Access to this document will be restricted to those approved for the following specific activities:

________________________
________________________
________________________
________________________
Lesson 1 - Introduction to the Business Records (BR) FISA
Lesson 2 - Reasonable Articulable Suspicion (RAS)
Lesson 3 - First Amendment Considerations
Lesson 4 - The BR FISC Order
Lesson 5 - Accessing, Sharing, Dissemination, and Retention

Welcome to the Business Records (BR) FISA web-based training (WBT).

This course provides training for analysts who will be authorized to query the raw metadata collected by the BR FISA.

The course is comprised of five Lessons.

The lessons contained in the BR FISA course are:
- Lesson 1 - Introduction to the Business Records (BR) FISA
- Lesson 2 - Reasonable Articulable Suspicion (RAS)
- Lesson 3 - First Amendment Considerations
- Lesson 4 - The BR FISC Order
- Lesson 5 - Accessing, Sharing, Dissemination, and Retention

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20041001
The course begins with an overview of the BR FISA authority and then moves into an overview of the Reasonable Articulable Suspicion standard. Next, students will explore First Amendment considerations before taking a closer look at the BR FISC Order. The BR Order points out special considerations that distinguish this FISA authority from other FISAs typically encountered at this Agency. The final lesson of this course provides specific rules and procedures regarding the access, sharing, dissemination, and retention of BR FISA metadata.
Lesson "Welcome", Slide 3 Course Objectives

At the conclusion of this course you should be able to:

- Identify terms and processes associated with the Business Records FISA Order
- Identify common sources of information used for determining RAS
- State limitations for targeting US persons under the RAS standard
- Identify access, sharing, dissemination, and retention procedures under the BR FISA Order
As you progress through the different course lessons you may want to also access the related Legal Readings. The two core readings are the Reasonable Articulable Suspicion (RAS) memorandum written by OGC and the BR FISC Order issued by the FISA Court.

You can access these documents by clicking on the Legal Readings button located in eCampus.
BR FISA = Specific authority given by the FISA Court (FISC) that allows NSA to obtain metadata from the business records of certain specified telecommunication companies.
Lesson 1 - Introduction to the Business Records (BR) FISA

Lesson 1 – Introduction to the BR Objectives:

- Identify the purpose of the BR FISA
- Recognize the groups covered by the BR FISA Order
- Define terms relevant to the BR FISA Order: telephony metadata, telephony identifier, hops, and Seed
Overview of RAS

The term *associated* is defined in the RAS Memo to mean, “engaged in a common enterprise” with:

- One of the groups designated by the National Counter Terrorism Center (NCTC) to have allied itself with
  - Someone acting as their agent.

- No other groups other than those listed in the BR FISC Order can be used to justify access under the BR FISA authority.
“Telephony Metadata and Telephony Identifiers”

Telephony metadata
Metadata collected – includes comprehensive communications routing information
- Originating and terminating telephone numbers
- International Mobile Subscriber Identity (IMSI) numbers
- Mobile Subscriber Integrated Services Digital Network (MSISDN) numbers
- International Mobile station Equipment Identity (IMEI) numbers
- Trunk identifiers
- Telephone calling card numbers
- Time and duration of calls

Telephony metadata does NOT include
- Substantive content of any communication
- Name, address, or financial information about a subscriber or customer

Telephony identifiers correlate to Business Records metadata collected by the providers, such as MSISDN or a calling card number. Telephony identifiers are also known as identifiers.
A telephony identifier (selector), is called a Seed when it is being used to search the BR repository. When querying the BR metadata repository, Business Records FISA (BRF)-approved individuals, also known as BRF chainers, conduct contact chaining queries in order to obtain the contacts between a seed and other telephone identifiers (numbers in contact with the RAS-approved-Seed).

Under the BR FISA Order, a query always begins with a RAS-approved-Seed. In this case the RAS-approved-telephone identifier is called a 'Seed' because it is being used for chaining and analysis to create a 'tree' of contacts and identify new potential terrorist associations.

