

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160816 FINAL

OVSC1203: FISA Amendments Act Section 702

(U) Introduction

~~(TS//SI//NF~~) NSA operates under various authorities to acquire foreign intelligence information. FAA Section 702 provides NSA with the means to compel U.S. electronic communications service providers to assist in acquiring foreign intelligence information from communications of non-U.S. persons (non-USPs) reasonably believed to be located outside the U.S. This course provides training and guidance to enable you to handle and protect

(U) Course Objectives

(U) At the completion of this course, you should be able to:

- ~~(U//FOUO)~~ Describe the target requirements under the FAA Section 702 authority
- ~~(U//FOUO)~~ Describe the collection methods in which NSA acquires FAA Section 702 data
- ~~(U//FOUO)~~ Summarize the analyst's responsibilities pertaining to targeting, reviewing, retaining, and disseminating the data collected under NSA's FAA Section 702 authority
- ~~(U//FOUO)~~ Summarize the steps that might be required to remediate a potential compliance incident

(U) The overall classification of this course is ~~TOP SECRET//SI//NOFORN~~.

(U) This course, including the final assessment, requires an estimated **4 hours** to complete.

(U) Course Audience

~~(U//FOUO)~~ This course is intended for all personnel who require access to raw SIGINT databases containing FAA Section 702 derived data.

(U) Course Requirements

(U) This course is required annually.

(U) The annual prerequisites for this course are:

- (U) Overview of Signals Intelligence (SIGINT) Authorities (OVSC1100), and
- (U) USSID SP0018 Training for Analytical Personnel (OVSC1800)

(U) Course [REDACTED] Reporting & Notifications

~~(U//FOUO)~~ This course is reported in the [REDACTED] tool (at "go" [REDACTED]) as OVSC1203.

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

~~TOP SECRET//SI//NOFORN~~**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL****(U) LESSON ONE: FAA Section 702 OVERVIEW**

(U//~~FOUO~~) The FISA Amendments Act (FAA) of 2008 is a law that added Section 702 to FISA (hereafter referred to as FAA Section 702) with a 5-year sunset that expired on December 31, 2012. After briefings to Congress and debate, it was renewed and extended to December 31, 2017. Please keep in mind that the FAA's continued existence depends upon executive, legislative, and judicial approval of NSA's compliant implementation of FAA Section 702. This means that your actions could have an effect on the future of the authority. You need to know how all the pieces of the authority fit together so that you can take full advantage of the collection opportunities generated by the FAA and still meet your responsibilities under relevant law and policies.

(U//~~FOUO~~) In this lesson we will introduce you to the FAA Section 702 authority, detail the various components of this authority, and highlight key concepts associated with this authority. Subsequent lessons will build upon the core concepts presented in this lesson.

(U) By the end of this lesson, you should be able to:

- (U//~~FOUO~~) Identify the target requirements when using the FAA Section 702 authority
- (U) Identify appropriate targets under FAA Section 702
- (U) Summarize the use of AG/DNI Certifications, including component documents for obtaining approval under FAA Section 702
- (U) Identify the [REDACTED] FAA Section 702 Certifications under which NSA operates
- (U//~~FOUO~~) Recall NSA's partnership with the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) as it relates to FAA Section 702
- (U//~~FOUO~~) Identify the [REDACTED] ways in which NSA acquires FAA Section 702 data

(U) WHAT FAA SECTION 702 ALLOWS

(TS//SI//NF) NSA operates under various authorities to acquire foreign intelligence information. FAA Section 702 provides NSA with the means to compel U.S. electronic communications service providers to assist in acquiring foreign intelligence information from communications of non-U.S. persons (non-USPs) reasonably believed to be located outside the U.S. There are three foundational requirements of the authority.

- The target is NOT a U.S. Person (USP).¹
- The target is reasonably believed to be located outside of the U.S.²

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

- The target is expected to possess, receive, and/or is likely to communicate foreign intelligence information³ regarding an approved target set.

¹(U) U.S. Person (USP) is defined as within FISA

- (U) A citizen of the United States (by birth or naturalization);
- (U) An alien lawfully admitted for permanent residence (LPR)** in the U.S., or a "Green Card holder"
- (U) Unincorporated groups and associations, a substantial number of the members of which constitute U.S. citizens or "Green Card" holders; or
- (U) Corporations incorporated in the U.S., but not including entities that are openly acknowledged by a foreign government or foreign faction to be directed and controlled by such a foreign government or foreign faction

***(U) Legal Permanent Residents (LPR) status will be discussed in detail in Lesson 2.*

²(U) Locations designated as "United States"

(U) The United States encompasses all areas under the territorial sovereignty of the U.S., including not only all areas of the 50 states (and the District of Columbia), but also the U.S. territories, including American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Johnson Atoll, Midway Island, Wake Island, Puerto Rico, Swains Island, and the U.S. Virgin Islands of St. Thomas, St. Croix, and St. John. This extends to any U.S. soil, airspace, or territorial waters.



³(U) FISA defines "foreign intelligence information" in Section 101(e). The FISA Definition is:

- (U) "Foreign intelligence information" means –*
- (1) Information that relates to, and if concerning a United States person 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 United States 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.*

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(~~TS//SI//NF~~) Please note that unlike other Sections of FISA, FAA Section 702 does not require that the non-USP targets qualify as foreign powers or agents of a foreign power. FAA Section 702 allows targeting of non-U.S. persons who are expected to possess, receive and/or are likely to communicate foreign intelligence information related to one of the approved Certifications. However, reverse targeting (which will be discussed later in this course) is not allowed.

(U) Examples⁴

^{4(U) Example 1:}

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



^{(U) Example 2:}

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



^{(U) Example 3:}

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



^{(U) Example 4:}

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



^{(U) Example 5:}

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



(U) HOW FAA SECTION 702 IS IMPLEMENTED

(~~TS//SI//NF~~) FAA Section 702 is unique in that  Certifications are used instead of many thousands of target-specific court orders. The U.S. Government issues Directives to compel collection from U.S. providers. A Certification signed by the Attorney General (AG) and the Director of National

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

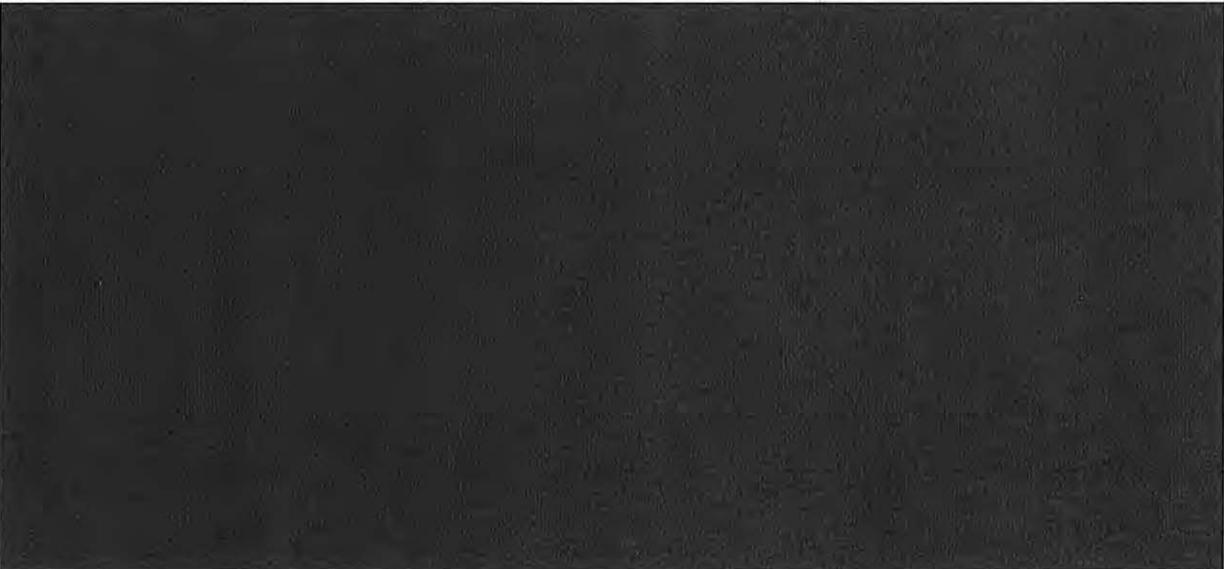
Intelligence (DNI) authorizes the acquisition of foreign intelligence information on an [redacted] by targeting non-USPs reasonably believed to be located outside the U.S. The DNI/AG Certification affirms that NSA has met specific requirements of the law to include the adoption of procedures for targeting non-USPs reasonably believed to be located outside the U.S. and for minimizing the acquisition, retention, and use of any incidentally acquired U.S. person information.

(TS//SI//NOFORN) An FAA Section 702 Certification has historically been approved for one year. The Foreign Intelligence Surveillance Court (FISC) reviews each Certification package, including the Targeting and Minimization Procedures. If the FISC determines that the Government has met the statutory requirements for each Certification and has adequate procedures in place to protect U.S. Person privacy, it issues an order approving the Certification. NSA can then acquire selector specific data associated with a foreign target as needed throughout the approval year with the assistance of electronic communications service providers.

(S//SI//NOFORN) While the FAA Section 702 process enables expeditious targeting of our foreign targets without having to seek individual court orders, there is significant oversight review both internally and also from the Department of Justice (DOJ), the Office of the Director of National Intelligence (ODNI), the FISC, and Congress. For example, DOJ and ODNI currently review all targeting decisions, all disseminations of U.S. person information, and the use of U.S. person identifiers to query FAA Section 702-acquired communications.

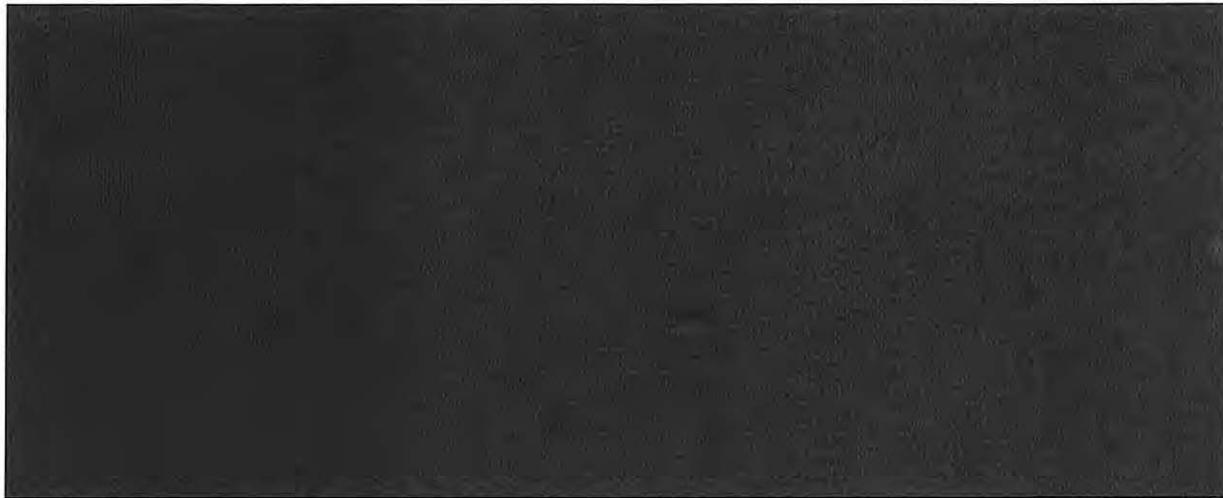
(U) TYPES OF CERTIFICATIONS

(S//SI//NOFORN) NSA currently operates under [redacted] Certifications:

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**



(U) COMPONENT DOCUMENTS

~~(TS//SI//NOFORN~~ Each Certification includes an Affidavit signed by the Director of NSA (DIRNSA) that describes the foreign intelligence to be acquired, including the types of targets that will be pursued. Each Affidavit also identifies the Targeting and Minimization Procedures that will be used, references any applicable data sharing provisions, and summarizes how NSA will acquire data.

~~(TS//SI//NOFORN~~ Each Certification package includes Exhibits specific to each Certification. Here's a brief summary of these exhibits:

- ~~(TS//SI//NOFORN~~ Exhibit A is the NSA FAA Section 702 Targeting Procedures (hereafter "the Targeting Procedures") and includes requirements that apply to the pre- and post-targeting of selectors used by foreign intelligence targets. Exhibit A is currently the same for each FAA Certification, regardless of topic area.
- ~~(TS//SI//NOFORN~~ Exhibit B is the NSA FAA Section 702 Minimization Procedures (hereafter "the Minimization Procedures") and includes the rules for collection, processing, retention, and dissemination of incidentally acquired U.S. person information and domestic communications under this authority. Exhibit B is currently the same for each FAA Certification and at each renewal is traditionally applied retroactively to all data collected under previous FAA Certifications since 2008. **
- ~~(TS//SI//NOFORN~~ Exhibit F (when present) is the Foreign Power Target List that typically identifies ~~██████████~~ about which NSA is seeking to acquire foreign intelligence information.

~~(U//FOUO)~~ **Please Note: While many of the requirements in the FAA Section 702 Minimization Procedures are similar to the requirements in USSID SP0018, the two sets

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

of Minimization Procedures are not synonymous or interchangeable. You must follow the Minimization Procedures that apply to the authority under which you acquired the data.

(U//FOUO) ACQUIRING DATA

(TS//SI//NF) Under FAA Section 702 authority, the AG and the DNI issue Directives to certain U.S. companies that fit the statutory definition of electronic communication service providers compelling them to assist the U.S. Government in its acquisitions of various types of data. Let's first discuss Digital Network Intelligence, or DNI, data.

(TS//SI//NF) There are two ways NSA can obtain DNI data under FAA Section 702:
(b) (3) (A) (also known as DOWNSTREAM) and UPSTREAM. [REDACTED]

(S//SI//NF) ACQUIRING DNI DATA:

(b) (3) (A)

(TS//SI//NF) The first method of obtaining DNI data is commonly referred to as (b) (3) (A) collection, [REDACTED]. We use (b) (3) (A) to obtain communications "to" or "from" a foreign target's electronic communications account [REDACTED]

(TS//SI//NF)



(S//SI//NF) ACQUIRING DNI DATA: UPSTREAM

(TS//SI//NF) The second way to obtain DNI data, specifically DNI surveillance data, is UPSTREAM collection. We use UPSTREAM to obtain communications "to", "from", or "about" a foreign target [REDACTED]



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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

[REDACTED] acquire communications as they transit the Internet backbone. [REDACTED]

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

[REDACTED]

(~~TS//SI//NF~~) WHAT IS AN "ABOUTS" COMMUNICATION IN UPSTREAM?

