-compliance with FAA §702 targeting and minimization procedures, coordinating with TV when a potential incident involves a system. SV works with the mission team to document FAA §702 incidents, promptly reports them to OGC, OIG, and ODOC, and maintains a permanent record
- (U//~~FOUO~~) Works with mission personnel and OGC to process destruction waivers as needed
- (U//~~FOUO~~) Conducts super audits of queries of raw SIGINT databases that provide records of queries to the corporate logging and auditing system to analyze the quality of query reviews by auditors
- (U//~~FOUO~~) Completes Purge Verification Activities quarterly for [redacted] and certain other stores that hold FAA §702 data to assess NSA's effectiveness in purging non-compliant SIGINT (b)(3)-P.L. 86-36
- (U//~~FOUO~~) Oversees use of MCTs as a source for reporting and verifies completion of required documentation [96]
- (U//~~FOUO~~) Serves as the FAA §702 tasking liaison for the NSA enterprise, IC customers (FBI and CIA), and overseers from DoJ NSD and ODNI
- (U//~~FOUO~~) Provides documentation for review by DoJ NSD and ODNI. SV reviews [redacted] for each selector tasked and reviews records of information shared with NSA SIGINT partners for compliance with dissemination requirements. Records of database queries using USP query terms and records of USP reporting are also provided to overseers. SV coordinates responses by NSA organizations to questions from DoJ NSD and ODNI during their review of information SV made available. (b)(3)-P.L. 86-36
- (U//~~FOUO~~) Pre-approves USP content queries in conjunction with OGC
- (U//~~FOUO~~) Participates in the verification of accuracy process for renewals of certifications and targeting and minimization procedures
- (U//~~FOUO~~) Partners with the Associate Directorate for Education and Training to develop and implement oversight and compliance training for the SIGINT workforce. SV co-develops and reviews all updates of the FAA §702 course.

(U//~~FOUO~~) **SID Analysis and Production, Mission and Compliance Office** This office supports all areas of NSA's SIGINT operations by overseeing:

[96] ~~(S//NF)~~ Three types of MCTs are made available to analysts. Two types of transactions made available to analysts after the MCT sequestration process are those that contain only discrete communications (no MCTs) and those where the active user of the selector is a targeted individual. SV performs oversight of the third type, where the active user of the selector is a non-targeted individual outside the U.S. (an example of "abouts" collection). SV examines these MCTs for compliance with NSA reporting guidance (ISS-185-11), which states that analysts are "only authorized to use those discrete portions of MCTs containing the targeted selector."

- (U//~~FOUO~~) FAA §702 adjudication and training (interfacing with analysts on how to use the authority, approving new adjudicators who meet training and mission requirements, and reviewing adjudicated TRs for compliance)
- ~~(S//NF)~~ Dual-route adjudication (approving provision of the results of targeting to the CIA or FBI for selectors already on NSA collection)
- ~~(S// REL TO USA, FVEY)~~ FISA and production metrics (providing feedback to management on use of the authority and analyst/adjudicator performance)
- ~~(S// REL TO USA, FVEY)~~ The application of the authority (e.g., instructions for maintaining compliance when [redacted] were not operating, targeting and adjudication checklists, and general guidance on the analytic use of the authority).

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

(U//~~FOUO~~) **TD Office of Compliance (TV)** is responsible for identifying, assessing, tracking, and mitigating compliance risks, including USP privacy concerns, in NSA mission systems across the extended enterprise, including systems that hold FAA §702 data. TV manages the system compliance certification process, continuous compliance monitoring, and technical compliance incident reporting and also trains technical personnel. TV performs VoAs for areas assigned to it in NSA representations.

(U//~~FOUO~~) [redacted] TV began certifying FISA systems, including the FAA §702 systems, to ensure compliance with the law and policies protecting USP privacy (see the Repositories section).

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

(U) The **Office of the General Counsel** provides legal advice to NSA and is the liaison to DoJ NSD for NSA's FAA §702 program. One of its main oversight responsibilities includes independently assessing potential incidents of non-compliance.

(U) OGC receives reports of potential incidents of non-compliance from SV. OGC compiles FAA §702 incidents daily, provides them to DoJ NSD and ODNI, and makes an initial determination whether incidents represent non-compliance with the FAA §702 certifications and targeting and minimization procedures. OGC notifies DoJ NSD and the ODNI's oversight team of potential incidents of non-compliance with the targeting procedures within five business days of discovery, as FAA §702 targeting procedures require. OGC reviews all proposed disseminations of information constituting USP attorney-client privileged communications before dissemination, as NSA's FAA §702 minimization procedures require. For all violations of NSA's FAA §702 targeting and minimization procedures, OGC coordinates input from NSA organizations and edits the content for factual and legal accuracy. DoJ NSD prepares Rule 13 notices, in coordination with ODNI.

(U) OGC performs additional oversight responsibilities including:

- (U//~~FOUO~~) Reviews requests to perform content queries using USP selection terms. Only OGC approved selection terms can be used to perform content queries of USP information.
- ~~(S//NF)~~ [redacted]
- ~~(TS//SI//NF)~~ Reviews [redacted] tasking requests for completeness.
- (U//~~FOUO~~) Participates in the VoA process.
- (U//~~FOUO~~) Reviews and makes updates to the FAA §702 course, as necessary.

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

(U) **Office of the Inspector General (OIG)** conducts audits, special studies, inspections, investigations, and other reviews of the programs and operations of NSA and its affiliates. OIG oversight includes:

- (U) Performing audits and special studies of the FAA §702 program
- (U) Receiving notification of incident reports for all NSA authorities, including FAA §702, saved in the Agency's corporate incident reporting database
- (U//~~FOUO~~) Reviewing Congressional notifications and notices filed with the FISC of incidents of non-compliance with FAA §702 targeting and minimization procedures
- (U) Preparing Intelligence Oversight Quarterly Reports, in coordination with the DIRNSA and OGC, that summarize compliance incidents for all authorities occurring during quarterly review periods and forwarding the reports to the President's Intelligence Oversight Board through the ATSD(IO) [97]
- (U) Performing intelligence oversight reviews during OIG inspections of joint and field sites
- (U) Maintaining the OIG Hotline, responding to complaints, including allegations of SIGINT misuse by NSA affiliates operating under DIRNSA's authority
- (U) Reporting immediately to the ATSD(IO) a development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the IC or otherwise call into question the propriety of an intelligence activity.

[97] (U//~~FOUO~~) In 2014, the ATSD(IO) was changed to the Office of the Senior DoD Intelligence Oversight Official.

(U//~~FOUO~~) The OIG reviews management controls, maintains awareness of compliance incidents, and stays informed of changes affecting NSA authorities, including FAA §702. OIG reviews of the FAA §702 program allow it to independently assess compliance with minimization procedures. Since the Agency obtained FAA §702 authority in January 2008, the OIG has completed annual reviews of reports containing references to USP identities and targets later determined to be in the United States, as the statute requires. The OIG has also completed two special studies of the program (Table 40).