The BR FISC Order authorizes "3-hop chaining"; however it is CT's[1] recommended practice to restrict chaining to two hops. This means that telephony identifiers up to two hops away from the Seed may be chained. Chaining reveals the contacts of the identifier.
Associations to establish a RAS nomination

Reasonable Articulable Suspicion (RAS) standard - requires that an NSA analyst must be able to point to a single fact that points to the fact that a selector may be associated with a terrorist group listed in the FISC Order before we are authorized to conduct analysis on it.

RAS determination - should cause a reasonable person to suspect that the identifier is associated with one of the terrorist organizations named in the Order.

(TS//SI//NF) Recall that the BR FISC Order allows NSA to obtain an immense amount of foreign and US metadata contained in the Business Records. The FISC Order contains strict guidelines on when this metadata is allowed to be accessed and when it is not. It must be associated with specific terrorist organizations named in the Order. It also must meet a standard that is referred to as the Reasonable Articulable Suspicion (RAS) Standard. In a nutshell, the RAS standard requires that an NSA analyst must be able to point to a single fact that points to the fact that a seed/telephone selector may be associated with a terrorist group listed in the FISC Order before we are authorized to conduct analysis on it.

(TS//SI//NF) We will address the RAS standard in detail in the next lesson, but for now, understand that the fact or facts which make up a RAS determination should cause a reasonable person to suspect that the identifier is associated with one of the terrorist organizations named in the Order.
# Legal Disclaimer

This course is not designed to take the place of specific guidance from a Homeland Mission Coordinator (HMC), the Office of Oversight & Compliance (SV), or from the Office of General Counsel (OGC). The course is designed to enhance your understanding of how to comply with the BR FISC Order and to understand the RAS standards used in concert with BR FISA.

Because, the BR FISC Order is renewed approximately every 60-90 days, the FISC may change the authority or place new restrictions in a new FISC Order. It is important to understand that unique operational circumstances may result in a change in guidance from this course. Therefore, if you experience any uncertainty, it is always sound advice to contact your local HMC, SV, or OGC for case-specific guidance.

<table>
<thead>
<tr>
<th>IS NOT designed to take the place of:</th>
<th>IS designed to enhance understanding of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homeland Mission Coordinator (HMC)</td>
<td>BR FISC Order</td>
</tr>
<tr>
<td>Office of Oversight &amp; Compliance (SV)</td>
<td>RAS standards</td>
</tr>
<tr>
<td>Office of General Counsel (OGC)</td>
<td></td>
</tr>
</tbody>
</table>

Renewed approximately every 60-90 days
Contact your local HMC, SV, or OGC for case-specific guidance.
Summary

You should now be able to

- Identify the purpose of the BR FISA Order
- Recognize the groups covered by the BR FISA Order
- Define terms relevant to the BR FISA Order: telephony metadata, telephony identifier, hops, and Seed

(TSO/NF) You have now completed the lesson that discusses the BR FISA authority.

(TSO/NF) You should now be able to:
- Identify the purpose of the BR FISA Order
- Recognize the groups covered by the BR FISA Order
- Define terms relevant to the BR FISA Order: telephony metadata, telephony identifier, hops, and Seed
BR FISA course lessons:
Lesson 2 – Summary of the Standard

• Define the Reasonable Articulable Standard (RAS) used to justify a BR FISA metadata search
• Identify prohibitions against instinct and hunches in contrast to facts
• Identify common sources of information used for justifying a RAS
• List the common sources of information on which analysts rely in making RAS determinations

This lesson provides an overview of the Reasonable Articulable Suspicion (RAS) Standard. RAS guidance is outlined in an OGC memo. It provides definitions and descriptions that will help you understand how to satisfy RAS and how to apply it to identifiers under the BR Court Order.

The BR FISA Order also states that in order to access the BR FISA metadata, NSA must establish RAS on each selector that it wishes to query within the metadata. Only a Homeland Mission Coordinator (or named individual in the Order) may make a RAS determination and thus authorize a selector for querying. However, you are responsible for ensuring that a selector has been approved for RAS prior to querying the BR FISA metadata. You may even be responsible for drafting RAS requests outlining why a selector should be RAS approved.