(~~TS//SI//NF~~) An "abouts" communication is one in which the targeted selector is referenced within a collected communication, but the target is not necessarily a participant in the communication. For example, [REDACTED]

(~~TS//SI//NF~~) "Abouts" collection only occurs when the targeted selector itself specifically [REDACTED]

(~~TS//SI//NF~~) NSA only acquires "abouts" communications through UPSTREAM collection.

[Click here for a comparison of the data acquisition methods under FAA Section 702 \(link to job aid #1\)](#)

(~~S//SI//NF~~) ACQUIRING TELEPHONY DATA

(~~TS//SI//NF~~) We can use FAA Section 702 for Telephony collection using Dialed Number Recognition (DNR) methods. This allows us to obtain communications such as telephone [REDACTED] communications that are "to" or "from" targeted foreign communicants. Like (~~b~~ (3) (A) [REDACTED] and UPSTREAM, we accomplish this collection with the assistance of electronic communications service providers who have been served AG/DNI Directives.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(U//~~FOUO~~) CLASSIFY THE TYPE OF ACQUISITION

(S//~~SI//NF~~) (b) (3) (A) or UPSTREAM?

- a.
- b.
- c.
- d.

(S//~~NF~~) COOPERATING WITH FBI AND CIA

(S//~~SI//NF~~) The FAA Section 702 authority is a joint Intelligence Community (IC) authority used by NSA, the FBI, and the CIA. Although each agency has its own minimization procedures for the proper handling, retention and dissemination of collected FAA Section 702 information, all three agencies must follow the requirements established by NSA's Targeting Procedures in order to target under this authority. [REDACTED]

[REDACTED] All three agencies are subject to rigorous oversight by the DoJ and the ODNI. Specific details about how NSA works with FBI and CIA will be discussed throughout the course in the relevant lessons.

(U) SUMMARY

(U//~~FOUO~~) In this lesson we introduced you to the FAA Section 702 authority, detailed the various components of this authority, and highlighted key concepts associated with this authority.

(U) You should be able to:

- (U//~~FOUO~~) Identify the target requirements when using the FAA Section 702 authority
- (U) Identify appropriate targets under FAA Section 702
- (U) Summarize the use of AG/DNI Certifications, including component documents for obtaining approval under FAA Section 702.
- (U) Identify the [REDACTED] FAA Section 702 Certifications under which NSA operates
- (U//~~FOUO~~) Recall NSA's partnership with the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) as it relates to FAA Section 702
- (U//~~FOUO~~) Identify the [REDACTED] ways in which NSA acquires FAA Section 702 data

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

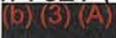
~~TOP SECRET//SI//NOFORN~~

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

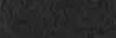
(U//~~FOUO~~) You should now be ready to build upon theses core concepts in the following lessons. To test your understanding, please complete the knowledge checks presented on the next screens.

(U) KNOWLEDGE CHECKS

(TS//SI// Which of the following are target requirements under FAA Section 702? (Check all that apply)

- a. 
- b. 
- c. 
- d. 

(TS//SI//NF) Which of the following would be an appropriate target under FAA Section 702?

- a. 
- b. 
- c. 
- d. 

(TS//SI// Which of the following are the current FAA Section 702 Certifications? (Check all that apply)

- a. 
- b. 
- c. 
- d. 

(TS//SI//NF) How does the use of Certifications under FAA Section 702 differ from other authorities?

- a. 

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

b. (b) (3) (A)

c.

d.

(TS//SI//NF) The Affidavit within each Certification identifies many requirements for proper targeting, collection, and dissemination. Which of the following is NOT included within the Affidavit?

a. (b) (3) (A)

b.

c.

d.

(TS//SI//NF) Which of the following is the FALSE statement about how NSA, FBI, and CIA work together under FAA Section 702?

a. (b) (3) (A)

b.

c.

d.

(TS//SI//NF) Identify the three categories of data NSA collects under FAA Section 702.

a. (b) (3) (A)

b.

c.

d.

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) LESSON TWO: PRE-TARGETING BASICS UNDER FAA Section 702

(S/-) The Targeting Procedures lay out in detail what analysts need to do to properly target and task foreign intelligence targets under FAA Section 702. Of these responsibilities, in this lesson we will focus on applicable research and required documentation prior to targeting under this authority.

(U) By the end of this lesson, you will be able to:

- (U//~~FOUO~~) Identify how one would determine whether a target is appropriate to target or retarget under the FAA Section 702 Targeting Procedures based on the "totality of the circumstances"
- (U) Summarize an analyst's research and documentation responsibilities for "foreignness" and "foreign intelligence purpose"
- (U//~~FOUO~~) Identify the characteristics of the following prohibited or restricted activities: reverse targeting, consensual collection, and [redacted] targeting

(U//~~FOUO~~) IS THE TARGET AND SELECTOR APPROPRIATE TO TASK UNDER FAA SECTION 702?

(TS//SI//) Before a selector¹ may be targeted under FAA Section 702, you must determine if the target¹ is a non-USP who fits within an existing Certification and otherwise meets the "foreignness" test based on the "Totality of Circumstances" (to be discussed further).

¹(U//~~FOUO~~) The word "target" indicates a person or persons against whom NSA seeks to collect information. In the case of FAA 702, [redacted] and must be non-U.S. persons located outside the U.S., and [redacted].

(S//SI//) NSA targets persons by tasking the "selectors" that those persons use to communicate foreign intelligence information. A selector is a specific communications identifier targeted to acquire information that is "to", "from," or "about" a target. Examples of selectors include [redacted]

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(S/ [REDACTED]) Let's start with the foreign intelligence purpose: Does your potential target fit within the terms of one of the Certifications approved by the AG and the DNI? According to the Targeting Procedures, this assessment must be particularized and fact-based, informed by analytic judgment, the specialized training of the analyst, as well as the nature of the foreign intelligence information expected to be obtained.

(S/ [REDACTED]) Remember there are currently [REDACTED] Certifications. Your target must be reasonably believed to possess, expected to receive, and/or likely to communicate foreign intelligence information about [REDACTED]

(S/ [REDACTED]) Although a potential new target does not have to be [REDACTED], you must have an articulable reason why you believe that the new target [REDACTED]
For example, think about how you first identified the new selector:

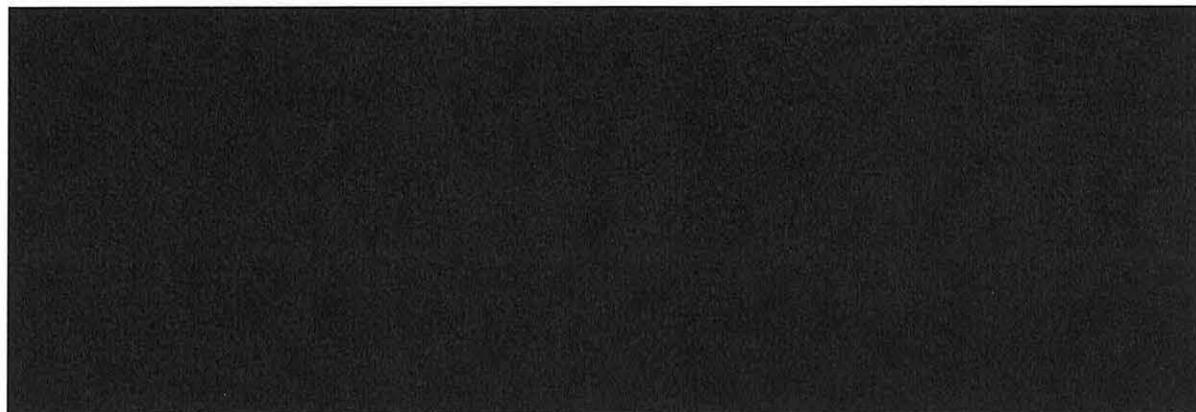
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

(S/ [REDACTED]) While this is not an exhaustive list of ways to connect the target to a certification, there are certain facts that by themselves do not meet the expected foreign intelligence standard and would need additional consultation with relevant Mission Leads, SV, and OGC prior to targeting. For example, further coordination is required if [REDACTED]

(S/ [REDACTED]) Another example where there is not enough information to justify targeting under FAA Section 702 focuses on [REDACTED]

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**



(U) Examples⁵

⁵(U) Example 1:

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

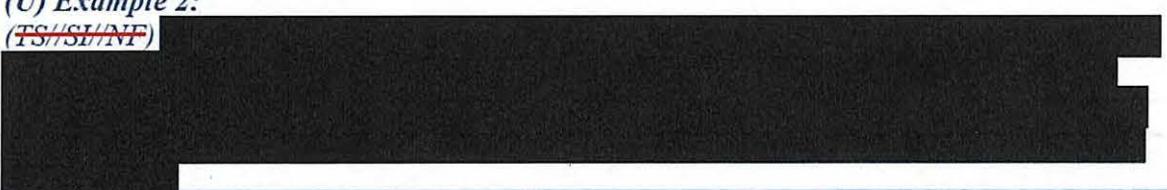


~~(TS//SI//NF)~~



(U) Example 2:

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



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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

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



(U) Example 3:

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



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



(U)



(S//SI//



(U) The "FOREIGNNESS" TEST: NATIONALITY

(S//) Secondly, you must determine if you have enough facts about the person you want to target to meet the requirements for a reasonable belief that the target is a non-USP and is located outside the U.S., which is known as the "foreignness" test. To determine this, you need information regarding the target's nationality and location.

(U) You may not target any USP regardless of the USP's location. There are no exceptions. FISA provides the following categories of individuals defined as USPs:

- (U) A citizen of the United States (by birth or naturalization);
- (U) An alien lawfully admitted for permanent residence in the U.S., or a "Green Card holder;"

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- (U) Unincorporated groups and associations, a substantial number of the members of which constitute U.S. citizens or "Green Card" holders; or
- (U) Corporations incorporated in the U.S., but not including entities that are openly acknowledged by a foreign government or foreign faction to be directed and controlled by such a foreign government or foreign faction

(U//~~FOUO~~) LEGAL PERMANENT RESIDENT (LPR) STATUS

(U)

[REDACTED]

(U//~~FOUO~~)

[REDACTED]

(U//~~FOUO~~)

[REDACTED]

(U//~~FOUO~~)

[REDACTED]

(U)

[REDACTED]

(U) The "FOREIGNNESS" TEST: LOCATION

(U) You may not target a selector if [REDACTED] currently located in the U.S. [REDACTED]. There are no exceptions.

(U) The United States encompasses all areas under the territorial sovereignty of the U.S., including not only all areas of the 50 states (and the District of Columbia), but also

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

the U.S. territories, including American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Johnson Atoll, Midway Island, Wake Island, Puerto Rico, Swains Island, and the U.S. Virgin Islands of St. Thomas, St. Croix, and St. John. This extends to any U.S. soil, airspace, or territorial waters.

(U) [REDACTED]

~~(TS//SI//~~



~~(TS//SI//~~



(U) [REDACTED]

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



⁶~~(TS//SI//NF)~~



(U) TOTALITY OF THE CIRCUMSTANCES

~~(TS//SI//NF)~~ Per the FAA Section 702 Targeting Procedures, NSA will assess the "foreignness" of a target based on the "totality of the circumstances" as a result of diligent research. The Targeting Procedures list examples of valid sources of

~~TOP SECRET//SI//NOFORN~~**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

information, such as lead information, [REDACTED], finished foreign intelligence, and NSA [REDACTED] NSA analysts typically examine three categories of information, as appropriate under the circumstances, to make this foreignness determination:

1. ~~(TS//SI//NF)~~ Lead information [REDACTED]

2. ~~(TS//SI//NF)~~ Research [REDACTED]

[REDACTED] that would provide evidence concerning the target and the target's location

3. ~~(TS//SI//NF)~~ [REDACTED] to determine or verify information about the target and the target's location

~~(TS//SI//NF)~~ As you look at the totality of the information, as appropriate under the circumstances, ask yourself whether you have a reasonable belief that your target is a non-USP located outside the U.S. Do not simply identify the first source of information that would support foreignness (such as [REDACTED])

[REDACTED] and then proceed to target the selector. If you do this, you may be excluding or discounting other information that negates the reasonable belief that the target and all other users of the selector are non-USPs outside the U.S.

~~(TS//SI//NF)~~ What is important is to look at everything reasonably available, so cast your search wide. You should consider a broad base of sources to inform your analytic judgment of the target's location, nationality and any USP status. Your assessment should consider factors appropriate to the characteristics of your target set.

~~(TS//SI//NF)~~ "Totality of the circumstances" does not necessarily mean that if more pieces of information point to one conclusion regarding the foreignness of the target, then that conclusion can form the basis for targeting (or re-targeting). Some information may be weighed more heavily than other information based on, for example, [REDACTED]. If you find conflicting information, you'll need to resolve these conflicts before you can target through further research in the various tools and databases available to you.

~~(S//SI//NF)~~ Remember that certain tools may indicate only the most recent information, while other tools, such as ~~(b) (3) (A)~~ provide a range of information. No tool, however, is an "easy button". It is incumbent upon the analyst to evaluate the information presented to them in the context of their other target knowledge to arrive at a foreignness determination.

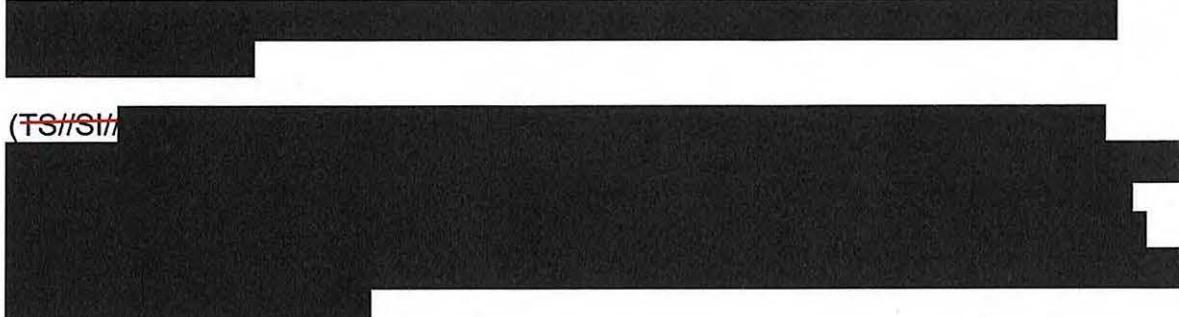
~~(TS//SI//NF)~~ For example, [REDACTED]

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(TS//SI//)



(TS//SI//)



(TS//SI//)



(TS//SI//)



(S//SI//NF)



- (S//SI//NF)
- (S//SI//NF)



(U//FOUO) Always perform your own assessment of the target to make sure it is appropriate for FAA 702 targeting.