(U) Table 40. OIG Reviews of the FAA §702 program

~~(S//NF)~~

Date Issued	OIG Review	Scope of the Review
3/29/13	(U) Assessment of Management Controls Over FAA §702 (ST-11-0009)	(U//~~FOUO~~) Reviewed management controls for maintaining compliance with targeting and minimization procedures.
10/29/13	~~(S//NF)~~	~~(S//NF)~~

~~(S//NF)~~

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

(U) External oversight

(U//~~FOUO~~) **DoJ NSD and ODNI** closely coordinate to perform oversight to ensure that NSA's FAA §702 program is compliant with the statute and FISC rulings. DoJ NSD is the primary liaison between NSA and the FISC for all matters pertaining to the FAA §702 program. DoJ NSD and ODNI oversight includes:

- (U//~~FOUO~~) Reviewing and approving annual certification renewals and updates of the associated targeting and minimization procedures and filing them for FISC approval
- (U) Providing guidance to the NSA OGC on legal opinions relating to the interpretation, scope, and implementation of the FAA §702 authority
- (U//~~FOUO~~) Reviewing briefings on NSA proposals to substantially modify systems or processes supporting FAA §702. This allows NSD to determine that the modifications are lawful and that the Attorney General (AG) and the FISC are aware of the scope and nature of the changes
- (U) Evaluating and investigating potential incidents of non-compliance with the statute or procedures and reporting any matter determined to be a compliance incident to the FISC
- (U) Reviewing NSA briefings and training transcripts to ensure that they accurately describe the requirements of the FAA §702 Orders
- ~~(S//NF)~~ Performing bi-monthly reviews of NSA authorities under the [redacted] FAA §702 certifications. The reviews include NSA's targeting decisions,

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

including source documentation supporting these determinations, to assess compliance with NSA targeting procedures and AG Acquisition Guidelines. The reviews also examine database queries using USP query terms and disseminations of serialized reporting and EMT.

- (U) Preparing the periodic reports the statute requires:

  1. ~~(S//NF)~~ DoJ submits the *Semiannual Reports of the AG Concerning Acquisitions under Section 702 of the FISA* to Congress and the FISC. Pursuant to FISA §707, the AG reports on the acquisition of foreign intelligence information conducted under the [redacted] FAA §702 certifications by NSA and FBI. While the CIA does not acquire the information, it may receive unminimized data that NSA and FBI acquired. The AG's semiannual reports focus on analysis of incidents of non-compliance with targeting and minimization procedures by NSA and FBI and incidents of non-compliance with minimization procedures by CIA.

  2. ~~(S//NF)~~ Jointly, the AG and the DNI submit the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the FISA* to Congress and the FISC. These reports summarize the oversight performed on implementation of the FAA §702 authority, trends in targeting and minimization (e.g., changes in the number of selectors under collection and statistics on use of the [redacted] certifications), and compliance incidents with the FAA §702 authority for NSA, FBI, and the CIA.

- (U) ODNI hosts bi-monthly interagency meetings and a weekly phone call to discuss FAA §702 implementation and compliance matters.

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

~~(S//NF)~~ The **FISC** reviews and, when satisfied that the legal requirements have been met, approves all renewals of certifications and targeting and minimization procedures for the FAA §702 authority that have been authorized by the AG and DNI.[98] In addition, the FISC reviews representations NSA made regarding the operation of the program and Rule 13 notices of incidents of non-compliance filed by DoJ NSD on behalf of NSA. If the Court finds that incidents of non-compliance result from processes inconsistent with the targeting and minimization procedures (e.g., incomplete application of the [redacted] identification), NSA will be required to change its internal systems or procedures and report to the Court on the progress made to achieve compliance. The Court may also determine that additional measures or changes are required to the targeting and minimization procedures (e.g., sequestration of MCTs), if it deems that NSA processes do not adequately protect USPs.

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

[98] (U//~~FOUO~~) The AG and DNI authorize the collection of data pursuant to FAA §702 using targeting and minimization procedures adopted by the AG (in consultation with the DNI). The FISC must approve the certifications and associated procedures that the AG and DNI have authorized.

(U//~~FOUO~~) Table 41 summarizes the oversight provisions of the FAA §702 targeting and minimization procedures and the controls NSA implemented to maintain compliance.

(U) Table 41. Oversight Provisions and Controls

~~(S//NF)~~

Provision	Control
(U) NSA will implement a compliance program, and will conduct ongoing oversight, with respect to its exercise of the authority under FAA §702, including the associated targeting and minimization procedures.	(U//~~FOUO~~) NSA operates a comprehensive oversight framework to maintain compliance with the FAA §702 targeting and minimization procedures. This compliance framework is collectively managed by the NSA organizations described above.
(U) NSA will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition.	(U//~~FOUO~~) SV partners with the Associate Directorate for Education and Training to develop and implement oversight and compliance training for the SIGINT workforce. SV co-developed and reviewed all updates of the FAA §702 course. OGC also reviews and updates the FAA §702 course.
(U) NSA will establish processes for ensuring that raw traffic is labeled and stored only in authorized repositories and is accessible only to those who have had the proper training.	(U//~~FOUO~~) TV certifies FISA systems periodically, including the FAA §702 systems, to ensure that they comply with law and policy protecting USP privacy. TV's certification process evaluates system controls for maintaining compliance in a number of areas, including data tagging and data access.
(U) NSA will conduct ongoing oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA OIG and OGC, in accordance with the NSA charter.	(U//~~FOUO~~) SV and TV investigate incidents of non-compliance with FAA §702 targeting and minimization procedures. SV works with mission teams to document FAA §702 incidents. SV promptly reports potential incidents to OGC and ODOC and maintains a permanent record. When a potential incident involves a system, TV manages the incident investigation. (U//~~FOUO~~) The OIG receives notification of incident reports for all NSA authorities, including FAA §702. The OIG also receives Congressional notifications and notices filed with the FISC of incidents of non-compliance with the FAA §702 targeting and minimization procedures. (U//~~FOUO~~) OGC receives notifications of potential incidents of non-compliance for all NSA authorities. OGC compiles FAA §702 incidents daily (which it provides to DoJ NSD and ODNI), and assesses whether incidents represent possible non-compliance with the FAA §702 certifications and associated targeting and minimization procedures.

(U) NSA will ensure that necessary corrective actions are taken to address any identified deficiencies.	(U//~~FOUO~~) SV and TV investigate all incidents of non-compliance with FAA §702 targeting and minimization procedures and monitor corrective actions. (U) OIG performs audits and special studies of the FAA §702 program; tracks recommendations until completion.
(U) NSA will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.	(U//~~FOUO~~) SV performs oversight of targeting decisions, queries, and dissemination and provides documentation for review by DoJ NSD and ODNI to support their oversight of NSA's implementation of FAA §702. SV also conducts super audits of queries of raw SIGINT databases. (U) OGC reviews all proposed disseminations of information constituting USP attorney-client privileged communications before dissemination.
(U//~~FOUO~~) NSA will report incidents of non-compliance with the targeting and minimization procedures within five business days of discovery to the DoJ NSD and ODNI OGC, and ODNI CLPO.	(U//~~FOUO~~) OGC notifies external overseers of incidents of possible non-compliance with the targeting procedures within five business days of discovery. OGC coordinates input by NSA organizations for Rule 13 notices prepared by DoJ NSD, in coordination with ODNI, for all violations of the FAA §702 targeting and minimization procedures.
(U//~~FOUO~~) DoJ NSD and ODNI will oversee NSA's exercise of the FAA §702 authority, which will include bi-monthly reviews to evaluate the implementation of the procedures.	~~(S//NF)~~ DoJ NSD and ODNI perform bi-monthly reviews of NSA authorities under the [redacted] FAA §702 certifications. DoJ NSD and ODNI review NSA's targeting decisions, including the source documentation supporting these determinations, to assess compliance with NSA targeting procedures and Attorney General's (AG) Acquisition Guidelines. NSD and ODNI also review queries, and disseminations of serialized reporting and EMT.
(U//~~FOUO~~) DoJ NSD and ODNI will oversee NSA's activities with respect to use of USP identifiers to query communications collected under FAA §702.	