This lesson will enable you to:
• Define the Reasonable Articulable Standard (RAS) used to justify a BR FISA metadata search
• Identify prohibitions against instinct and hunches in contrast to facts
• List the common sources of information on which analysts rely in making RAS determinations
• List the ten most typical sources of information on which analysts rely in making assessments of Reasonable Articulable Suspicion (RAS)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20341081
Summary of RAS Standard

BR FISC Order

Government may request to use specific identifiers to query the metadata for purposes of obtaining foreign intelligence through contact chaining or:

- telephone numbers
- [Redacted]
- [Green Redacted]

"Reasonable Articulable Suspicion standard"

You will recall from Lesson One that the BR FISA Order is authorized because the FISC recognizes there is a counterterrorism interest in obtaining those business records. However, because NSA is receiving a great deal of US person telephony records, we have strict guidelines on when NSA can access the metadata under this authority. One of the requirements is that in order to access the metadata, NSA must establish RAS on each selector prior to querying the BR FISA repositories.

The BR FISA Order states that NSA may query specific identifiers that satisfy the RAS standard for purposes of obtaining counterterrorism intelligence.

In order to assist in determining when a selector has satisfied the RAS standard, the Office of General Counsel (OGC) has issued a RAS Memo to help Signals Intelligence Directorate (SID) personnel make RAS determinations on telephone identifiers. The memo contains guidelines that apply to both the BR and Pen Register and Trap and Trace (PR/TT) FISA Orders.
RAS Standard Definition

RAS standard requirements

- fact(s) that cause suspicion the number is associated with
  - must be approved by the a Homeland Mission Coordinator or other named official in the FISC Order before you use a telephone number identifier to query the database of records
- no hunches or guesses to justify targeting

There must be at least one qualifying fact giving rise to a reasonable articulable suspicion that the identifier is associated with one of the terrorist groups listed in the BR FISA Order.

The RAS must be approved BEFORE you can use an identifier to query the BR metadata. Analysts are not allowed to use a hunch or a guess to nominate selectors for RAS. RAS nominations or requests nominations must specify facts that would cause a reasonable person to form that suspicion.

The RAS standard is far less than proof by "probable cause" or "a preponderance of evidence" — it merely requires one fact that can be articulated which would cause a reasonable person to form a suspicion.
Lesson 2: Reasonable Articulable Suspicion (RAS)

Sources of Information

1. A published NSA report
2. Unpublished SIGINT collection
3. Content analysis
4. SIGDEV work
5. Direct collection
6. NSA target knowledge databases
7. Any content analysis where a targeted person
8. Information from NSA target knowledge databases
9. Information obtained from belonging to one of the Foreign Powers
Sources of Information

- SIGINT reports
- Investigations by the CIA or FBI
- FISA surveillance data derived from other authorized targets
- SIGDEV work tied to published information
- Other transcripts

Published reports
- Preliminary investigations
- Full field investigations
- FISA surveillance
- SIGDEV work tied to published information
- Transcripts

The RAS memo also lists other sources of information available for researching a RAS. These include but are not limited to:

- Published reports such as:
  - SIGINT reports
  - Investigations by the CIA or FBI
  - FISA surveillance data derived from other authorized targets
  - SIGDEV work tied to published information
  - Other transcripts

Looking at the IC and public sector (open source) sources we use, these include:

- The Federal Bureau of Investigation
- The Central Intelligence Agency
- The National Counterterrorism Center
- The National Counterterrorism Center
- Public records available on the internet, newspapers or other public resources.
SUMMARY

You should now be able to:

- Define the Reasonable Articulable Standard (RAS) used to justify a BR FISA metadata search
- Identify prohibitions against instinct and hunches in contrast to facts
- Identify common sources of information used for justifying a RAS
- List the common sources of information on which analysts rely in making RAS determinations
Lesson 3 – First Amendment Considerations

- List some basic protections of US persons provided by the First Amendment of the US Constitution.