(C//) Once you evaluate the totality of the circumstances, you should then use the most recent information to support your documentation in the tasking tool.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(TS//SI//**[REDACTED]**) Do not confuse the evaluation of the totality of the circumstances with the act of documentation in the tasking tool. The former requires you to consider information appropriate under the circumstances; the latter requires you to document the most recent data in the tasking tool.

(U) DOCUMENTING TARGETING DECISIONS

(C//SI//**[REDACTED]**) Once you've established that the target is a non-U.S. person reasonably believed to be outside the United States who possesses, will receive, and/or is likely to communicate foreign intelligence information related to one of the appropriate Certifications, you can begin to target specific selectors.

(TS//SI//NF) The Targeting Procedures require you to document certain facts about your target. NSA's targeting tool for FAA Section 702 is the (b) (3) (A) Tool, or (b) (3) Special fields in (b) allow you to record your assessment of both the foreign intelligence purpose and the foreignness for each targeted selector. You should also be able to identify why you assess that your target uses the selector you want to target.

(U) FOREIGN INTELLIGENCE PURPOSE

(C//SI//**[REDACTED]**) The Targeting Analyst Rationale (TAR) guidance ("go tar") requires a written explanation of what foreign intelligence information NSA expects to receive by targeting an individual. The TAR is recorded in the TAR field in (b) It is important to write a TAR statement that is specific and thorough to fulfill your documentation obligations under the Procedures.

(S//SI//**[REDACTED]**) The essential elements of information needed in the targeting rationale are:

- the target (User)
- link between the user and the selector to be targeted
- foreign intelligence purpose for the targeting and expected foreign intelligence to be gained

(U) Examples⁷

⁷ (U//FOUO) These examples are excerpted from the <go tar> page.

1. (C//SI//**[REDACTED]**) *Needs Improvement:* **[REDACTED]**

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(C//SI//

This is unacceptable because

(C//SI//

Better -

(C//SI//

2. (C//SI//

Needs Improvement:

(C//SI//

This statement does not specify what foreign intelligence information is being sought.

(C//SI//

Better -

(C//SI//

(U) DOCUMENTING FOREIGNNESS

(S//SI// Once you have assessed the totality of circumstances and identified the foreignness of the selector, there are multiple ways to document foreignness within the 702 Authorization block in (b) (3)

(TS//SI//NF) "Foreignness factors" are designed to facilitate that documentation using the most recent foreignness information. Please remember that it is not appropriate to only research what is necessary to fill in the blanks for one of the foreignness factors and then proceed to targeting – that is not what is meant by first evaluating the "totality of the circumstances".

(S//SI// Having done your research, you should select the most appropriate foreignness factor⁸ listed in the (b) (3) field. Examples can also be found on the "FAA 702 Targeting Guidance" link on the "go FAA" page or at "go S2-FAA".

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

⁸ ~~(U//FOUO)~~ Foreignness Factors:

1. ~~(U//FOUO)~~
2. ~~(U//FOUO)~~
3. ~~(U//FOUO)~~
4. ~~(U//FOUO)~~
5. ~~(U//FOUO)~~
U.S.
6. ~~(U//FOUO)~~
7. ~~(U//FOUO)~~
8. ~~(U//FOUO)~~
9. ~~(U//FOUO)~~
10. ~~(U//FOUO)~~
U.S.
11. ~~(S//SI//~~ [REDACTED]
12. ~~(S//SI//~~ [REDACTED]

~~(S//SI//~~ [REDACTED]

(U) MEMORIALIZATION OF FOREIGNNESS

~~(TS//SI//NF~~) Depending on the situation, not all of the information necessary to document foreignness will fit in ~~(b) 1~~. For some selectors, you will need to provide copies of the source material that is used within the 702 Authorization block within ~~(b) 3~~. This may include ~~[REDACTED]~~ or other lead information. NSA refers to the preservation of original source material as foreignness "memorialization." We do this because we may not be able to retrieve the information at a later date, as reports may be cancelled, or ~~[REDACTED]~~. The Targeting Procedures require that NSA be able to provide documentation used in targeting decisions for later review by NSA's external overseers from the DOJ and ODNI.

~~(TS//SI//~~ [REDACTED] REMINDER: You cannot use purged data to support or document a foreignness determination.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

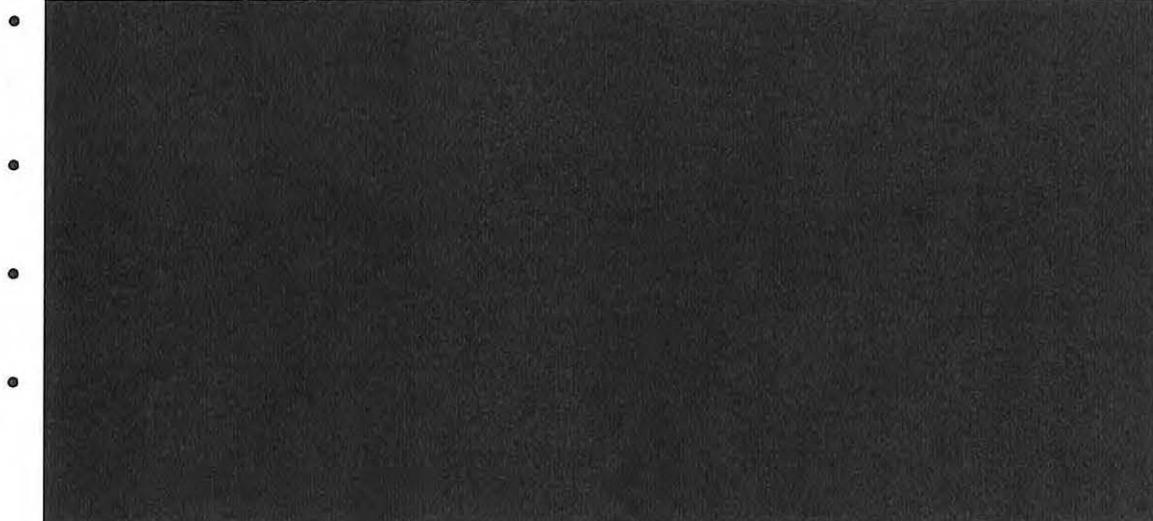


(U) RETARGETING

~~(TS//SI//NF)~~ To re-target a selector following a break in coverage for any reason, you must provide the following:

- a new assessment of foreignness
- a foreign intelligence purpose
- new memorialization/documentation that will be subject to internal and external oversight. (see Compliance Advisory #51 for more information)

~~(TS//SI//NF)~~ It is critical that you address the targeting history of a selector as part of the "totality of the circumstances". Remember, even if this is the first time that YOU are targeting a selector, there may have been previous targeting/detargeting by other targeting analysts. YOU are responsible for making sure that any prior issues are resolved before retargeting. For example:



(U) PROHIBITED ACTIVITIES

(U) ATTORNEY GENERAL GUIDELINES

~~(S//NF)~~ Under FAA Section 702, we may not target a USP or any target located within the U.S. FAA Section 702 and The Attorney General's 2008 "Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

Surveillance Act of 1978, as amended" address four specific statutory prohibitions pertaining to the foreignness of a target:

- ~~(U//FOUO)~~ NSA may not intentionally target any person known at the time of acquisition to be located in the U.S.
- ~~(U//FOUO)~~ NSA may not intentionally target a person reasonably believed to be located outside the U.S. if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the U.S. (a/k/a no "reverse-targeting").
- ~~(U//FOUO)~~ NSA may not intentionally target a U.S. person reasonably believed to be located outside the U.S.
- ~~(U//FOUO)~~ NSA may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the U.S. (a/k/a "domestic communications").

(U) REVERSE TARGETING

~~(TS//SI//NF)~~ **Reverse targeting:** defined as targeting selectors belonging to a foreign target when the primary interest in the foreign target is to acquire the communications of a U.S. person or a person in the U.S. with whom the foreign target is in contact.

~~(S//NF)~~ Reverse targeting can also occur when NSA targets a selector for a valid foreign intelligence purpose, but later determines that the target is not themselves of foreign intelligence interest but is only of interest when communicating with a person in the U.S. or a U.S. person. That selector cannot remain targeted; that would be reverse targeting.

(U) REVERSE TARGETING EXAMPLES

~~(U//FOUO)~~ Here are a few examples of reverse targeting:

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

~~(TS//SI//NF)~~ The answer is "no." Even though [REDACTED], FAA Section 702 prohibits collection of all persons inside the U.S. Targeting [REDACTED] to primarily get information on her would constitute reverse targeting.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(S//SI//NF) Here is another example: You've been appropriately targeting an individual located overseas for a valid foreign intelligence purpose. You later determine that he, himself, no longer provides information of foreign intelligence value. However, someone in the U.S. with whom he communicates does provide foreign intelligence information of interest. Can you continue to collect communications from the first individual to obtain foreign intelligence information from the individual located in the U.S.?

(S//SI//NF) The answer is "no." This would constitute reverse targeting of the individual in the U.S., which is strictly prohibited.

(S//SI//NF) Here is another example: You want to target an extremely violent terrorist located abroad under FAA Section 702. Prior to targeting, you discover that the terrorist is a U.S. person, but [REDACTED]

(S//SI//NF) The answer is "no" because of the terrorist's USP status. Although [REDACTED] will provide foreign intelligence information on the terrorist operations, the primary purpose of the targeting would be to obtain the communications of the U.S. person terrorist, and thus, would constitute reverse targeting.

(S//SI//NF) In this case, to collect this foreign intelligence, you would need to exercise other FISA authorities against the USP terrorist. If you are unclear whether the primary purpose of a targeting is to obtain communications regarding a U.S. person, you should consult with compliance personnel or OGC prior to targeting.

(U//FOUO) Reverse Targeting and Roamers

(S//SI//NF) Under FAA Section 702, it is appropriate to task non-USP persons who are reasonably believed to be overseas [REDACTED]

[REDACTED] However, you must be extra vigilant in following the location of your primary target and detask in the event that the primary target is about to enter the United States. For example:

(S//SI//NF) [REDACTED]

[REDACTED] All selectors used by Target X must be detasked while he is in the U.S. [REDACTED]

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

Target

X's presence in the U.S. prohibits continuing to target him.

(U) CONSENSUAL COLLECTION

(~~TS//SI//NF~~) Consensual Collection is a procedure whereby a U.S. person may authorize collection of his or her own communications for any technical or foreign intelligence purpose. Consent does not apply to FAA Section 702. Under FAA Section 702, we may not target, under any circumstances, ANY person who is considered either a U.S. person or a person in the U.S. – even if the person signed a consent form.

(U) RESTRICTED ACTIVITY: [REDACTED] POLICY CONSIDERATIONS

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

(U) Additional guidance for [REDACTED]

⁹ (~~TS//SI//NF~~) [REDACTED]

(U//~~FOUO~~) WORKING WITH CIA and FBI

(U//~~FOUO~~) The following are key points to remember when working with CIA and FBI during targeting:

- (~~S//SI//NF~~) NSA is responsible for all targeting and all targeting follows NSA's Targeting Procedures.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

- ~~(S//SI//NF)~~ In addition, the FBI is the implementing agency and has its own additional Targeting Procedures [REDACTED].
- ~~(S//SI//NF)~~ Both the CIA and the FBI may nominate specific selectors to NSA for targeting under the rules of NSA's Targeting Procedures for FAA Section 702.
- ~~(S//SI//NF)~~ The FBI and the CIA may receive unminimized and unevaluated data from those nominated selectors, [REDACTED]

(U) SUMMARY

~~(S/~~ [REDACTED] In this lesson we focused on applicable research and required documentation prior to targeting under this authority. These activities are grounded in the Targeting Procedures that lay out in detail what analysts need to do to properly target and task foreign intelligence targets under FAA Section 702.

(U) You should now be able to:

- ~~(U//FOUO)~~ Identify how one would determine whether a target is appropriate to target or retarget under the FAA Section 702 Targeting Procedures based on the "totality of the circumstances"
- (U) Summarize an analyst's research and documentation responsibilities for "foreignness" and "foreign intelligence purpose"
- ~~(U//FOUO)~~ Identify the characteristics of the following prohibited or restricted activities: reverse targeting, consensual collection, and [REDACTED]

(U) KNOWLEDGE CHECKS

~~(U//FOUO)~~ Before you target a selector, what are all of the criteria you must evaluate to determine if it is an appropriate target under FAA Section 702?

- a. ~~(b) (3) (A)~~
- b.
- c.
- d.

~~(S//SI/~~ [REDACTED] Which pieces of information should be included in the TAR statement? (Check all that apply)

- a. ~~(b) (3) (A)~~
- b.

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- c. (b) (3) (A)
d.

(S//REDACTED) What information should you provide in REDACTED to document foreignness?

- a. (b) (3) (A)
b.
c.
d.

(TS//SI//REDACTED) If you find conflicting information about the foreignness of your selector, based on the concept of "totality of circumstances", what should you do?

- a. (b) (3) (A)
b.
c.
d.

(S//SI//NF) A U.S. person has signed a consent form to authorize the collection of his or her communications for any technical or foreign intelligence purpose. Under FAA Section 702, may we target this person?

- a. (b) (3) (A)
b.
c.
d.

(TS//SI//NF) You've targeted Selector A, which is associated with a user who is a non-USP located overseas based on a reasonable belief that collection would yield significant foreign intelligence. Over the months, the user's communications have not yielded significant foreign intelligence. However, particular communications between this person and a USP who is also located overseas have become a source of significant foreign intelligence. Under FAA Section 702, can you continue to target your original user's communications to collect information from the USP?

- a. (b) (3) (A)
b.
c.
d.

~~TOP SECRET//SI//NOFORN~~**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL****(U) LESSON THREE: POST TARGETING**

~~(S//SI//NF)~~ The NSA FAA Section 702 Targeting Procedures require that you perform certain pre-targeting checks before any targeting and collection can occur. The Targeting Procedures also require post-targeting checks on a regular and ongoing basis. In this lesson, we'll detail your responsibilities regarding Post Targeting Checks as well as circumstances that require timely and accurate detargeting of selectors.

~~(U//FOUO)~~ At the end of this lesson, you will be able to:

- Identify the required activities that pertain to your "obligation to review" or "OTR" responsibilities
- Differentiate between foreign and domestic communications
- Identify the factors involved in data retention decisions
- Compare the ~~(b) (3) (A)~~ with ~~(b) (3) (A)~~ post-targeting checks
- Identify your responsibilities in resolving an alert
- Identify your responsibilities under a "change in status" situation
- Identify situations when de-targeting a selector is required
- Identify the requirements for retargeting a selector

(U) POST TARGETING RESPONSIBILITIES

~~(S//SI//NF)~~ Remember how you made your pre-targeting decisions based on the totality of the circumstances? The same is true for continued post-targeting assessments.