~~(S//NF)~~

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

(U) FAA §702 Incidents of Non-Compliance

(U//~~FOUO~~) FISC Rules of Procedure require NSA to report to the FISC "corrections of material facts" and "disclosures of non-compliance" with FAA §702. In addition, NSA determines whether Congressional notifications are required.

(U) FISC Rules of Procedure

(U//~~FOUO~~) The FISC Rules of Procedure govern all FISC proceedings. Rule 13, *Correction of Misstatement or Omission; Disclosure of Non-compliance*, is the procedure NSA follows when notifying the Court, through DoJ NSD, of incidents of non-compliance with FAA §702.

(U) **Rule 13(a) Correction of Material Facts** If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the

government must immediately, in writing, inform the Judge to whom the submission was made of:

(1) (U) the misstatement or omission;

(2) (U) necessary corrections;

(3) (U) the facts and circumstances relevant to the misstatement or omission;

(4) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and

(5) (U) how the government proposes to dispose of or treat information obtained as a result of the misstatement or omission.

(U) **Rule 13(b) Disclosure of Non-compliance** If the government discovers that an authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government must immediately, in writing, inform the Judge to whom the submission was made of:

(1) (U) the non-compliance;

(2) (U) the facts and circumstances relevant to the non-compliance;

(3) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and

(4) (U) how the government proposes to dispose of or treat information obtained as a result of the non-compliance.

(U) Identifying and Reporting Incidents of Non-compliance

(U) Identifying incidents of non-compliance

(U//~~FOUO~~) All potential incidents of non-compliance with FAA §702 certifications and targeting and minimization procedures are reported to SV or TV upon discovery by analysts and others operating under the authority, as documented in the *FAA §702 Program Control Framework* section - *Incident Recognition and Reporting.* Training provides a heightened sense of awareness for personnel to identify potential violations. Incidents may also be discovered through oversight mechanisms addressed in the *FAA §702 Program Control Framework* section *Post-Targeting and Oversight.* Monitoring and oversight include manual and technical controls to detect abnormalities.

(U//~~FOUO~~) After review of the incident, SV or TV forwards documentation to OGC. If OGC believes a violation of the targeting and minimization procedures has or may have occurred, even if all the facts have not been gathered, preliminary notification is sent to DoJ NSD. OGC notifies DIRNSA of instances of non-compliance, as appropriate. Upon receiving initial notification from OGC, DoJ NSD drafts, in conjunction with ODNI, a notification to the Court, should one be required under the FISC Rules of Procedure.

(U//~~FOUO~~) Once the facts have been gathered and OGC has made an initial determination that a non-compliant FAA §702 event has occurred, OGC finalizes a notification of non-compliance and forwards it to DoJ NSD and ODNI, which make the final determination as to whether there has been an incident of non-compliance that must be reported to the FISC. If DoJ NSD and ODNI determine that an incident of non-compliance has occurred, DoJ drafts a notification, which is coordinated with the IC elements involved, finalizes it, and files the notice with the Court.

(U//~~FOUO~~) DoJ NSD often follows up on preliminary notifications with one or more additional notifications. In some cases, the preliminary notification of an incident serves as the final notice of that incident.[99]

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

(U//~~FOUO~~) In 2013, [redacted] incidents of non-compliance (13(b)s) were filed with the FISC for matters identified in that calendar year. None of these incidents involved inaccurate information in previously filed declarations to the Court, requiring that a Rule 13(a) notice of correction of material fact be filed.

(U) Congressional notifications

(U//~~FOUO~~) DIRNSA, as head of an IC element, has a statutory obligation to keep the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence fully and currently informed of all significant intelligence activities.[100] NSA resolves doubts about notification in favor of notification. In addition to notifying Congress and the Director of National Intelligence, DIRNSA must notify the USD(I) and other USD(I) staff, as directed by USD(I) guidance. For all FAA §702 incidents of non-compliance reported to Congressional intelligence committees, NSA also provides discretionary notifications to the Senate and House Committees on the Judiciary.

(U//~~FOUO~~) NSA's LAO manages NSA's liaison with the Congress, and with the DNI, DoD, the IC, and other U.S. government departments and agencies regarding matters of concern to Congress. LAO is NSA's focal point for Congressional inquiries, correspondence, questions for the record, and RFIs directed to NSA.

(U//~~FOUO~~) NSA/CSS Policy 1-33 provides guidelines for identifying matters that OGC and LAO must consider reporting to the Congressional intelligence committees under 50 U.S.C. §§3091 and 3092. The guidelines do not constitute a comprehensive list of what must be reported. Compliance incidents are assessed under a general guideline to consider reporting matters that the intelligence committees have

---

[99] (U//~~FOUO~~) DoJ NSD files the "*Quarterly Report to the Foreign Intelligence Surveillance Court Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act*" which includes incidents DoJ NSD and ODNI determined to be violations of the targeting and minimization procedures (13(b)s) as well as all other incidents determined not to meet the reporting requirements of 13(b). This quarterly report to the FISC also provides supplemental information on previously reported compliance incidents.

[100] (U) 50 U.S.C. §3091, as implemented by Intelligence Community Directive 112, *Congressional Notification*, 16 November 2011, requires the head of each element of the IC to inform Congress on significant intelligence activities.

expressed a continuing interest in or which otherwise qualify as significant intelligence activities or failures.

(U//~~FOUO~~) NSA works to keep Congressional intelligence committees fully and currently informed about the Agency's activities over and above what is strictly required to be reported under the guidelines outlined in NSA/CSS Policy 1-33. At a minimum, however, NSA must keep the Congressional intelligence committees timely informed of all major intelligence policies and activities and provide the information those Committees request.

(U//~~FOUO~~) Determining whether Congressional notification should be provided is a judgment based on the facts and circumstances and on the nature and extent of previous notifications to Congress on the same matter. Not every intelligence activity warrants Congressional notification. NSA's analysis of the FAA §702 incidents of non-compliance filed during 2013 resulted in two incidents reported in Congressional notifications; one related to a 2013 incident, and the other to an incident first reported in 2012.

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

~~(TS//SI//NF)~~ **Congressional Notification,** [redacted] reported a retention and dissemination compliance incident involving an NSA corporate database [redacted]

~~(TS//SI//NF)~~ **Congressional Notification,** [redacted] provided resolution of a matter first reported to the Congressional intelligence committees on [redacted] This update reported on the actions taken to resolve the matter, including correction of the affected system component, purge of affected transactions, verification that no disseminated reports had been based upon overcollected data, and implementatio n of a post-acquisition review of this type of data to identify future overcollection.