- Describe the prohibition against using First Amendment protected activities as the sole justification for a RAS involving a US person.
The First Amendment of the US Constitution prohibits Congress from making any laws that would infringe on the free exercise of:

- Religion
- Speech
- The press
- Peaceable assembly
- To petition the government for redress of grievances

Remember the RAS Memo clarifies the FISC’s prohibition of a RAS determination based solely on activities that are protected by the First Amendment. This applies when targeting a US person as defined in USSID SP0018 or a person reasonably believed to be located inside the United States.
SUMMARY

You should now be able to:

• List five basic protections for US persons provided by the First Amendment of the US Constitution

• Describe the prohibition against using First Amendment protected activities as the sole source of justification for a selector involving a US person.
In this lesson we will examine a Business Records (BR) FISA Court (FISC) Order.

At the conclusion of this lesson you will be able to:

• Identify BR FISC Orders as NSA’s authorization to collect telephony metadata from specified US telecommunication companies in order to protect against international terrorism.
"What are BR Orders?"

The authority is for collection of tangible things gathered by the FBI to protect the US against international terrorism.

- The RAS standard requires an ability to articulate an association with terrorist groups listed within the order.
“Tangible Things as only Telephony metadata”

“tangible things”

“an electronic copy of telephony metadata (call records).”

- Comprehensive communications routing information including:
  - Originating and terminating telephone number
  - International Mobile subscriber Identity (IMSI) number
  - International Mobile station Equipment Identity (IMEI) number
  - The trunk identifier
  - Telephone calling card numbers
  - Time and duration of call

The telephony metadata does not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer within these.

(TS/SCI/NF) The BR FISA Order specifically states that the telephony metadata does not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer within these. The FISA Order deliberately restricts access to only communications metadata.
"Affiliation with Foreign Power"

RAS (Reasonable Articulable Suspicion)

- Justifies the search of metadata
- a statement of fact that supports a reasonable suspicion that the identifier is affiliated with one of the terrorist groups listed in the BR FISA Order.

(TS/SCI) The metadata obtained from the BR FISA authority is used to establish connections with terrorist organizations by using contact chaining and queries. These queries look at the contacts of known terrorists to help NSA establish new connections and affiliations with terrorist groups listed in the BR FISA Order.

(TS/SCI) Before searching the BR metadata repository, NSA must establish RAS on each selector in order to conduct a search within the metadata. RAS is a statement of fact that supports a reasonable suspicion that the identifier is affiliated with one of the terrorist groups listed in the BR FISA Order. Only Homeland Mission Coordinators and others named in the BR FISA Order can make a RAS determination.

(TS/SCI) Remember, the RAS cannot be solely based on activities which are protected by the First Amendment of the US Constitution.

(TS/SCI) To see samples of RAS statements please open the ‘RAS statements’ Job Aid located in the legal readings for this course.
You should now be able to:

- Identify BR FISC orders as NSA's authorization to collect telephony metadata from specified US telecommunication companies in order to protect against international terrorism.
Lesson Objectives

In this lesson we will continue to examine the Business Records (BR) FISA Court (FISC) Order. At the conclusion of this lesson you will be able to:

- Distinguish between analysts authorized to query BR FISA metadata and individuals authorized to receive results of those queries
- Identify further limitations on accessing, sharing, disseminating, and retaining BR FISA metadata
The BR FISA Query Analyst

The Director of NSA (DIRNSA) strictly controls access to and use of raw BR metadata.

Query access to BR raw metadata is limited to individuals trained and designated as BR FISA Query Analysts.

The BR metadata is authorized to be stored in two NSA repositories—

Authorized Query Analysts are permitted to query BR raw metadata within___ ___to receive query results.
Oversight for Access Restrictions

BR Court order requires logging for auditing purposes:
- Query requests
- User login
- IP address
- Date and time of the access

(U//FOUO) This is very important so we'll reiterate it with more detail.