~~(S//SI//NF)~~ Post-targeting information may come from collected FAA Section 702 data, other SIGINT collection, open source, or lead information, such as tips or reporting from other agencies. Consider any new information as you receive it that may relate to the physical location or U.S. person status ~~of a targeted selector, as well as the foreign intelligence purpose for targeting. You need to maintain a reasonable belief that the intended target~~ ~~remain appropriate to target.~~

~~(S//SI//NF)~~ Remember that renewing a selector in ~~(b)~~ (required at least annually for all selectors per ~~(b)~~ policy) is a reassertion of NSA's reasonable belief of foreignness and on-going foreign intelligence purpose. Ultimately, NSA will be required to account for its actions including the timeliness and accuracy of any required detargeting decisions. Therefore, it's important to take your post targeting responsibilities seriously and to act quickly when there's a question about whether a selector should remain targeted.

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) POST TARGETING OBLIGATION TO REVIEW

(S//SI//NF) As an analyst, you have primary responsibility for reviewing collected data for both operational and compliance reasons. This "Obligation to Review" (OTR) means that you must regularly review collected traffic, [REDACTED] to ensure that NSA still maintains a reasonable belief that:

- **(S//NF)** The intended target [REDACTED]
- **(S//NF)** [REDACTED] believed to be located outside the U.S.; and
- **(S//NF)** There is a valid foreign intelligence purpose for targeting the selector under one of the FAA Section 702 Certifications.

(S//SI//NF) It is important to consider that users of targeted selectors may roam to the U.S.; [REDACTED] a new or previously unknown U.S. person status; they may stop using a targeted selector; or they may cease to be of foreign intelligence interest. It's also possible that [REDACTED]

(S//SI//NF) Therefore, during the content review, NSA expects you to catch references to the user's current location and promptly identify and research facts that may indicate previously unknown status as a U.S. person or user in the U.S. [REDACTED]

(S//SI//NF)

[REDACTED] If you have any questions, please immediately consult compliance and OGC personnel.

(S//SI//NF) While targeting offices have some flexibility in how often OTR activities must take place, based on mission priorities and knowledge about the specific target set, NSA requires that analysts regularly review enough target traffic to verify that targeting remains appropriate to that authority. Please remember that new facts may arise that require more frequent review (such as an indication of future planned travel or [REDACTED]).

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U//~~FOUO~~) HOW DOES "REASONABLE BELIEF" APPLY TO POST-TARGETING REVIEW?

(S//SI/ [REDACTED] The Targeting Procedures require an ongoing examination of facts to determine whether your reasonable belief assessment of a target's foreignness is still valid. If [REDACTED]
[REDACTED] then you must immediately detarget. If [REDACTED]
[REDACTED] then retargeting is possible.

(S//SI/ [REDACTED]

(U) Examples¹

¹(U) Example 1:

(S//SI/ [REDACTED]

(U) Example 2:

(S//SI/ [REDACTED]

(U) Example 3:

(S//SI/ [REDACTED]

(U) Example 4:

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(S//SI/[REDACTED]

(U) Example 5:

(S//SI/[REDACTED]

(U) Information that may indicate presence in the U.S. or U.S. person status²

²(U) *This is not an all-inclusive list!!!!*

[REDACTED]

(U) CRITERIA FOR PROCESSING AND RETENTION

(S//SI/[REDACTED] According to the FAA 702 Minimization Procedures, you are not required to review every collected communication. However, you must review enough communications to ensure that NSA is not intentionally collecting on targets that are not eligible for targeting under FAA Section 702. [REDACTED]

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(S//SI//NF) As you review any collected communication, you need to determine whether or not NSA is authorized to retain the communication for further processing or later dissemination. According to the FAA Section 702 Minimization Procedures, you must determine three things when making your decision about retention:

1. (S//SI//NF) Is the communication a "foreign communication" or a "domestic communication?"
2. (S//SI//NF) Is it "to", "from," or "about" the target?
3. (S//SI//NF) Does the communication contain U.S. person information?

(S//SI//NF) Let's take a closer look at each criterion, starting with foreign communication vs. domestic communication.

(U) DETERMINATION #1: FOREIGN VS. DOMESTIC COMMUNICATIONS

(S//SI//NF) The FAA Section 702 Minimization Procedures define a "foreign communication" as a communication that has at least one communicant outside of the U.S.; anything else is a "domestic communication." Domestic communications include any communication in which the sender and all intended recipients are reasonably believed to be located in the U.S. at the time NSA acquires the communication.

(S//SI//NF) NSA is not authorized to intentionally acquire domestic communications. If NSA incidentally collects a domestic communication, the communication must be promptly destroyed unless DIRNSA specifically determines, in writing and on a communication-by-communication basis, that the target was properly targeted (i.e., was there a reasonable but mistaken belief concerning the target's location and USP status) and the communication: 1) is reasonably believed to contain significant foreign intelligence information; 2) contains evidence of a crime; 3) contains information for cryptanalytic, traffic analytic, or signal exploitation purposes or is necessary to understand or assess a communications security vulnerability; or 4) contains information pertaining to an imminent threat of serious harm to life or property.

(U) Examples of foreign or domestic communications³

³(U) Example 1:

(S//SI//NF)

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(U//FOUO) [REDACTED]

(U) Example 2:

(S//SI//NF) [REDACTED]

(S//SI//NF) [REDACTED]

(U) Example 3:

(S//SI//NF) [REDACTED]

(S//SI//NF) [REDACTED]

(U) DETERMINATION #2: "TO", "FROM", or "ABOUT" THE TARGET

(TS//SI//NF) Even if you've determined that your communication is a foreign communication, you also need to determine whether it is "to", "from", or "about" the target. You need to verify that you are still collecting on the target that you intended to target. NSA should destroy communications that are not to, from, or about the target. Additionally, you must also consider whether the collection of communications that are not to, from, or about the target may be indicative that the target no longer uses the tasked selector.

(U) DETERMINATION #3: DOES THE COMMUNICATION CONTAIN U.S. PERSON INFORMATION?

(S//SI//NF) According to Section 3(b)(1) of the Minimization Procedures, if the communication is of or concerning any USP, you must destroy the communication at the earliest practicable point at which such communication can be identified as either: clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated. We will discuss evidence of a crime later.

(U) Examples of appropriate foreign intelligence information⁴

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

⁴(S//SI//NF)



(S//SI//NF) Here's another example.



(S//SI//NF)



(S//SI//)



(U) If there is U.S. Person Information:

(S//SI//NF)



(C//SI//)

CHECKS: (b) (3) (A)

(S//SI//NF) NSA's Targeting Procedures require post-targeting [] checks [] to look for indications that the intended target or any user of a targeted selector has entered the U.S.



⁵(U//FOUO)



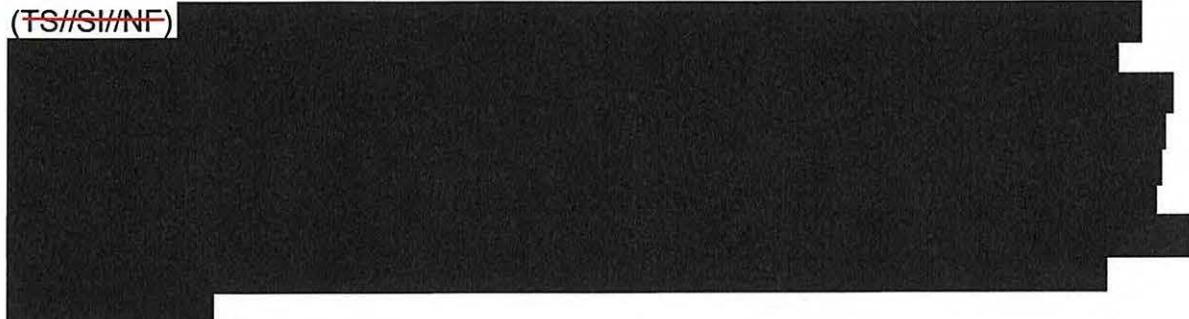
(TS//SI//NF)



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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

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



⁶(U)  Examples:

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



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



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



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



(~~TS//SI//~~) The FISA Court has previously advised that it considers even a one-day delay between when NSA makes a determination that detargeting is

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

needed and the date NSA actually detargets the account (and alternates as required) to be a detargeting delay, and thus a compliance incident. That means that the detargeting action must take place within the same duty day (or shift) as the decision is made. It is a myth that NSA has "24 hours" to act once a detargeting decision has been made. We will discuss "detargeting" later in this lesson.

~~(S//SI//~~CHECKS: ~~(b) (3) (A)~~

~~(TS//SI//~~ The ~~(b) (3) (A)~~ tool is a ~~check~~ that "alerts" SV of any targeted FAA Section 702 selector when it appears that ~~██████████~~ inside the U.S. This might be an indication that a user is located inside the U.S. or it might not; therefore in the case of notifications, NSA has the opportunity to research first -- before detargeting -- to see if the Alert really indicates that a user is in the U.S.

~~(TS//SI//~~ While research is permitted when reviewing an Alert, NSA must promptly detarget the selector as soon as:

- ~~██████████~~
- ~~██████████~~

~~(TS//SI//~~ As with ~~████~~ roammers, the FISA Court has previously advised that it considers even a one-day delay between when NSA makes a determination based on an Alert that detargeting is needed and the date NSA actually detargets the account (and alternates as required) to be a detargeting delay, and thus a compliance incident. That means that the detargeting action must take place within the same duty day (or shift) as the decision is made. It is a myth that NSA has "24 hours" to act once a detargeting decision has been made.

(U) RESOLVING AN ALERT

~~(TS//SI//~~ SV receives the ~~████~~ Alert in ~~(b) (3) (A)~~ and performs preliminary research to help determine whether the Alert is truly indicative of a user's location in the U.S. or is a false positive.

~~(TS//SI//~~

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

selector. NSA made a commitment to our overseers and the Court to promptly resolve alerts. Therefore, the targeting analyst must immediately begin research and diligently respond to any request for information from SV. In no case may an Alert be left unresolved for more than [REDACTED] business days.

(U) Analyst responsibilities:

(~~TS//SI//NF~~) To resolve an Alert, the analyst must promptly review all of the following:

- [REDACTED]
- [REDACTED]
- [REDACTED]

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

(U//FOUO) RESOLVING AN ALERT: CONFIRMED ROAMER

(~~TS//SI//NF~~) If the target [REDACTED] is identified as being in the U.S., then you must immediately detarget any selector to which that user has access and work with SV on a "confirmed roamer" incident report (more details later).

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

(U//FOUO) Please note that an extremely limited exception to the need to immediately detask certain FAA Section 702-tasked selectors was included in the USA Freedom Act that was enacted in June 2015. If DIRNSA determines that a lapse in targeting a non-U.S. person who has roamed in the U.S. poses a threat of death or serious bodily harm, the selector may be kept on task for up to 72 hours to ensure no gap in coverage will occur while and until an emergency Title I FISA authorization is being obtained. If you believe you have encountered such an emergency situation, you should contact SV and OGC immediately.

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) RESOLVING AN ALERT: ADDITIONAL [REDACTED] REVIEW

(~~TS//SI//NF~~) Alternatively, while researching an Alert, the analyst may find information that indicates the intended target remains outside of the U.S. and the information [REDACTED]

[REDACTED] Additional [REDACTED] research may be required to resolve such an Alert. In that case, consult with SV who will coordinate such research to determine [REDACTED]

[REDACTED]

(S// [REDACTED] RESOLVING AN ALERT: [REDACTED]

(~~TS//SI//NF~~) Finally, there are situations where [REDACTED]

[REDACTED]

[REDACTED]

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

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

(U) [REDACTED]

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- ~~(S//SI//NF)~~ [REDACTED]

- ~~(S//SI//NF)~~ [REDACTED]

(U) [REDACTED]

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

(U) CHANGE IN STATUS OF A TARGETED SELECTOR

~~(S//SI//NF)~~ What if you collect a foreign communication only to find out that the target [REDACTED] is actually a U.S. person or a person in the U.S.? The FAA Section 702 Minimization Procedures describe these situations as a "change in status" that require you to treat a communication or possibly multiple communications as if they were domestic communications.

~~(S//SI//NF)~~ Specifically, if you validly target a selector and, after targeting has begun, you determine that a U.S. person or a person inside the U.S. is using the selector, [REDACTED] then you must immediately emergency detarget the selector. This is to avoid intentionally targeting a U.S. person or a person in the U.S.

~~(S//SI//NF)~~ Under the Minimization Procedures, you must treat any communication acquired while any user of the targeted selector was in the U.S. or after a user is discovered to have U.S. person status as a domestic communication, subject to purge requirements, with limited exceptions, which we'll discuss later in this course.

TOP SECRET//SI//NOFORN

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) CHANGE IN STATUS EXAMPLE 1:

(S//SI// [REDACTED]

(S//SI// [REDACTED] The intended target is a non-USP located overseas.

Because [REDACTED]

[REDACTED] there has been a "change in status" [REDACTED] and you cannot continue to target this selector. You must terminate further acquisition of this selector [REDACTED] without delay and NSA must purge (with limited exceptions) any collected communications in which a U.S. person is using the targeted selector.

(U) CHANGE IN STATUS EXAMPLE 2:

(S//SI// [REDACTED]

If, alternatively, you discover after targeting that the intended target [REDACTED]

[REDACTED] You would have to purge (with limited exceptions) any other FAA Section 702 collected data from those other selectors.

(U) CHANGE IN STATUS EXAMPLE 3:

(S//SI// [REDACTED] Besides a change in U.S. person status, you may also encounter a change in the target's physical location, for example:

(S//SI// [REDACTED] You've tasked [REDACTED]. When reviewing a communication, you realize that the target was in the U.S. [REDACTED] What should you do?

(S//SI// [REDACTED] Due to this change in status of the user of the targeted selector, you need to immediately emergency detarget [REDACTED] and any other targeted selectors while the target is in the U.S. NSA must also purge (with limited

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

exceptions) any communications collected from any FAA Section 702 selectors tasked for the target while the target was in the U.S.

(U) CHANGE IN STATUS EXAMPLE 4:

(S//SI//
[REDACTED]

What about this example? [REDACTED]
[REDACTED]

[REDACTED]
What should you do?

(S//SI//
[REDACTED]

You have to immediately emergency detarget [REDACTED] because you no longer have a reasonable belief that the user of that selector is outside the U.S. You had a reasonable belief at the time of targeting that the user was overseas;

[REDACTED]. Additional information reveals that either your reasonable belief at the time of targeting was mistaken or the target's location has changed.

(S//SI//
[REDACTED]

What about purge? [REDACTED]
[REDACTED]

[REDACTED]
all collected communications will need to be purged (with limited exceptions).