[101] (U//~~FOUO~~) [redacted] (b)(3)-P.L. 86-36

(U) Incidents of Non-compliance in 2013 (b)(3)-P.L. 86-36

(U//~~FOUO~~) In 2013, DoJ reported to the Court [redacted] incidents of non-compliance with FAA §702. The incidents and rates of occurrence are in Table 42.

(U//FOUO) Table 42. FAA §702 Incidents of Non-Compliance Reported in 2013

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

Incident Type	Percentage
Tasking Errors*	12%
Detasking Errors†	19%
Non-compliance with Notification Requirement‡	57%
Non-compliance with Documentation Requirement§	5%
Minimization Errors¶	6%
Other**	1%

* (U) Tasking errors—foreignness support was insufficient to support tasking (e.g., foreignness was not reestablished following travel to the United States, foreign intelligence purpose explanation was insufficient, or a typographical error was made).

† (U) Detasking error examples include: (1) delayed detasking which occurs when NSA has a foreign intelligence target, reasonably believed to be outside the United States at the time of tasking, and later learns that the target plans to travel to the United States, but does not detask the target's selectors before the target arrives in the United States; and (2) incomplete detasking of all tasked selectors when it is determined the target is no longer eligible for tasking.

‡ (U) Notification—NSA's targeting procedures require certain incidents be reported to NSD and ODNI within five business days, even if these incidents do not involve non-compliance with the targeting procedures. Specifically, NSA is required to terminate acquisition and notify NSD and ODNI if "NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person."

§ (U//~~FOUO~~) Documentation Errors—The targeting procedures require that NSA provide a citation to the source of information upon which the determination of the target's foreignness was made. These errors, in which the citations were not considered adequate to support the foreignness of the user of the selector tasked, were identified through DoJ and ODNI review of NSA tasking.

¶ (U) Minimization errors may include errors in querying, reporting, and retention.

** (U) The "other" incident type often pertains to instances in which systems that support compliance are not operating as intended.

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

(U//~~FOUO~~) Examples of incidents, including actions NSA took to mitigate recurrence, follow. This information is taken from the 13(b) notices DoJ NSD filed with the FISC.

(U//~~FOUO~~) Example 1: Incident as a result of delayed detasking

~~(TS//SI//NF)~~ Notice of Compliance Incident Regarding Section 702-Tasked Facilities, [redacted]

~~(S//SI//NF)~~ [redacted] NSA reported to the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) a delay in the detasking of

[redacted]

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

~~(TS//SI//NF)~~ [redacted] NSA determined [redacted] that the targeted user of [one of the selectors] had traveled to the U.S. [redacted] an NSA analyst detasked [the selector associated with the U.S. travel]. The analyst, however, inadvertently did not detask the other [redacted] [selectors] used by the target. NSA discovered this error [redacted] and detasked [redacted] the same day. The continued tasking of the [remaining selector] was not discovered until [redacted] when [the selector] was immediately detasked.

(U//~~FOUO~~) **Action taken to mitigate recurrence** The target office [was] reminded of the need to identify and immediately detask all facilities used by a target when the target is found to be in the United States.

(U//~~FOUO~~) NSA did not issue a Congressional notification about this incident. The incident was included in the *Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act*, dated March 2014.

(U//~~FOUO~~) Example 2: Other incident (technical error)

~~(S//NF)~~ Notice of Compliance Incident [redacted] 2013 (Preliminary) and [redacted] 2013 (Supplemental/Final)

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

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

~~(S//NF)~~ **Preliminary** [redacted] NSA orally notified the NSD of an incident regarding the [redacted] post-tasking checks NSA conducts to help ensure that [redacted] accounts tasked for collection pursuant to Section 702 are not being used from inside the U.S. NSA provided written notice of this incident to NSD and the ODNI [redacted]

~~(S//NF)~~ NSA identified the following compliance incident as a result of its ongoing process [redacted]

~~(S//NF)~~ NSA's post tasking [redacted] checks are intended to identify indications that users of Section 702-tasked [selectors] may be inside the U.S. [redacted]

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

~~(S//NF)~~ On [redacted] NSA identified that certain Section 702 [selectors] were not being sent from [redacted] to [redacted] thereby preventing [redacted]

[redacted]

[102] ~~(S//NF)~~ [redacted]

[103] ~~(S//NF)~~ [redacted]

checks from being conducted regarding these [selectors]

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

NSA has reviewed and confirmed that there is no indicating that any of the users of the selectors] were located in the U.S. as of

NSA made a modification to ensure that records with the are now sent to

~~(S)~~ NSA, NSD, and ODNI [at the time] continue[d] to investigate this incident. The Department of Justice [committed] to continue to inform the Court of additional information regarding this incident as it became available.

~~(S//NF)~~ **Supplemental/Final** As detailed in the preliminary notice..., NSA determined that certain Section 702 [selectors] were not being sent from NSA's to NSA's thereby preventing post-tasking from being conducted regarding these [selectors].

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

~~(S//NF)~~ NSA made a modification to ensure that

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

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

NSA determined that with respect to revealed no previously unknown indications

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

[104] ~~(S//NF)~~ NSA was in the process of fixing this issue at the time the 13(b) was reported to the FISC.

[105] ~~(S//NF)~~ NSA [at that time] continued to investigate the alert.

[106] ~~(S//NF)~~ To prevent the potential for a future compliance incident, NSA has corrected the error that prevented

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

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

[redacted] while those facilities were tasked for Section 702 acquisition. With respect to the remaining [redacted] [selectors], NSA has identified one confirmed period of roaming in the United States by the intended target, which lasted [redacted] days. [redacted] accounts have been detasked.

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

~~(S//SI//NF)~~ **Summary of action taken to mitigate recurrence** With respect to [redacted] [selectors] discussed above, NSA advises that the unique identifiers associated with communications acquired while users were or may have been in the U.S. were added to NSA's Master Purge List (MPL) in discover status[107] [redacted]

~~(S//NF)~~ The notice also stated that DoJ would include this issue in its quarterly report to the Court regarding Section 702 compliance occurrences and that the report would confirm that NSA had added the communications to the MPL in purge state.

(U//~~FOUO~~) NSA did not issue a Congressional notification about this incident. The preliminary incident of non-compliance was included in the *Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act*, dated March 2014.

(U) NSA Use of the FAA §702 Authority

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

~~(S//NF)~~ NSA asserts that the FAA §702 authority provides significant foreign intelligence information related to the foreign intelligence categories specified in the [redacted] FAA §702 certifications. The [redacted] certifications cover [redacted]

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

(U) Methods Used to Assess Effectiveness

(U//~~FOUO~~) NSA maintains a variety of statistics related to the FAA §702 authority that show the overall contributions to NSA SIGINT reporting, how customers value and use reports, and the unique access to foreign intelligence information FAA §702 provides. Data presented in this report is for calendar year 2013, unless otherwise noted, and statistics are limited to NSA reporting.