(TS//SI//NF) Signals Intelligence Directorate's Office of Oversight and Compliance has implemented a series of auditing controls designed to limit access to the BR FISA metadata only to those who have been briefed by the OGC and those who have completed all of the required training.

(TS//SI//NF) When the raw metadata is accessed in order to perform a query, an automatic audit log is recorded that includes:
- Query request
- User login
- Internet protocol address
- Date and time of the access
Distributing BR FISA query results

It is the BR FISA Query Analyst's responsibility to ensure that the recipient of the query results is approved to receive BR derived information.

(TS/SCI/NF) Remember only a select number of analysts are authorized to query the raw metadata.

(TS/SCI/NF) When distributing BR FISA query results the distributions are categorized as those internal to NSA which will be called 'Sharing' and those outside of NSA which will be called 'Dissemination'.

(TS/SCI/NF) It is the BR FISA Query Analyst's responsibility to ensure that the recipient of the query results is approved to receive BR derived information.
Before we discuss distribution, it is important to define query results. So, what are query results?

A “query result” is a piece of information that would not have been known, or a statement of fact or opinion that would not have been made, but for information revealed following a BR or Pen Register and Trap and Trace (PR/TT) query using a RAS (Reasonable Articulable Suspicion) -approved selector.

- This definition includes information in the form in which it appears immediately following a BR or PR/TT query, e.g., ____ as well as information that has changed form, e.g., a statement describing certain links in a contact chain. Summaries derived from BR chaining are also query results.
- This definition makes no distinction between minimized and unminimized information.
Sharing of BR FISA query results can take place formally or informally and may take place orally or in writing. Sharing can even include a phone call.

So, when do the restrictions on the sharing of query results cease to apply?

The term "query result" does not govern properly disseminated SIGINT products containing information derived from authorized queries of the BR or PR/TT metadata.

The term "query result" does not extend to identifiers discovered as a result of authorized queries of the BR or PR/TT metadata, to the extent those identifiers are used for tasking purposes elsewhere. E.g., a foreign identifier discovered as a result of an authorized BR query may be tasked in __________ and neither the tasking information contained in __________ nor the collection that results would continue to require the sharing restrictions applicable to BR query results.
You are responsible for following current Order's rules when sharing BR FISA query results.

The person who is sharing a query result is responsible for ensuring that the recipient is authorized to receive it. To see your current responsibility please refer to the job-aid entitled BR FISA Query Analyst Responsibilities.

Individuals who receive BR derived information (query results) must be briefed by the OGC and have current OVSC1800 training. They will be authorized by SID Office of Oversight and Compliance SV4 to receive BR query results. Remember, authorization to receive query results does not authorize access to BR raw metadata.
Sharing Procedures

If any BR FISA derived metadata is to be shared or coordinated beyond the personnel who are approved to receive it, contact the Office of Oversight and Compliance or the Office of General Counsel BEFORE you share!
**Dissemination Procedures**

The Court Ordered procedures for disseminations of query results apply from USSID SP0018. In addition, there are a couple of unique requirements:

1. Chief S12 or the NSOC SOO (or one of the three other named positions in the BR FISA Order) must approve the dissemination of US person information.

2. Any US person information disseminated must be for a counterterrorism purpose and necessary to understand the counterterrorism information or assess its importance.

3. Further, all disseminations must be reported in a weekly report to the FISC.
Retention

Retention of raw metadata, chain summaries, and query results is limited to 5 years.

This applies to all repositories holding BR FISA metadata.
Lesson Summary

You should now be able to:

- Distinguish between analysts authorized to query BR FISA metadata and individuals authorized to receive results of those queries
- Identify further limitations on accessing, sharing, disseminating, and retaining BR FISA metadata
Homeland Mission Coordinators:
DL S2I41_HMC (ALIAS) S2I5

Oversight and Compliance:
SV4  DL_SV42

General Counsel:
'go gc' or