(U) PLANNED TRAVEL VS. CHANGES IN STATUS

(S//SI//NF)
[REDACTED]

[REDACTED]
if you know in advance that a user plans to travel to the U.S. but you don't identify and detarget all of the user's selectors prior to the travel, it will result in a compliance incident. More on that in a later lesson.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(S//SI//NF) Here's an example:

What should you do?

(S//SI//

You must detarget this selector and any other selectors prior to his travel to the U.S.

So, if you know in advance that a user plans to travel to the U.S. but you don't identify and detarget all of the user's selectors prior to the travel, it will result in a compliance incident.

(U) SPECIAL CASES: ATTORNEY-CLIENT PRIVILEGE/EVIDENCE OF CRIME

(S//NF) There are some special cases that you should be aware of when handling FAA Section 702 communications. These include communications between an individual and his or her attorney (or any person who, based on the information in the communication, appears to be communicating on behalf of an attorney, such as a paralegal or administrative assistant), and communications that reveal evidence of a crime.

(S//NF) Attorney-client communications require special handling under NSA's Minimization Procedures because generally what a person tells his or her attorney and vice versa cannot be used against that person in a court. Therefore, NSA must take into account the U.S. Government's need to prosecute certain individuals who violate U.S. law.

(S//NF) The rule is straightforward: if you discover any FAA Section 702 communications that appear to be between a client and his or her attorney, whether the attorney appears to be a U.S. attorney or a non-U.S. attorney, bring it to the NSA's OGC for immediate attention; OGC will provide you with further instructions.

(U) ATTORNEY CLIENT PRIVILEGE REVIEW REQUIREMENT HAS CHANGED IN THE 2015 MINIMIZATION PROCEDURES!

(S//NF) In the past, NSA

(S//NF) NSA's 2015 Minimization Procedures now require

NSA must, upon recognition, evaluate unminimized communications

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

between [REDACTED]

[REDACTED] NSA may still be able to report the communications, but because of the complexity of this issue, **it is essential that you alert OGC immediately to any 702 collection involving an attorney or attorney representative.**

(S//SI// [REDACTED]) The same holds true for any FAA Section 702 communication that reveals criminal activities or evidence of a crime. If, during the course of collection, you come across information indicating criminal activity or that reveals evidence of crime, consult with OGC immediately.

(U) DETARGETING

(S//SI// [REDACTED] If you have information indicating that any user of an FAA Section 702 targeted selector is a U.S. Person and/or is located in the U.S. then you must immediately emergency detarget any and all selectors to which that user has access. (b) [REDACTED] is the targeting/detargeting system for FAA Section 702. (3)

(S//SI// [REDACTED] Analysts are responsible for ensuring that detargeting actions complete in (b) [REDACTED]. This includes ensuring that any pending targeting records are stopped if the target becomes inappropriate to target and ensuring that [REDACTED] detargeting requests complete in (b) [REDACTED]. **Going through (b) (3) (A) [REDACTED] or any other database in lieu of working directly in (b) [REDACTED] is not an excuse for not verifying that a selector has been detargeted in (b) [REDACTED] (3)**

(S//SI// [REDACTED]) DETARGETING REASONS in (b) (3)

(S//SI// [REDACTED]) You must use the correct "detask reason" and priority in your (b) [REDACTED] detasking record to ensure that all FAA Section 702 targeting and collection will cease either immediately (in the case of a user in the U.S. or a user who is a USP) or in the case of planned travel, before the user enters the U.S. [REDACTED]

(S//SI// [REDACTED]

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- [REDACTED]
- [REDACTED]
- [REDACTED]

(S//
[REDACTED])

(S//
[REDACTED]) A [REDACTED]
[REDACTED]

(S//
[REDACTED])

- [REDACTED]

(S//
[REDACTED])

(S// [REDACTED] Detargetings for compliance reasons (related to U.S. persons or persons in the U.S. or coming to the U.S.) should be detargeted at EMERGENCY priority to ensure prompt detargeting.

(U) COMMON ERRORS

(U//~~FOUO~~) Please remember: If you fail to use the correct detask reason, the correct priority, or make any other error in detargeting in (b) [REDACTED] that fails to stop unauthorized targeting and collection, NSA will have to report it as a compliance incident.

(S//~~SI//NF~~) If you choose the wrong detask reason or priority for example, using [REDACTED] then NSA may incur a delayed detargeting compliance incident which will be reported to the FISA Court and Congress. **The following are examples of what NOT to do:**

- (S//
[REDACTED])

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- (S//SI// [REDACTED]

- (S//SI// [REDACTED]) [REDACTED]

(U//FOUO) Lastly, it cannot be repeated enough, that failure to promptly and completely identify and detarget all known selectors once you have determined that the target or any other user is in the U.S. or is a U.S. person will result in a compliance incident. Such detargeting must take place within the same duty day (or shift) as the decision is made.

(U) Examples⁷

⁷(S//SI// [REDACTED]

What should you do?

(S//SI// [REDACTED]

(S// [REDACTED]

(S//NF) [REDACTED]

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

If you suspect that a user of any targeted selector may have a change in status that would invalidate continued targeting, it's critical that you act quickly.

(U) RETARGETING

(S//SI//**[REDACTED]**) If NSA has detargeted a selector either because a user has roamed to the U.S. **[REDACTED]** you won't be able to retarget those selectors under FAA Section 702 unless and until you can re-establish a reasonable belief (with new documentation) that **[REDACTED]**

[REDACTED] There's no cooling off period after which you can presume the user is likely to have left the U.S. Instead, you must rely on the totality of the information available after the detargeting to re-establish reasonable belief that a U.S. person or a person in the U.S. is not using the selector.

(U) SUMMARY

(S//SI//**[REDACTED]**) In this lesson, we detailed your responsibilities regarding Post Targeting Checks as well as circumstances that require timely and accurate detargeting of selectors.

(U//FOUO) You should be able to:

- Identify the required activities that pertain to your "obligation to review" or "OTR" responsibilities
- Differentiate between foreign and domestic communications
- Identify the factors involved in data retention decisions
- Compare the (b) (3) (A) **[REDACTED]** with (b) (3) (A) **[REDACTED]**
- Identify your responsibilities in resolving an alert
- Identify your responsibilities under a "change in status" situation
- Identify situations when de-targeting a selector is required
- Identify the requirements for retargeting a selector

(U) KNOWLEDGE CHECKS

(S//SI//**[REDACTED]**) Which of the following is **NOT** one of your responsibilities with regard to your "obligation to review" (OTR)?

- a. (b) (3) (A) **[REDACTED]**
- b. **[REDACTED]**
- c. **[REDACTED]**

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

d. [REDACTED]

(S//SI//NF) Which of the following is NOT an example of a foreign communication?

- a. [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

(S//SI//NF) What are factors to consider when making the determination to retain data collected under FAA Section 702? (Check all that apply)

- a. (b) (3) (A) [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

(TS//SI//NF) Which type of post-tasking [REDACTED] check contains definitive information about a selector's U.S. location for which you must immediately identify and detarget alternate selectors?

- a. (b) (3) (A) [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

(TS//SI//NF) [REDACTED] Which of following is NOT one of your responsibilities in resolving a post-tasking [REDACTED] notification?

- a. (b) (3) (A) [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

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

TOP SECRET//SI//NOFORN

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(S//SI// You validly target a selector and, after targeting has begun, you determine that a U.S. person or a user in the U.S. is using the selector, what do you do?

- a. (b) (3) (A)
 - b.
 - c.
 - d.
- 

(S//SI//) In which situation is it appropriate to continue targeting a selector?

- a. (b) (3) (A)
 - b.
 - c.
 - d.
- 

(S//SI//) Which of the following actions must happen before you are able to retarget a selector that roamed under FAA Section 702?

- a. (b) (3) (A)
 - b.
 - c.
 - d.
- 

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) LESSON FOUR:

In this lesson, we'll discuss some specific issues related to (b)(3)(A) collection, including the difference between [REDACTED] and [REDACTED] [REDACTED] and the rules for querying collected FAA Section 702 data using USP identifiers.

(U) By the end of this lesson, you should be able to:

- (U//~~FOUO~~) Describe the characteristics of (b)(3)(A) collection
- (U//~~FOUO~~) Distinguish between [REDACTED] and [REDACTED]
- (U//~~FOUO~~) Apply the Targeting and Minimization Procedures to the retention of [REDACTED]
- (U//~~FOUO~~) Identify the rules for conducting U.S. Person queries in collected data
- (U//~~FOUO~~) Identify the procedures for dealing with [REDACTED]"

(U) (b)(3)(A)

(U//~~FOUO~~) Let's do a quick recap. With (b)(3)(A) we can:

- (~~TS//SI//NF~~) Acquire communications that are "to" and "from" the targeted selector [REDACTED]

(S//SI//NF) IDENTIFYING (b)(3)(A) DATA FROM UPSTREAM DATA

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(TS//SI//NF) NSA applies different (b) (3) (A) data and UPSTREAM data. [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

(TS//SI//NF) You can also distinguish FAA 702 collection by [REDACTED]

[REDACTED]

[REDACTED]

~~(S)~~ SURVEILLANCE [REDACTED] DATA

(S//CI//NF) NSA's FAA Section 702 Minimization Procedures apply to [REDACTED] surveillance data [REDACTED]. The Minimization Procedures do not require that you review every collected communication. As you review collected data, however, you need to make decisions about continued targeting, processing, retention, and dissemination. Whether or not you can continue with any of those activities depends on whether a communication was legally acquired or not.

(TS//SI//NF) To help you make this determination you need to know a few things related to any specific communication:

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. Was the intended target [REDACTED] in the U.S. at the time NSA acquired the communication.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(U) We discussed point #1 previously. Let's discuss points #2 and #3.

(U)

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

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

(~~TS//SI//NF~~) What about point #4: the location of the user [REDACTED] of the targeted selector at the time of acquisition?

- (~~TS//SI//NF~~) [REDACTED] targeting must cease if the intended target [REDACTED] of the targeted selector is in the U.S. at the date/time of acquisition. It is not legal for NSA to collect or continue to collect such communications.
- (~~TS//SI//NF~~) [REDACTED]

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

(U) Examples²

²(~~TS//SI//NF~~)

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

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

Are you allowed to retain/report from these communications?

(~~TS//SI//NF~~) Yes, you can keep and report on any of the foreign communications [REDACTED] Any domestic communications contained [REDACTED] must be handled in accordance with the minimization procedures.

(U) GENERAL QUERY GUIDELINES

(S//SI//~~FOUO~~) When querying collected FAA Section 702 data, as with any of NSA's authorities, whether you are using U.S. identifiers or not, you must design your query to return foreign intelligence. To appropriately query and avoid an overly broad query, follow these guidelines:

- Focus on the foreign intelligence and articulate the foreign intelligence justification
- Be as specific as possible
- Do pre-query foreignness checks
- Be aware of [REDACTED] and be prepared to make adjustments (query rules are different under different authorities)
- Use (b) (3) and (b) (3) (A) to distinguish authorities as necessary
- Use appropriate (b) (3) (A) logic and/or defeats
- (U//~~FOUO~~) [REDACTED]
- (U) Combine multiple associated general search terms to narrow the query to the greatest extent possible

(U) QUERYING USING U.S. PERSON IDENTIFIERS

(U//~~FOUO~~) Now let's turn our attention to U.S. Person Identifiers.

(S//SI//~~NF~~) U.S person identifiers include but are not limited to [REDACTED]

(~~TS//SI//NF~~) The FAA Section 702 Minimization Procedures (specifically Section 3(b)(5)) allow us to query certain collected FAA 702 data using U.S. person identifiers as query terms. The querying of FAA Section 702 data using U.S. person identifiers has received intense scrutiny, and we must give great care to how we run these queries.

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(S//SI//) QUERYING METADATA AND CONTENT DATABASES USING U.S. PERSON IDENTIFIERS

(S//SI//NF) When using USP identifiers to query already collected FAA Section 702 communications metadata and content data, NSA follows special implementation procedures designed to enable the internal and external oversight that is required in Section 3(b)(5) of the Minimization Procedures. The implementation procedures are available on the "go FAA page". Rules for Querying USP identifiers for metadata and content:

- (~~TS//SI//NF~~) Only run U.S. person queries against  and Telephony data. **The minimization procedures prohibit querying collected FAA Section 702 UPSTREAM data using U.S. person identifiers.** This restriction is in place because queries in UPSTREAM data may return results that do not contain the targeted selector. (We'll discuss UPSTREAM in the next lesson)
- (~~TS//SI//NF~~) When composing and executing your query, be sure to check your default data sets and use  as needed to prevent querying any UPSTREAM data (Refer to the "go FAA" page for instructions)
- (~~TS//SI//NF~~) 
- (~~S//SI//NF~~) Design and document all database queries to be reasonably likely to return foreign intelligence information, as defined in FISA.

(~~TS//SI//NF~~) NSA makes all U.S. person communications metadata queries and all pre-approved U.S. person content query terms, as well as the articulated foreign intelligence purpose for each such query or term, available to DOJ and ODNI as part of their bi-monthly oversight reviews.