(U) FAA §702 contributions to SIGINT reporting

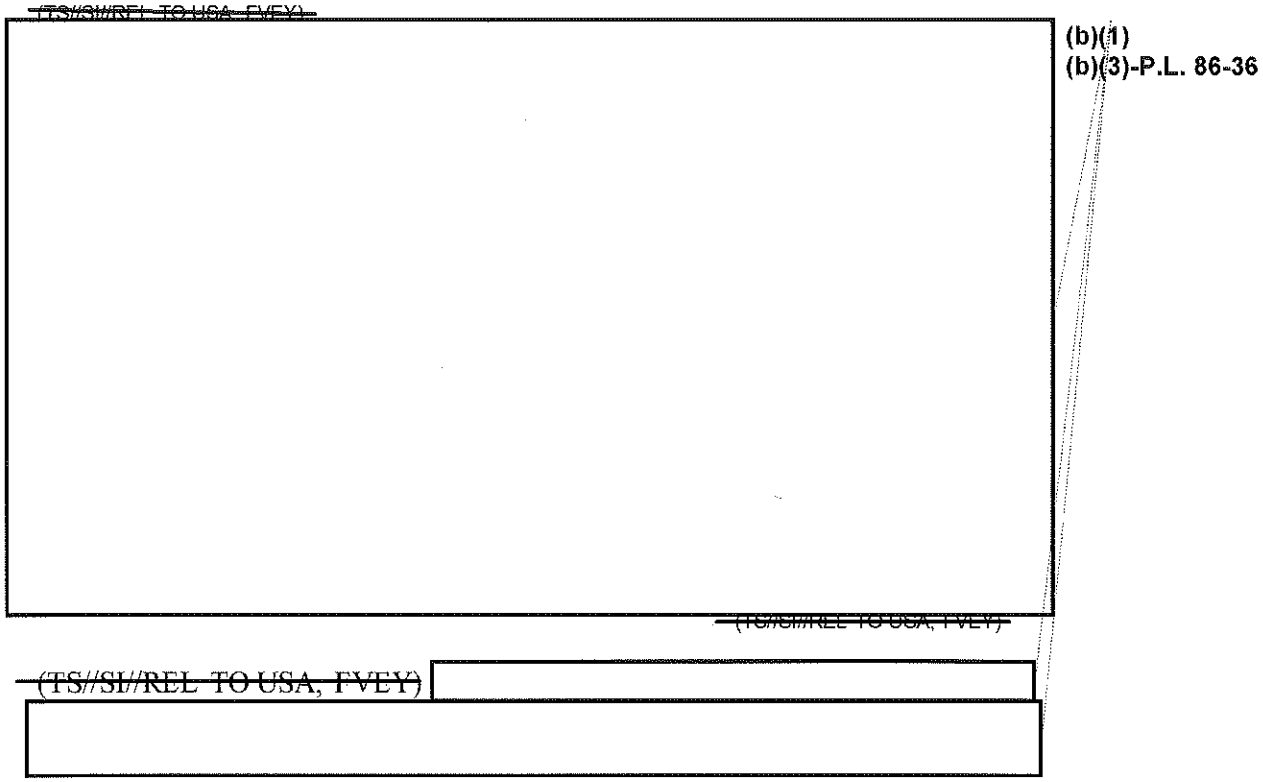
(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ As Figures 9 and 10 show, information obtained under FAA §702 is a key and growing source of reportable foreign intelligence to U.S. government consumers and allied foreign governments. Of the more than [redacted] SIGINT reports issued in calendar year 2013, [redacted] percent were based in whole or in part on FAA §702 information.

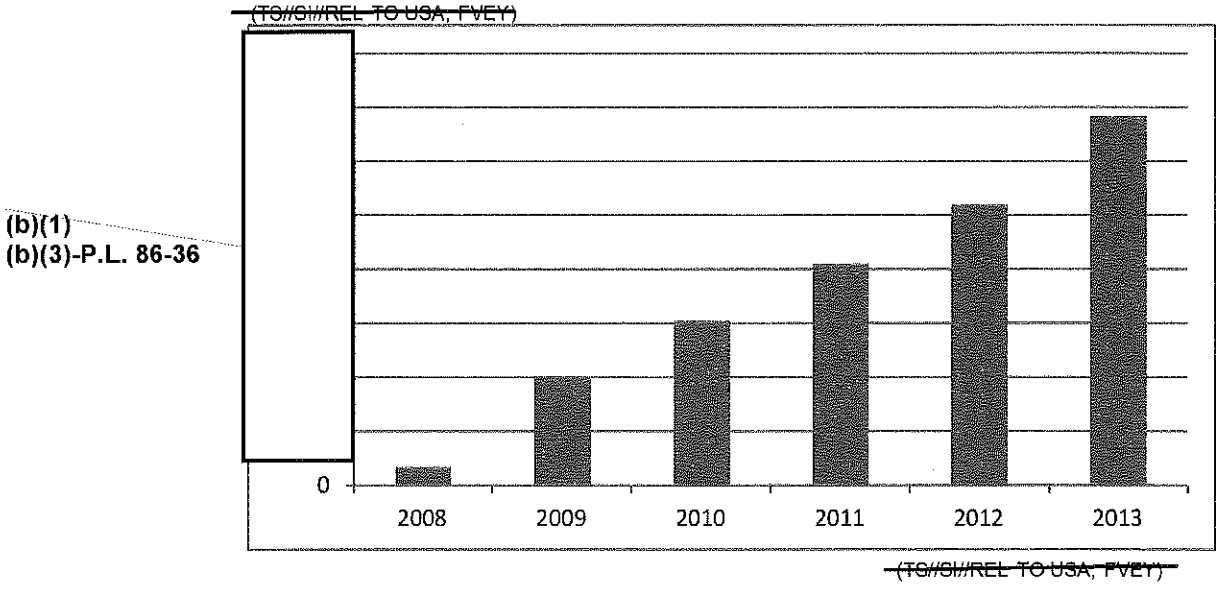
[107] ~~(S//NF)~~ [redacted]

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

(U) Figure 9. Total SIGINT Reports Issued in CY2013



(U) Figure 10. SIGINT Reports Based in Whole or in Part on FAA §702 or PAA Collection



[108] ~~(C//REL TO USA, FVEY)~~ When a report is solely sourced to an authority, it indicates that a particular source was used by the analyst but does not mean that the collection was only available from that one source of collection.

~~(TS//SI//REL TO USA, FVEY)~~ During 2013, NSA disseminated an average of over [redacted] serialized SIGINT reports a month that included information collected under the [redacted] FAA §702 certifications.[109]

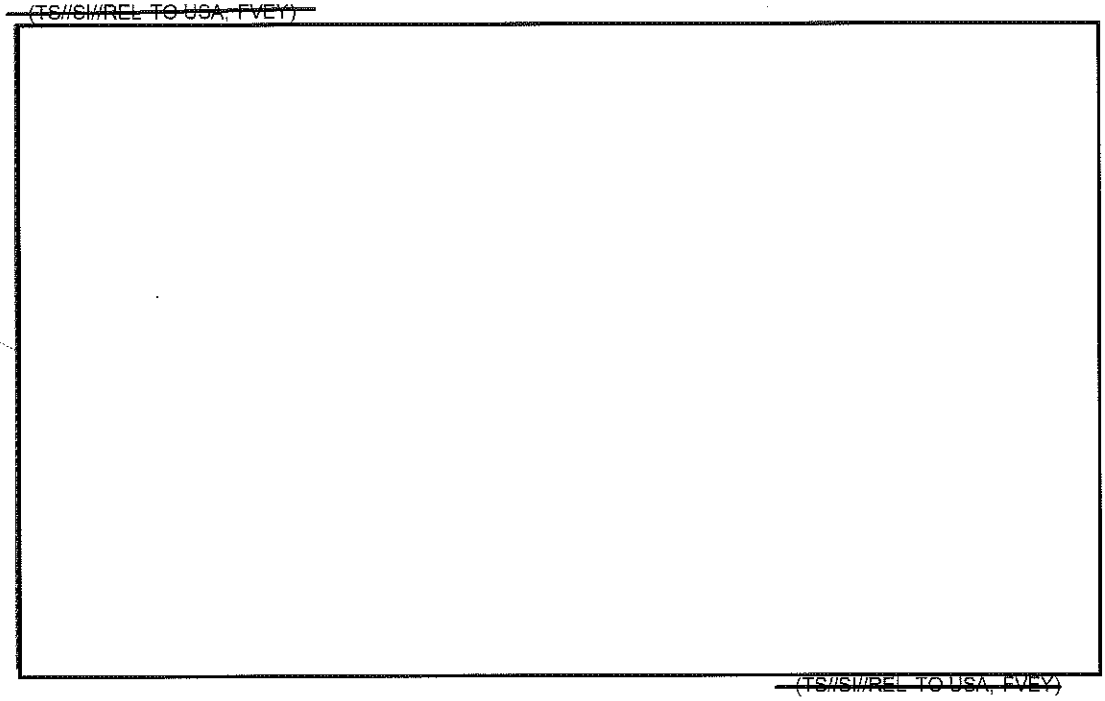
(b)(1)
(b)(3)-P.L. 86-36 ~~(S//SI//REL TO USA, FVEY)~~ NSA management believes that disseminated reports based on FAA §702 collection further the U.S. government's understanding of high priority international terrorism targets. Beyond disseminated reports, collection obtained under FAA §702 contributes to [redacted] and helps intelligence analysts [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ On average, during 2013 NSA disseminated [redacted] SIGINT reports per month concerning international terrorism that include information derived from FAA §702 collection.

(U) Figure 11. Terrorism-Specific SIGINT Reports Sourced with FAA §702 Information CY2013

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

~~(TS//SI//REL TO USA, FVEY)~~



~~(TS//SI//REL TO USA, FVEY)~~

[109] (U//~~FOUO~~) The number of issued reports was obtained in November 2014 from NSA's management information system for SIGINT production. The number of reports for any period is net of any reports recalled after they were issued.

~~(TS//SI//NF)~~ On average, more than [redacted] selectors were tasked for acquisition under FAA §702 during 2013. [redacted]

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

(U) Analyst Use of the Authority

~~(S//NF)~~ The FAA §702 authority is utilized broadly to support NSA missions. Its usefulness is confirmed by the above statistics, as well as the fact that the number of selectors tasked to the authority has increased [redacted] since 2010. Similarly, the increase in the number of reports sourced by FAA §702 communications has increased [redacted] in the same period.

(U) FAA §702 Contributions to the Intelligence Mission

(U) In 2013, NSA reported to the Senate Committee on the Judiciary that "information gathered from Section 702 of the FISA Amendments Act and Section 215 of the Patriot Act, in complement with NSA's other authorities, has contributed to the United States government's understanding of terrorism activities and, in many cases, has enabled the disruption of potential terrorist events at home and abroad."

(U) On 21 June 2013, NSA provided to several Congressional committees testimony concerning 54 cases in which these programs contributed to the U.S. government's understanding and, in many cases, disruption of terrorist plots in the United States and more than 20 countries.

(U) The SIGINT Directorate provided to the OIG additional examples of the value of FAA §702 collection to NSA missions.

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

~~(TS//SI//NF)~~ **Disruption of plot** [redacted] **targeting U.S. and** [redacted]

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

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

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

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

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

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

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

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

~~(TS//SI//NF)~~ Section 702

~~(TS//SI//NF)~~ Section 702

~~(TS//SI//NF)~~ Based on Section 702 collection, disrupted the potential attack

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

~~(TS//SI//NF)~~ **Disruption of plot**

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

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

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

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

~~(TS//SI//NF)~~ NSA analyzed and disseminated [redacted] information to the larger Intelligence Community. [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] based upon information obtained pursuant to Executive Order 12333 and Section 702, NSA [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ [redacted]

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

[redacted] NSA's analysis of Section 702-acquired communications revealed [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ Section 702 [redacted]

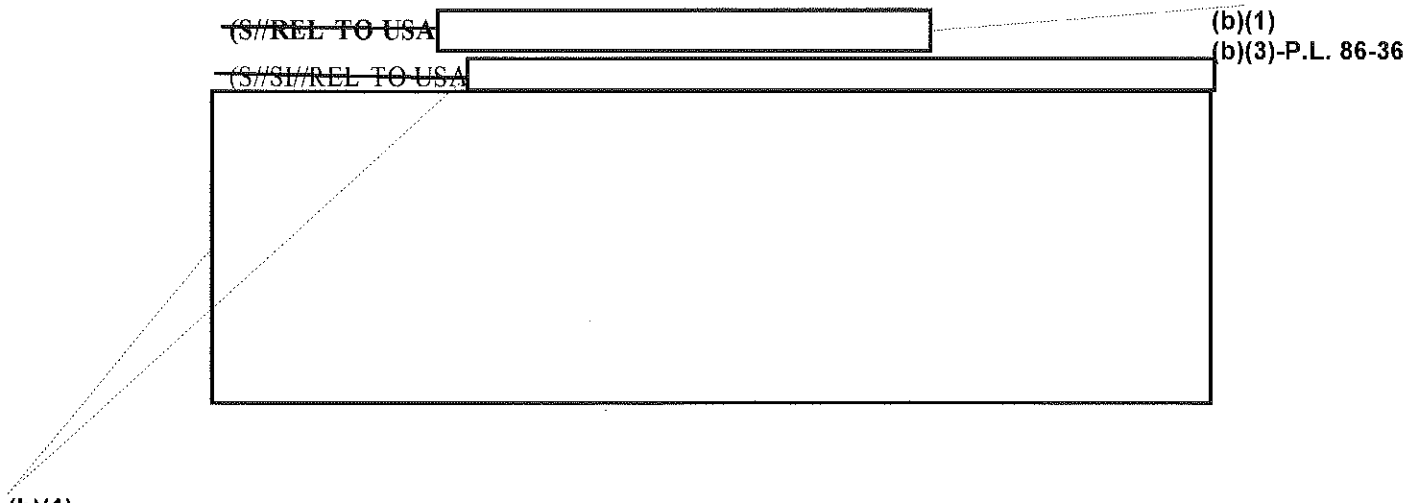
~~(TS//SI//NF)~~ [redacted]

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

~~(S//NF)~~ [redacted] had been arrested [redacted]