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



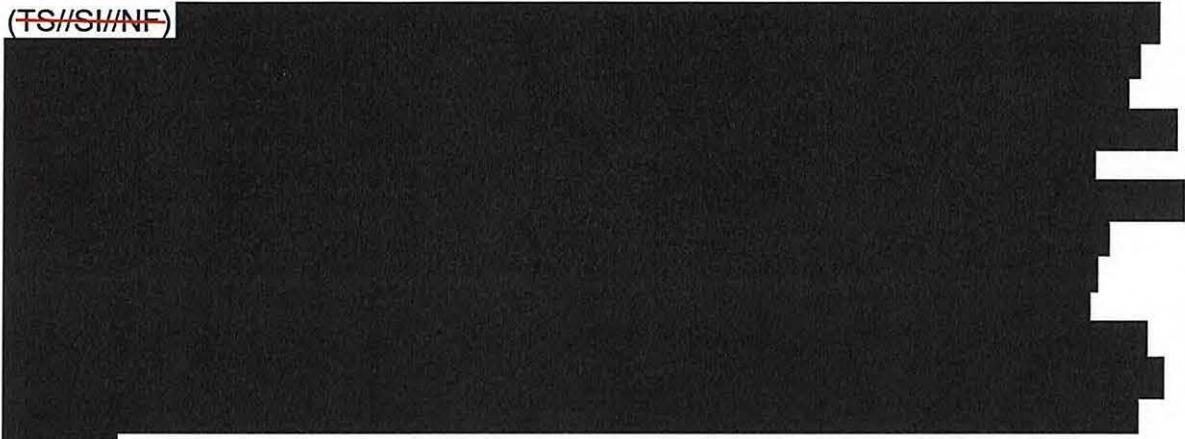
~~TOP SECRET//SI//NOFORN~~

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(TS//SI//NF)

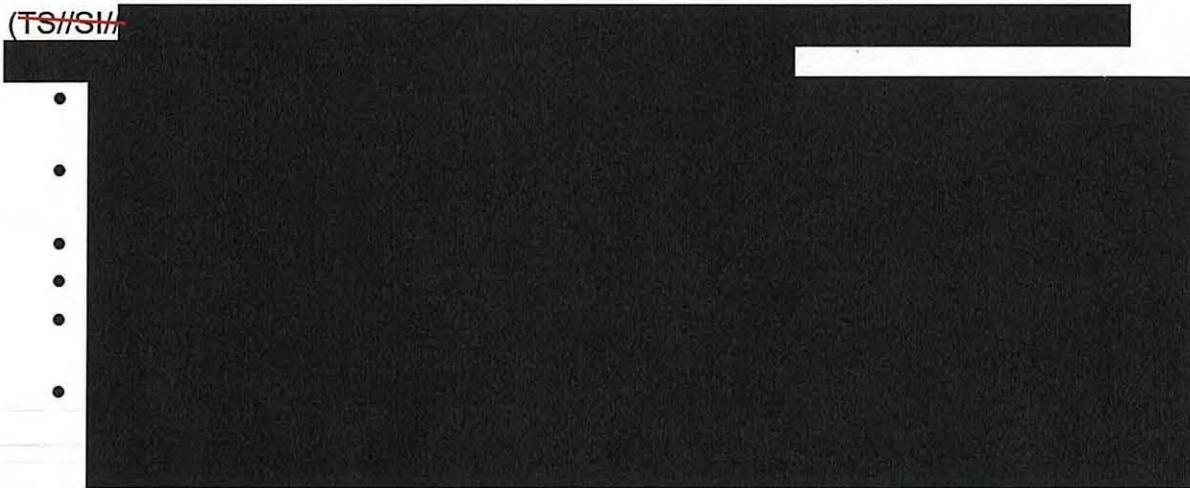


(TS//SI//NF)



(TS//SI//NF) The Targeting Procedures require that the USG have a reasonable belief that a target is located outside the U.S. in order to target a target's selectors. Reasonable belief is based on a totality of the circumstances, not just one single fact. Once the USG is made aware of another possible fact about a target's location (that is, [REDACTED] the USG must consider that fact in its on-going analysis of whether a selector remains appropriate to target.

(TS//SI//NF)



- [REDACTED]

(U) With [REDACTED], here are some common scenarios:

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

- (TS//SI//NF)

- (S//SI//NF)

- (TS//SI//NF)

(U) SUMMARY

(TS//SI//NF) In this lesson, we discussed specific issues related to (b) (3) (A) collection,

(U) You should be able to:

- (U//FOUO) Describe the characteristics of (b) (3) (A) collection
- (U//FOUO) Distinguish between [REDACTED] and [REDACTED]
- (U//FOUO) Apply the Targeting and Minimization Procedures to the retention of [REDACTED]
- (U//FOUO) Identify the rules for conducting U.S. Person queries in collected data
- (U//FOUO) Identify the procedures for dealing with [REDACTED]"

(U) KNOWLEDGE CHECKS

(TS//SI//NF) Data collected via (b) (3) (A) includes:

- a.
- b.
- c.
- d.

(TS//SI//NF) Which of the following is a FALSE statement?

TOP SECRET//SI//NOFORN

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- a.
- b.
- c.
- d.

(TS//SI//NF) Which of the following is a true statement about querying using USP identifiers in collected FAA Section 702 data?

- a. (b) (3) (A)
- b.
- c.
- d.

(TS//SI//NF) When [REDACTED] an NSA tasking of a FAA Section 702 selector, which of the following actions must you perform?

- a.
- b.
- c.
- d.

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

~~(TS//SI//NF)~~ LESSON FIVE: UPSTREAM AND MCTs

~~(TS//SI//NF)~~ In this lesson we'll discuss UPSTREAM collection and [REDACTED] to include [REDACTED] Multiple Communications Transactions (MCTs). We'll also detail the analyst's responsibilities with regard to MCTs.

~~(S//SI//NF)~~ At the end of this lesson, you will be able to:

- Describe the characteristics of UPSTREAM collection
- Define [REDACTED]
- Define Multiple Communications Transactions (MCTs)
- Differentiate NSA's use of the [REDACTED] different MCT categories
- Identify an analyst's role in working with MCTs

~~(TS//SI//NF)~~ UPSTREAM COLLECTION

~~(TS//SI//NF)~~ Let's do a recap of the basics of UPSTREAM collection.

~~(TS//SI//NF)~~ With UPSTREAM, NSA acquires any communications that [REDACTED]

~~(TS//SI//NF)~~ With UPSTREAM collection, NSA can also acquire communications from non-targeted selectors that refer to the target. So in addition to the communications "to" or "from" the target, we can also get the communications "about" the target.

~~(TS//SI//NF)~~ UPSTREAM collection enables NSA to acquire [REDACTED] Such collection, however, can bring in non-targeted communication of U.S. persons or persons located in the U.S. Because such non-targeted communicants might be in contact with other persons in the U.S., the resulting collection could contain domestic communications. As a result, the Foreign Intelligence Surveillance Court required NSA to adjust its Minimization Procedures to mitigate these concerns identified as "Multiple Communications Transactions" or MCTs. We will talk about this later in this lesson. First, we'll detail how UPSTREAM allows for [REDACTED]

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) Examples¹

¹~~(TS//SI//NF)~~ Here are a few examples of [REDACTED]

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

~~(TS//SI//NF)~~ Example 2: [REDACTED]

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

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

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

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

²~~(TS//SI//NF)~~ [REDACTED]

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

³(~~TS//SI//NF~~) [REDACTED]

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

(~~TS//SI//NF~~) MULTIPLE COMMUNICATIONS TRANSACTIONS (MCTs)

(~~TS//SI//NF~~) Also exclusive to UPSTREAM collection, since it can bring in non-targeted communicants who might be in contact with other persons in the U.S., is a concept called Multiple Communications Transactions (MCTs). Let's break this concept down.

(~~TS//SI//NF~~) The Minimization Procedures describe an "Internet transaction" as "an Internet communication that is acquired through NSA's UPSTREAM collection techniques."

(~~TS//SI//NF~~) An Internet transaction may contain information or data representing a "single, discrete communication," such as a single e-mail message that is "to", "from", or "about" a targeted selector.

(~~TS//SI//NF~~) Or an Internet transaction may contain multiple "single, discrete communications" sent as a single transaction. An example would be [REDACTED]

(~~TS//SI//NF~~) Currently our UPSTREAM collection systems cannot break apart these MCTs. One example of this is [REDACTED]

(~~TS//SI//NF~~) MCT CATEGORIES and the ACTIVE USER

(~~TS//SI//NF~~) Some MCTs are made available to analysts; others are not. NSA uses information about the "active user"⁴ in an Internet transaction to differentiate various types of MCTs.

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

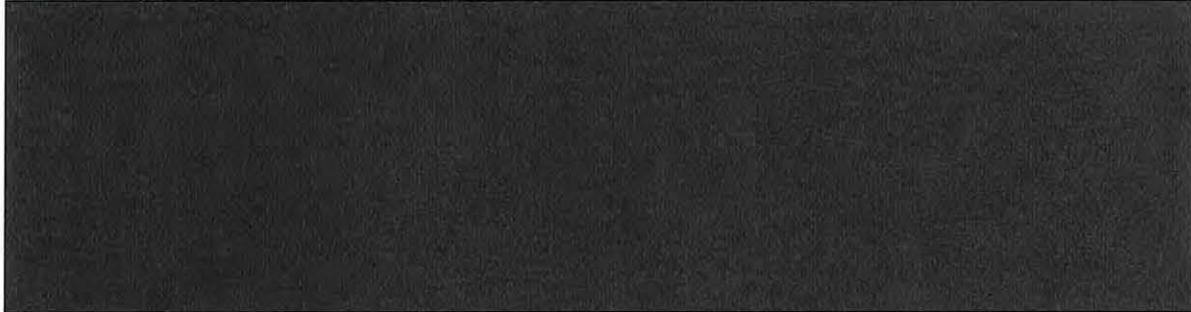
OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

⁴(~~TS//SI//NF~~) The "active user" is the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider.

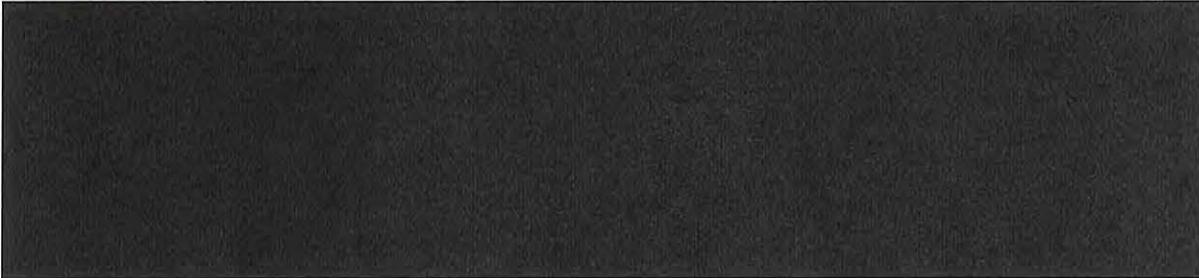
~~(TS//SI//NF)~~ MCT CATEGORIES

(~~TS//SI//NF~~) NSA developed a labeling convention for the [REDACTED] types of UPSTREAM traffic, [REDACTED], to distinguish between types of Internet transactions and what can be determined technically about the "active user." Some of these MCTs are available to analysts in corporate stores and some are segregated from the analytic population. Access to such data requires specialized training and pre-coordination with SV and OGC.

(~~TS//SI//NF~~) MCTs available in corporate stores



(~~TS//SI//NF~~) Segregated MCTs



~~(TS//SI//NF)~~ ANALYST RESPONSIBILITIES WITH MCTs

(~~TS//SI//NF~~) While NSA systems automatically segregate certain MCTs for you as an analyst, you are also responsible for looking for and appropriately handling any MCTs when reviewing any UPSTREAM data.

(~~TS//SI//NF~~) Use in reporting, future FAA Section 702 targeting, and FISA applications:

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

- ~~(TS//SI//NF)~~ Only use single, discrete communications and those communications within an MCT that are "to", "from", or "about" the targeted selector [REDACTED]
- ~~(TS//SI//NF)~~ You may review the entire MCT to understand what kind of MCT it is, [REDACTED] and the relationship of the targeted selector to [REDACTED]. But you may only use the single discrete communications "to", "from", or "about" the targeted selector.

~~(TS//SI//NF)~~ Use of Metadata

- ~~(TS//SI//NF)~~ You may use metadata from Internet transactions as long as those Internet transactions are not segregated as [REDACTED]
- ~~(TS//SI//NF)~~ You must purge the associated metadata when the underlying content associated with the metadata is problematic and requires purging and/or recalling reports.
- ~~(TS//SI//NF)~~ If the metadata represents a domestic communication, then that metadata and the associated Internet transaction must be purged.

~~(TS//SI//NF)~~ Destruction of MCTs

~~(TS//SI//NF)~~ If you recognize that any portion of an MCT contains a domestic communication, then the entire MCT must be purged. The only exception to this would be if the domestic communication pertains to a targeted selector that has roamed into the U.S. and we've obtained a Destruction Waiver (to be discussed later).

~~(TS//SI//NF)~~ OTHER MCT USES

~~(TS//SI//NF)~~ We previously stated that the only piece of an MCT authorized for use is the single discrete communication to, from, or about the targeted selector. There are actually two exceptions to this rule.

~~(TS//SI//NF)~~ First, if you identify a single, discrete communication [REDACTED] that

- (1) contains foreign intelligence,
- (2) is not to, from, or about the targeted selector, AND
- (3) the discrete communication is not to or from an identifiable U.S. person or person located in the U.S.,

then you may use it in a similar manner as the treatment of any other foreign communication.

~~(TS//SI//NF)~~ Second, if you identify discrete communication within the MCT that

- (1) is not to, from, or about a targeted selector, but

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

~~TOP SECRET//SI//NOFORN~~**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(2) it IS to, from, or about a U.S. person or a person in the U.S., then it may only be used to protect against an immediate threat to human life. This information must be specifically documented and NSA must inform DOJ and ODNI of such use.

(U) SUMMARY

(S//SI//[REDACTED]) In this lesson we discussed UPSTREAM collection and the different targeting strategies we use exclusively with UPSTREAM [REDACTED] We also detailed the analyst's responsibilities with regard to MCTs.

- (S//SI//[REDACTED]) You should now be able to:
- Describe the characteristics of UPSTREAM collection
 - Define [REDACTED]
 - Define Multiple Communications Transactions (MCTs)
 - Differentiate NSA's use of the [REDACTED] different MCT categories
 - Identify an analyst's role in working with MCTs

(U) KNOWLEDGE CHECKS:

(TS//SI//NF) Which of the following is NOT a characteristic of UPSTREAM collection?

- a. [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

(TS//SI//NF) Which of the following is an accurate definition of [REDACTED]

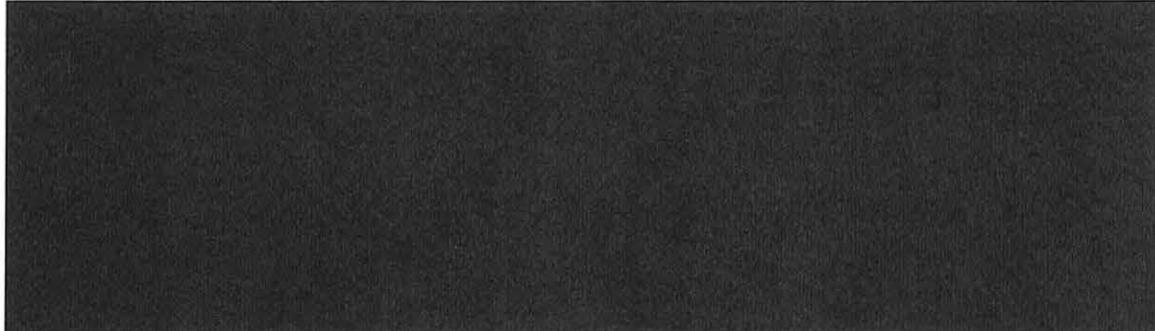
- a. [REDACTED]
- b. [REDACTED]
- c. [REDACTED]
- d. [REDACTED]

(TS//SI//NF) Which of the following describes a Multiple Communications Transaction?

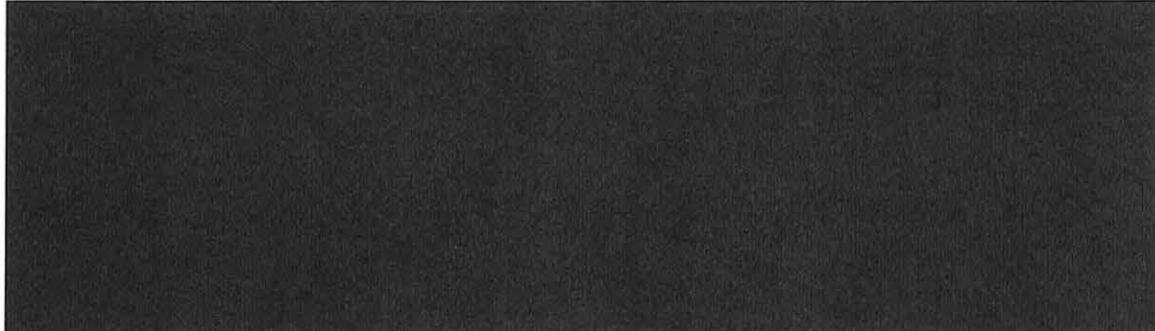
~~TOP SECRET//SI//NOFORN~~

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

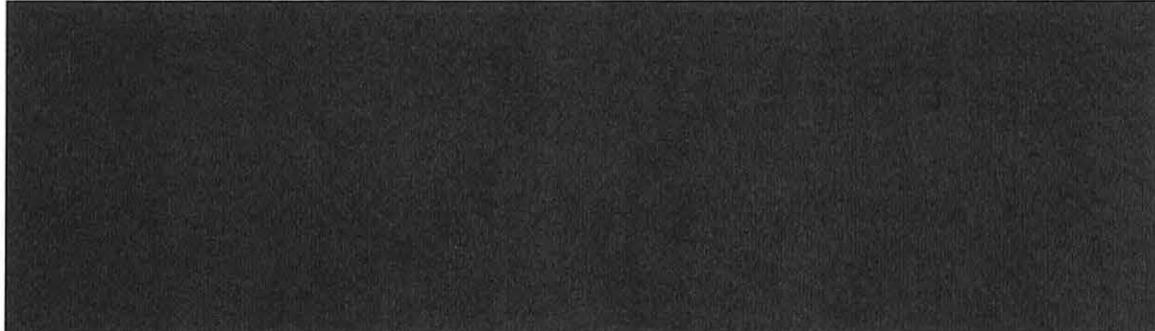
a.



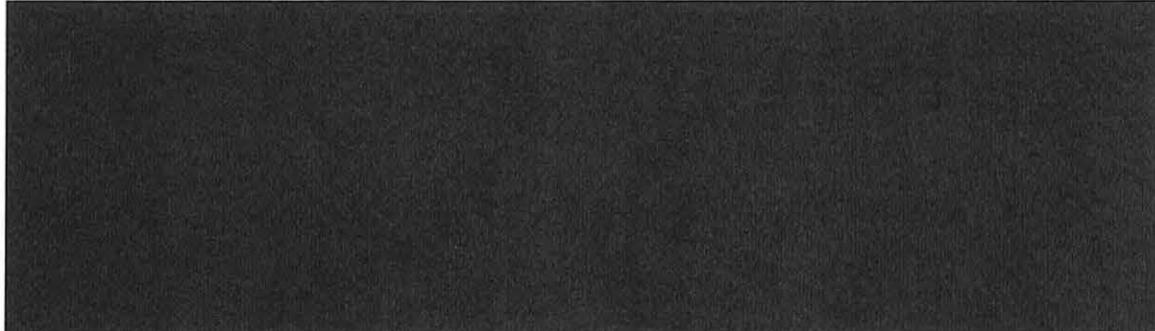
b.



c.

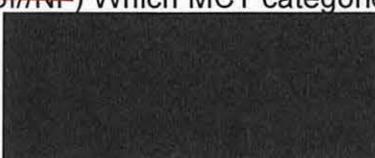


d.

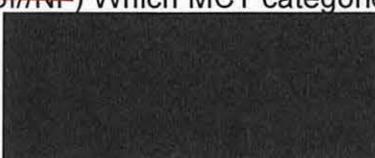


(~~TS//SI//NF~~) Which MCT categories are available in corporate stores?

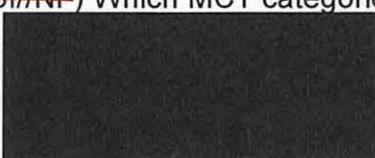
a.



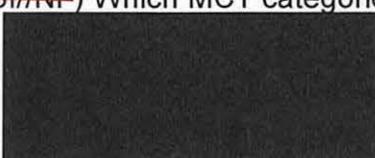
b.



c.



d.



(~~TS//SI//NF~~) Which of the following is NOT an allowable activity pertaining to MCTs?

a.



b.



c.



d.



~~TOP SECRET//SI//NOFORN~~**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL****(U) LESSON SIX: RETENTION**

(~~TS//SI//NF~~) As any specific communication is reviewed, whether from ~~(b) (3) (A)~~ UPSTREAM, or Telephony collection, an analyst makes a decision about retention. In the preceding lessons, we have detailed factors that guide the retention decision. In this lesson we will discuss the basic retention rules applied to all collected data. We will also discuss when it may be appropriate to request a destruction waiver.

(U//~~FOUO~~) At the end of the lesson, you will be able to:

- Identify the base retention periods for FAA Section 702 collected data
- Identify the various ways NSA can retain data that would otherwise be purged

(U) BASE RETENTION PERIOD

(~~TS//SI//NF~~) According to the Minimization Procedures, for those communications that have not been reviewed by analysts or for which final determinations haven't been made as to whether the communication meets the FAA Section 702 data criteria, the base retention or "age-off" period (the length of time that NSA may retain such communications) is:

- Five years for ~~(b) (3) (A)~~ and Telephony and
- Two years for UPSTREAM

(~~TS//SI//NF~~) In certain circumstances, the SIGINT Director may approve in writing an extension beyond the base retention for specific communications. Under current policy, the SIGINT Director may set a longer retention period not to exceed five years in total. Therefore these extensions will only apply to UPSTREAM collection. Any retention period longer than five years in total must be approved by DNI. A base retention extension is not be confused with DIRNSA's approval of a destruction waiver which will be discussed later in this lesson.

(U) FAA SECTION 702 RETENTION RULES

(~~TS//SI//NF~~) Remember, as discussed earlier in Lesson 3, as you review communications from any of FAA Section 702 data acquisition sources, you may need to destroy information earlier than five or two years based on the answers to these three questions:

1. (~~S//SI//NF~~) Is the communication a "foreign communication" or a "domestic communication?"
2. (~~C//~~) Is it "to", "from", or "about" the target?
3. (~~S//SI//NF~~) Does the communication contain U.S. person information?

According to Section 3(b)(1) of the Minimization Procedures, if the

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

communication is of or concerning any USP, you must destroy the communication at the earliest practicable point at which such communication can be identified as either: clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated.

~~(U//FOUO)~~ PRESERVATION ORDERS

~~(S//NF)~~ NSA may temporarily retain specific FAA section 702-acquired information that would otherwise need to be destroyed if the Department of Justice (DOJ) advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation.

~~(S//NF)~~ The specific information to be retained shall be identified in writing by the Department of Justice includes, but is not limited to:

- the target(s) or selector(s) whose information must be preserved;
- the relevant time period at issue in the litigation; and,
- the particular litigation for which the information will be retained.

~~(U//FOUO)~~ Click here for more details about Preservation Orders¹

¹~~(S//NF)~~ The retained, unminimized FAA section 702-acquired information that would otherwise have been destroyed according to FAA Section 702 Minimization Procedures will only be available to personnel working on the particular litigation matter. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice.

~~(S//NF)~~ The Department of Justice shall notify NSA in writing once the FAA section 702-acquired information is no longer required to be preserved, and then NSA shall promptly destroy the FAA section 702-acquired information as otherwise required by the FAA Section 702 Minimization Procedures.

~~(S//NF)~~ Should FAA section 702-acquired information subject to other destruction/age off requirements in the minimization procedures (e.g., Section 5/domestic communications) need to be retained because it is subject to a preservation requirement, the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate and consistent with law.

~~(S//NF)~~ Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain FAA section 702-acquired information. Should such circumstances arise, they will be brought to the attention of the appropriate court with jurisdiction over the underlying litigation matter for resolution.

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(U//~~FOUO~~) DESTRUCTION WAIVERS

(S//SI//[REDACTED]) Per Section 5 of the Minimization Procedures, if NSA determines after validly targeting a selector that NSA has unintentionally acquired domestic communications, or has acquired communications that must be treated as domestic communications (i.e., in the case of a change in status where the user has turned out to be a USP or person in the U.S.), then the NSA must purge those communications, unless the DIRNSA approves a written Destruction Waiver or the traffic is used for specific collection avoidance purposes to report the location of a user of an FAA Section 702 targeted selector to the FBI (to be discussed in Lesson 8). The waiver must contain sufficient facts to allow the Director to make an appropriate decision on a communication-by-communication basis.

(S//SI//[REDACTED]) As per DOJ, ODNI, and the Court's guidance, Destruction Waivers should be rare and must be pre-coordinated with DOJ/ODNI. Contact OGC or SV for assistance. Please keep in mind that we must list any data that is the subject of a Destruction Waiver on the Master Purge List (listed with a "Quarantine" state), and you can only use the data for the purposes outlined in the waiver.

(TS//SI//NF) Destruction Waivers fall into **four categories²:**

- (S//SI//[REDACTED]) Significant Foreign Intelligence
- (TS//SI//NF) Evidence of a Crime
- (TS//SI//NF) Technical Database Information or COMSEC Vulnerabilities
- (S//SI//[REDACTED]) Imminent Threat to Life

²(S//SI//[REDACTED]) **Significant Foreign Intelligence**

(TS//SI//NF) *If a waiver is secured with a finding of significant foreign intelligence that would allow the retention of specific communications that would otherwise have to be purged, then NSA would not have to recall previously disseminated reporting based on those same communications. If a waiver is not approved, any previously disseminated reporting would have to be recalled or, if alternate source material is available, an existing report could be re-sourced to exclude data that requires purging.*

(TS//SI//NF) Evidence of a Crime

(TS//SI//NF) *If a waiver is secured for evidence of a crime, such communications may be disseminated to appropriate law enforcement authorities as indicated in the Minimization Procedures. NSA may retain these communications for a reasonable period of time not to exceed 6 months unless extended in writing by the AG, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes.*

(TS//SI//NF) Technical Database Information or COMSEC Vulnerabilities

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

~~(TS//SI//NF)~~ If a waiver is secured for technical database information or COMSEC vulnerabilities, such communications may be disseminated to the FBI or other appropriate elements of the U.S. government and may be retained for a period sufficient to allow thorough exploitation as indicated in the procedures. In the case of retention for cryptanalysis purposes, enciphered data can be retained as long as needed; unenciphered data is subject to the base retention rules, which are 2 years for UPSTREAM and 5 years for [b] (3) (A) and Telephony.

~~(S//SI//NF)~~) Imminent Threat to Life

If a waiver is secured for imminent threat to life, such information may be retained and disseminated as reasonably necessary to counter the threat.

~~(TS//SI//NF)~~ Please keep in mind that domestic communications from MCTs are not eligible for a Destruction Waiver unless the target is one of the communicants.

~~(TS//SI//NF)~~ Additionally, the 702 Destruction Waiver can only be obtained when the communications to be waived were validly acquired. For example:

- If the selector was improperly targeted, a destruction waiver is not appropriate.
- If we knew that a target was coming to the U.S., but we neglected to detask the target's selectors before he arrived in the U.S., which resulted in a delayed detargeting, then a destruction waiver is not appropriate.

(U) SUMMARY

~~(TS//SI//NF)~~ In this lesson we discussed the basic retention rules applied to all collected data. We also detailed the reasons involved for requesting a destruction waiver.

~~(U//FOUO)~~ At the end of the lesson, you will be able to:

- Identify the base retention periods for FAA Section 702 collected data
- Identify the various ways NSA can retain data that would otherwise be purged

(U) KNOWLEDGE CHECKS

~~(TS//SI//NF)~~ What is the base retention period for [b] (3) (A) and UPSTREAM data?

- a. [b] (3) (A)
- b. [b] (3) (A)
- c. [b] (3) (A)
- d. [b] (3) (A)

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(~~TS//SI//NF~~) Under certain circumstances, NSA may retain specific FAA Section 702 data that would otherwise need to be destroyed. Which of the following is NOT one of those circumstances?

a. (b) (3) (A)

b.

c.

d.

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) LESSON SEVEN: DISSEMINATION

(S//[REDACTED]) This lesson will discuss how to disseminate information based on FAA Section 702 collection to U.S. customers and foreign governments.

(U//FOUO) At the end of this lesson, you should be able to:

- (U//FOUO) Summarize your responsibilities regarding dissemination of FAA data
- (S//SI//NF) Identify the procedures for sharing unminimized FAA Section 702 data with CIA and FBI
- (S//SI//[REDACTED]) Summarize the procedures for disseminating reports containing U.S. person information
- (U) Identify the different caveats in use
- (U//FOUO) Summarize the procedures for correcting dissemination errors
- (U//FOUO) Identify collaboration procedures with foreign governments

(U//FOUO) SHARING WITHIN NSA

(S//SI//[REDACTED]) Access to FAA Section 702 data within NSA repositories comes with responsibility. Only personnel, who are under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA), who have a documented mission need to access the data and who are trained on how to handle the data in a compliant fashion, may receive access to this data. This course (OVSC 1203) and the accompanying competency test satisfy the NSA training requirement.

(S//SI//[REDACTED]) Anyone with access to FAA Section 702 data may only share this data via proper channels with other NSAers that have up-to-date training. The data should not be removed from approved corporate stores unless it is handled in accordance with Compliance Advisory #038 and Executive Message 301. Use of corporate stores enables proper access controls, adherence to retention limits and data management, and effective purge actions.

(S//NF) SHARING WITH CIA AND FBI

(S//NF) As previously discussed, the Government implements FAA Section 702 through a partnership between NSA, CIA, and FBI. All three agencies abide by the same Targeting Procedures as described below:

- (S//SI//NF) NSA's Targeting Procedures set the requirements for determining the eligibility of a target and selector (i.e., outside of the U.S., a non-USP, and

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

Foreign Intelligence purpose for each target); the procedures apply for all

(b) (3) (A) Telephony, and UPSTREAM collection.