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

ST-14-0002



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

IV. (U) ABBREVIATIONS AND ORGANIZATIONS

(U) ADET	Associate Directorate for Education and Training
(U) AIG	Authorities Integration Group
(U) [redacted]	
(U) ATSD(IO)	Assistant to the Secretary of Defense for Intelligence Oversight
(U) [redacted]	
(U) BMD	Bulk metadata
(U) BR	Business Records
(U) [redacted]	
(U) CDR	Call Detail Record
(U) CIA	Central Intelligence Agency
(U) CMCP	Comprehensive Mission Compliance Program
(U) CSLI	Cell site location information
(U) CSP	Communication Service Provider
(U) CT	Counterterrorism
(U) DIA	Data Integrity Analyst
(U) DIRNSA	Director, NSA
(U) DMR	Dataflow Management Request
(U) DNI	Director of National Intelligence
(U) DoD	Department of Defense
(U) DoJ NSD	Department of Justice, National Security Division
(U) DTM	Directive Type Memorandum
(U) DTOI	Date and Time of Intercept
(U) EAR	Emphatic Access Restriction
(U) EDH	Enterprise data header
(U) [redacted]	
(U) E.O.	Executive Order
(U) FAA	FISA Amendments Act
(U) FBI	Federal Bureau of Investigation
(U) FISA	Foreign Intelligence Surveillance Act
(U) FISC	Foreign Intelligence Surveillance Court
(U) FTP	File Transfer Protocol
(U) [redacted]	
(U) [redacted]	
(U) HMC	Homeland Mission Coordinator
(U) IC	Intelligence Community
(U) IMEI	International Mobile Station Equipment Identity
(U) IMSI	International Mobile Subscriber Identity
(U) IO	Intelligence Oversight
(U) LAO	Legislative Affairs Office
(U) MCT	Multiple Communication Transaction

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

(U) MPL	Master Purge List
(U) MRG	Math Research Group
(U) [redacted]	
(U) NCTC	National Counterterrorism Center
(U) NSA	National Security Agency/Central Security Service
(U) NSAW	NSA Washington
(U) NSD	National Security Division
(U) NSOC	National Security Operations Center
(U) ODNI	Office of the Director of National Intelligence
(U) ODOC	Office of the Director of Compliance
(U) OGC	Office of General Counsel
(U) OIG	Office of the Inspector General
(U) OTR	Obligation to Review
(U) PKI	Public key infrastructure
(U) Q	Associate Directorate for Security and Counterintelligence
(U) RAS	Reasonable Articulable Suspicion
(U) RFI	Request for information
(U) [redacted]	
(U) S1S	Information Sharing Services Group
(U) S2	Analysis and Production
(U) S2I	Counterterrorism Production Center
(U) S2I4	Homeland Security Analysis Center
(U) S3	Data Acquisition
(U) S31324	[redacted]
(U) S354	[redacted]
(U) SCA	Special compliance activity
(U) SCIF	Sensitive Compartmented Information Facility
(U) [redacted]	
(U) SID	Signals Intelligence Directorate
(U) SIGINT	Signals Intelligence
(U) [redacted]	
(U) [redacted]	
(U) SOO	Senior Operations Officer
(U) [redacted]	[redacted]
(U) [redacted]	[redacted]
(U) [redacted]	Counterterrorism Division
(U) SV	SID Oversight and Compliance
(U) T12	[redacted]
(U) T1222	
(U) T131	
(U) T1323	
(U) T16	
(U) TD	Technology Directorate
(U) TR	Targeting request
(U) TS	[redacted]

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

(U) [redacted]	[redacted]
(U) TV	TD Office of Compliance
(U) TV4	Compliance and Verification
(U) USD(I)	Undersecretary of Defense for Intelligence
(U) USP	U.S. person
(U) USSID	U.S. Signals Intelligence Directive
(U) USSS	U.S. SIGINT System
(U) [redacted]	
(U) VoA	Verification of accuracy

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

(U) APPENDIX A: ABOUT THE §215 AND FAA §702 REVIEW

(U) Reason for Review

(U//~~FOUO~~) In September 2013, ten members of the Senate Committee on the Judiciary requested a comprehensive, independent review of the implementation of §215 of the USA PATRIOT Act and §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008 for calendar years 2010 through 2013.

(U) Objectives

(U//~~FOUO~~) In January 2014, the National Security Agency/Central Security Service's (NSA) Office of the Inspector General (OIG) and Committee staff agreed that the NSA OIG would review NSA's implementation of both authorities for calendar year 2013. The study has three objectives:

(U) Objective I

- (U) Describe how data was collected, stored, analyzed, disseminated, and retained under the procedures for §215 and FAA §702 authorities in effect in 2013 and the steps taken to protect US Person information.
- (U) Describe the restrictions on using the data and how the restrictions have been implemented, including a description of the data repositories and the controls for accessing data.
- (U) Describe oversight and compliance activities performed by internal and external organizations in support of §215 Foreign Intelligence Surveillance Court (FISC) Orders and FAA §702 minimization procedures.

(U) Objective II

- (U) Describe incidents of non-compliance with §215 FISC Orders and FAA §702 Certifications and what NSA has done to minimize recurrence.

(U) Objective III

- (U) Describe how analysts used the data to support their intelligence missions.

(U//~~FOUO~~) The report also provides a summary of the changes made in the implementation of both authorities for calendar years 2010 through 2012 and for §215, a list of incidents of non-compliance for calendar years 2010 through 2012.

(U) Scope and Methodology

(U//~~FOUO~~) Our study of NSA's implementation of the §Section 215 and FAA §702 authorities was based largely on program stakeholder interviews and reviews of policies and procedures and other program documentation. For this review, the NSA OIG documented the controls implemented that address the requirements of each authority. However, we did not verify through testing whether the controls were operating as described by program stakeholders.

(U) Section 215

(U//~~FOUO~~) Our §215 review focused on the BR FISA program control framework, incidents of non-compliance, and NSA's use of the authority to support its counterterrorism (CT) mission in 2013. To document the BR FISA control framework, we used BR Order 13-158, approved by the FISC on 11 October 2013 and effective through 30 January 2014, and compared the requirements listed in that Order with the processes and controls NSA used to maintain compliance with that Order. In addition, we documented the changes implemented in the BR FISA program following the President's directives in 2014.

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

(U//~~FOUO~~) We interviewed personnel in the Signals Intelligence Directorate's (SID) Oversight and Compliance (SV), Information Sharing Services Group (S1S), Homeland Security Analysis Center (S2I4), Data Acquisition (S3), [redacted] and Counterterrorism [redacted] division; the Technology Directorate's (TD) Office of Compliance (TV), [redacted] the Office of the Director of Compliance (ODOC); the Authorities Integration Group (AIG); the Legislative Affairs Office (LAO); and the Office of General Counsel (OGC).

(U) FAA §702

~~(TS//SI//NF)~~ In addition to FAA §702 stakeholder interviews and reviews of policies and procedures and other program documentation, information obtained in the OIG's *Assessment of Management Controls Over FAA §702,* revised and reissued 29 March 2013, was also used as a resource. That review examined the controls that NSA used to maintain compliance with FAA §702 and the targeting and minimization procedures associated with the 2011 certifications.

~~(TS//SI//NF)~~ Our FAA §702 review focused on the processes and controls in place in 2013. Two primary documents filed annually with each FAA §702 certification comprise NSA's procedures for complying with the FISA Amendments Act of 2008:

- (U//~~FOUO~~) The *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (FAA §702 Targeting Procedures), and

- (U//~~FOUO~~) The *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (the FAA §702 Minimization Procedures).

(U//~~FOUO~~) For calendar year 2013, the period under review, different versions of these documents were in effect because of changes made with the annual certification renewal and special amendments.

- (U//~~FOUO~~) FAA §702 Targeting Procedures
  - (U//~~FOUO~~) Procedures approved with the 2012 renewal of the authority, effective 24 September 2012
  - (U//~~FOUO~~) These procedures were not changed for the 2013 certification renewal and remained effective 10 September 2013 through 9 September 2014.
- (U//~~FOUO~~) FAA §702 Minimization Procedures
  - ~~(S//NF)~~ Procedures approved for the 2012 certification renewal, approved by the FISC 24 August 2012, were effective 24 September 2012 through 23 September 2013. [redacted]

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

  - ~~(S//NF)~~ [redacted]

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

(U//~~FOUO~~) We also examined implementing procedures and controls for the Attorney General's targeting guidelines.

(U//~~FOUO~~) We interviewed personnel in SID Policy and Corporate Issues Staff (S02), SV, Analysis and Production (S2) Staff and Product Lines, Data Acquisition (S3), [redacted] and [redacted] the TV, [redacted] and Mission Capabilities (T1), ODOC, the LAO, and OGC.

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

(U) Prior Coverage

(U//~~FOUO~~) Since 24 May 2006, the date the original BR Order was signed, the NSA OIG has completed five BR FISA program reviews. Table A-1 summarizes the reviews the NSA OIG has performed on the BR FISA program.

(U) Table A-1. NSA OIG Reviews of the BR FISA Program

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

Date Issued	OIG Review	Scope of the Review
09/05/06	Assessment of Management Controls for Implementing the FISC Order: Telephony BR (ST-06-0018)	Reviewed collection, processing, analysis, dissemination, and oversight controls.
05/12/10	NSA Controls for FISC BR Orders (ST-10-0004)	Reviewed querying and dissemination controls; summarized pilot test results for the period from January through March 2010.
05/25/11	Audit of NSA Controls to Comply with the FISC Order Regarding BR (ST-10-0004L)*	Reviewed querying and dissemination controls; summarized the monthly test results for 2010.
10/20/11	Audit of NSA Controls to Comply with the FISC Order Regarding BR Retention (ST-11-0011)	Verified age-off of BR FISA metadata in 2011 to maintain compliance with the 60 month retention requirement of the BR Order.
08/01/12	NSA Controls to Comply with the FISC Order Regarding BR Collection (ST-12-0003)	Reviewed collection and sampling controls for ensuring that NSA receives only the BR FISA metadata authorized by the BR Order.
* This report summarized monthly test results of the BR querying and dissemination controls during 2010.		

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

(U//~~FOUO~~) Since the Agency obtained FAA §702 authority in January 2008, the NSA OIG has completed annual reviews of reports containing references to USP identities and targets later determined to be located in the United States, as required by the statute. Table A-2 summarizes the two reviews the NSA OIG has completed of the FAA §702 program.

(U) Table A-2. NSA OIG Reviews of the FAA §702 Program

~~(S//NF)~~

Date Issued	OIG Review	Scope of the Review
3/29/13	(U) Assessment of Management Controls Over FAA §702 (ST-11-0009)	(U//~~FOUO~~) Reviewed management controls for maintaining compliance with the targeting and minimization procedures.
[redacted]	~~(S//NF)~~ [redacted]	~~(S//NF)~~ [redacted]

~~(S//NF)~~

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

(U) APPENDIX B: BR FISA PROGRAM CHANGES 2010-2012

(U) 2010

- (U//~~FOUO~~) On 25 June 2010 [redacted] NSA's RAS selection term management system, [redacted]
- (U//~~FOUO~~) [redacted] the Order requirement restricting the number of analysts allowed to access BR metadata was lifted.
- (U//~~FOUO~~) [redacted] the Order requirement for weekly reports of BR-related disseminations was changed to monthly.

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

(U) 2011

- (U//~~FOUO~~) [redacted] primary repository for detailed telephony transaction records.
- (U//~~FOUO~~) [redacted]

(U) 2012

- (U//~~FOUO~~) [redacted] the Order requirement for NSA to review a sample of records obtained was changed to a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired.
- (U//~~FOUO~~) [redacted] NSA notified the Court [redacted]
- (U//~~FOUO~~) [redacted] NSA notified the Court [redacted]
- (U//~~FOUO~~) [redacted] the Court authorized NSA to implement an automated querying process.[110]

[110] (U//~~FOUO~~) NSA is no longer authorized to use the automated query process since it withdrew its request to do so in the renewal applications and declarations that support the BR Orders approved by the FISC (beginning with BR Order 14-67, dated 28 March 2014).

- (U//~~FOUO~~) On 29 November 2012, the Order requirement to track and report the number of instances, since the preceding report, in which NSA has shared, in any form, results from queries of the BR metadata, in any form, with anyone outside NSA was changed to apply to only sharing of query results that contain U.S. person information.

(U) APPENDIX C: BR FISA PROGRAM INCIDENTS OF NON-COMPLIANCE 2010 THROUGH 2012

(U) Table C-1. BR FISA Incidents 2010 through 2012

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

Date Filed	Notice Type	Docket(s)	Congressional Notification	Description

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

* (U//~~FOUO~~) On 1 November 2010, Rule 10(b) and 10(c) notices were replaced by Rule 13(a) and 13(b) notices respectively.
† (U//~~FOUO~~) Final Rule 10(c) notice
‡ (U//~~FOUO~~) Supplemental Rule 13(b) notice
§ (U//~~FOUO~~) Final Rule 13(a) and 13(b) notice

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

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

(U) APPENDIX D: FAA §702 PROGRAM CHANGES

(U) Minimization Procedures

(U) 2011

- (U//~~FOUO~~) Language on upstream data added to Minimization Procedures.
- (U//~~FOUO~~) The retention period for Upstream Data is reduced to two years
- (U//~~FOUO~~) Clarified that the five-year retention period for unevaluated data began to run from the date of expiration of the certification under which the data was collected. Prior versions did not specify when the five-year period began.
- (U//~~FOUO~~) Permitted queries using USP identifiers to identify and select communications. Requires pre-approval before any queries are made. Specifically excludes queries against upstream data.
- (U//~~FOUO~~) Adds requirement to segregate Internet transactions that cannot be reasonably identified as containing single discrete communications.

(U) 2012

- (U//~~FOUO~~) Limited access to metadata from Internet transactions to data acquired on or after October 31, 2011.
- (U//~~FOUO~~) Adds specific requirements for DIRNSA determination that a domestic communication can be retained. This includes a requirement that DIRNSA first determine that the sender or recipient of the domestic communication was properly targeted under FAA §702.

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

- ~~(S//REL TO USA~~ [redacted]

(U) 2013

- (U) An amendment to the Minimization procedures was made in late 2013. A section was added precluding NSA from using information acquired pursuant to FAA §702 unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to be outside the United States at the time the information was acquired.

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

- ~~(S//REL TO USA~~ [redacted]

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

(U) Other Changes

(U) 2012

- ~~(TS//SI//NF)~~ Congress notified by NSA [redacted]
- ~~(TS//SI//NF)~~ NSA begins [redacted]

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

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