- (S//SI//NF)

(S//SI//NF)

CIA and FBI must handle the traffic they receive in accordance with their own FAA Section 702 Minimization Procedures. CIA and FBI analysts are also required to receive training on their own minimization procedures before accessing FAA Section 702 data in their own databases.

(S//SI//NF) For these reasons, analyst-to-analyst exchange of unminimized FAA Section 702 data is not authorized.

(S//SI//NF) What we just described is referred to as "sharing." Any other provision of FAA Section 702-derived information is dissemination to include [REDACTED] **Do not** provide unpublished data to CIA or FBI—even if it's evaluated and minimized.

(U) DISSEMINATION PROCEDURES

(S//SI//NF) The Minimization Procedures set forth limits on dissemination of FAA 702 derived data. Per the Minimization Procedures and NSA SIGINT reporting policy:

- If there's no U.S. person information, you may disseminate the report according to standard policy.
- If there is U.S. person information, you may disseminate it if you mask the identity.

(S//SI//NF) According to the FAA Section 702 Minimization Procedures, you may disseminate the actual U.S. person identifier ONLY to recipients who require the identity of that person in the performance of the recipients' official duties AND ONLY if at least one of the criteria listed in the Minimization Procedures¹ is also met. In addition, per NSA's SIGINT Reporting Policy's prior approval by S1 is required.

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

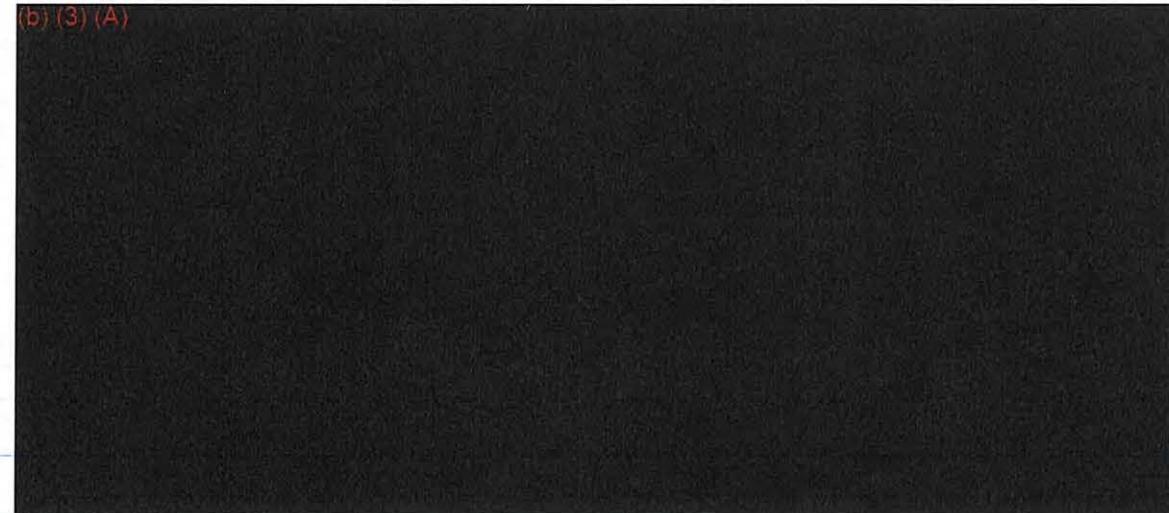
OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

¹(S//SI/ [REDACTED]) The criteria listed in the Minimization Procedures are as follows:

- U.S. person has consented to dissemination or the specific U.S. person information you wish to disseminate is publicly available
- U.S. person identity is necessary to understand the foreign intelligence or assess its importance
- There are indications that the U.S. person is an agent of a foreign power, a foreign power, 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 U.S. person has or has had access to classified national security information or material
- U.S. person may be the target of intelligence activities of a foreign power
- U.S. person is engaged in unauthorized disclosure of classified national security information (but only if the agency that originated the information certifies that it is properly classified)
- U.S. person may be engaging in international terrorist activities
- U.S. person communication was authorized by a court order AND the communication may relate to the foreign intelligence purpose of the surveillance
- There is evidence of a U.S. person engaging in a criminal activity (consult with OGC)

(S//SI/ [REDACTED]) For more guidance, the "Identities in SIGINT Manual" outlines the criteria NSA will use to determine whether and/or how to include U.S. person information in disseminations. Subject to approval, you may identify U.S. persons if they meet one of the criteria from the "Identities in SIGINT Manual"²:

²(U//FOUO) Criteria from Identities in SIGINT Manual:



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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) DISSEMINATION PROCEDURES: THREAT TO LIFE

~~(S//NF)~~ In situations involving "immediate threat to life", the [REDACTED] (b) (3) (A) prior written approval is not necessary to [REDACTED] on information. However, you must notify [REDACTED] (b) (3) (A) immediately of such disseminations because NSA m [REDACTED] Community. "Immediate" means [REDACTED]

(U) DISSEMINATION PROCEDURES: SENSITIVE INFORMATION

~~(S//NF)~~ In a specific situation wherein a report contains sensitive or potentially sensational references, you must send it to the [REDACTED] (b) (3) (A) team [REDACTED] (b) (3) via [REDACTED] (b) (3) (A) (DL [REDACTED] (b) (3)) prior to dissemination. The [REDACTED] (b) (3) team does not need to see all reports that contain U.S. person information.

(U) ATTORNEY CLIENT PRIVILEGED COMMUNICATIONS

~~(S//SI//[REDACTED])~~ NSA's OGC must be notified and must approve disseminations of information constituting attorney-client privileged communications, as discussed in Lesson Three.

(U//FOUO) UNAUTHORIZED USE OF DATA

~~(S//SI//[REDACTED])~~ Under no circumstances may you use or disclose any information derived from FAA Section 702 in any criminal proceeding, immigration proceeding, or in any other legal or administrative proceeding without the advance authorization of the AG of the U.S. Such requests will be coordinated by OGC.

(U//FOUO) "/FISA" PORTION MARKING

~~(U//FOUO)~~ As promulgated by [REDACTED] (b) (3) (A) [REDACTED] all information produced or issued after [REDACTED] (b) (3) (A) that is based directly on, or acquired from, information collected under the Foreign Intelligence Surveillance Act (FISA) and FISA Amendments Act (FAA) authorities must be portion marked as FISA.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(U//~~FOUO~~) In classified serialized NSA products releasable to U.S. [REDACTED] recipients, paragraphs/portions containing any FISA/FAA-acquired information must include FISA in the portion mark.

(U//~~FOUO~~) Portion marking example: [REDACTED]

(U//~~FOUO~~) Do not include FISA portion marks in serialized NSA products releasable to [REDACTED]

(U) APPROPRIATE USE OF CAVEATS

(S//SI/ [REDACTED]) We'll now focus on the caveats that you must apply to reports based on FAA Section 702 data in various situations.

(S//SI/ [REDACTED]) To prevent unauthorized use or disclosure, NSA requires that all disseminations of FAA Section 702 derived information bear various caveats to indicate the purpose of the information contained within the report or document.

(S//SI/ [REDACTED]) The following are the different caveats³ NSA uses on its disseminations

-
-
-
-
-
-
-

³"(U//~~FOUO~~) *Intelligence Purposes Only*" or IPO caveat (b) (3) (A)

"(U//~~FOUO~~) (b) (3) (A)

(U//~~FOUO~~) COMINT-derived information TEAR LINES

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

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

"~~(U//FOUO)~~ (b) (3) (A)



~~(U//FOUO)~~ (b) (3) (A)



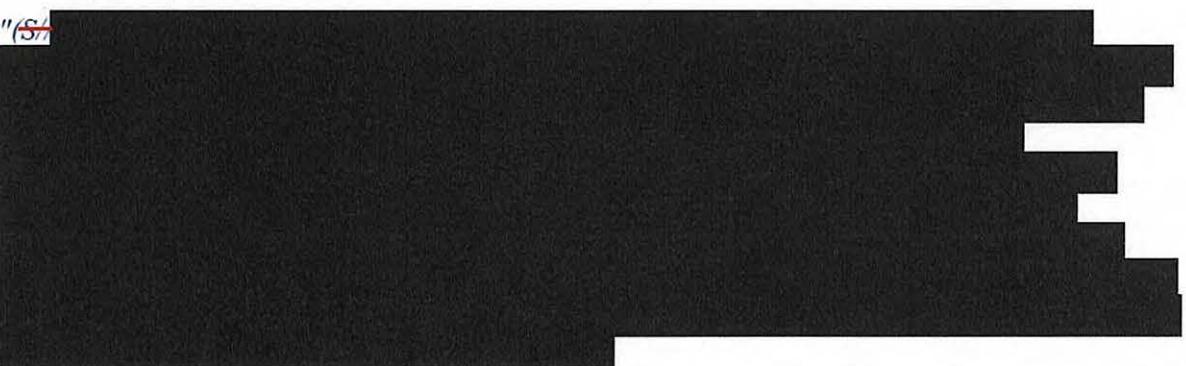
"~~(//NU)~~ (b) (3) (A)



~~(U//FOUO)~~ (b) (3) (A)



~~(S//~~) FBI FISA Caveat



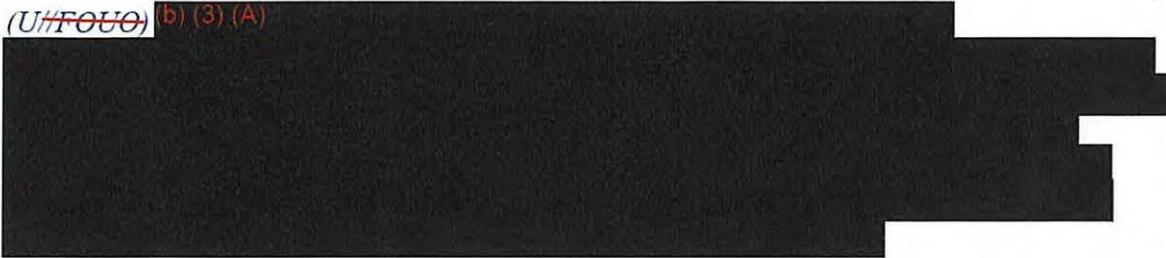
~~(U//FOUO)~~ FAA 702 Attorney Client Communications Caveat

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

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

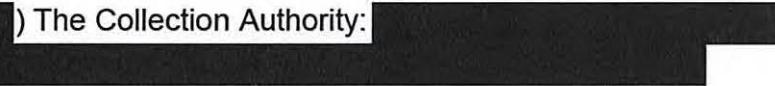
OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

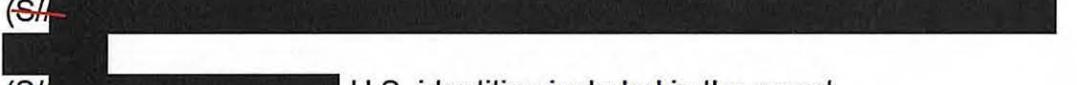
(U//~~FOUO~~) (b) (3) (A)

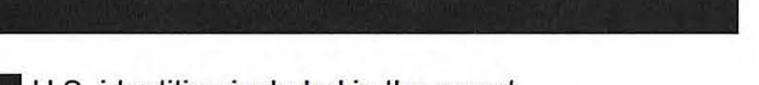
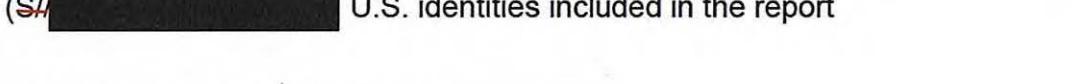
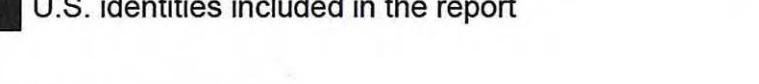


(U//~~FOUO~~) DOCUMENTING SOURCE VERIFICATION, MCT, AND COLLECTION AUTHORITIES

(S//~~REF ID: A1~~) NSA is required to account for and be able to trace any dissemination based on any FAA Section 702 derived information. Regardless of the tool used for dissemination, you are required to document:

- (S//~~REF ID: A2~~) The Collection Authority: 



- (S//~~REF ID: A3~~) 


- (S//~~REF ID: A4~~) 

- (S//~~REF ID: A5~~) U.S. identities included in the report 

(U) CORRECTING DISSEMINATION ERRORS

(S//SI//~~REF ID: A6~~) If NSA determines that an FAA Section 702 derived report or other dissemination contains U.S. person information that does not meet the standards for dissemination under these procedures, the TOPI must recall it. If appropriate, the TOPI may reissue the report, masking the U.S. identities. The TOPI must also report any improper FAA Section 702 dissemination as an incident to SV (d) SV41 INCIDENTS). We will discuss incidents in the next lesson.

(U//~~FOUO~~) COLLABORATION WITH FOREIGN GOVERNMENTS

(S//SI//~~REF ID: A7~~) **Section 8(a) of the Minimization Procedures** allows NSA to disseminate evaluated and minimized information to foreign governments. **NSA's preferred method for such disseminations is to use serialized product reports.** Alternatively, under that Section and per SID direction, NSA may choose to disseminate

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(i.e., [REDACTED] to a foreign partner for a specific purpose [REDACTED] Any dissemination of [REDACTED] to a foreign partner requires SID DIR's prior approval. [REDACTED]

[REDACTED] DOJ/ODNI review both NSA's disseminations of [REDACTED] to a foreign government and [REDACTED] at NSA's bi-monthly oversight review. The IPO caveat must be displayed on all [REDACTED] disseminations.

(S//SI//NF) For situations in which NSA lacks linguistic or technical capabilities to process FAA Section 702 acquired data, Section 8(b) of the Minimization Procedures allows NSA to disseminate raw data to a foreign government solely for the purpose of getting that partner's technical or linguistic assistance. The foreign partner may only use the raw material to provide the specific requested assistance and may make no other use of the material or disseminate it further. The foreign partner must return the raw material to NSA at the completion of the assistance and confirm that it retains no copies. Such disseminations may only occur under strict handling procedures on both the part of the foreign government and NSA. Any activity envisioned under Section 8(b) must first be cleared with NSA SV and OGC. SV and OGC will keep the necessary records and make reports to DOJ/ODNI.

(U//FOUO) DOJ/ODNI OVERSIGHT

(S//SI//NF) All NSA disseminations must be made available to Department of Justice (DOJ) and Office of the Director of National Intelligence (ODNI) oversight officials at NSA's bi-monthly FAA Section 702 reviews. DOJ and ODNI will assess NSA's minimization and handling of U.S. person information. The U.S. identity information from the source records will also be included in the bi-monthly reviews.

(U) SUMMARY

(S//SI//NF) This lesson discussed how to disseminate information based on FAA Section 702 collection to U.S. customers and foreign governments.

(U//FOUO) You should now be able to:

- (U//FOUO) Summarize your responsibilities regarding dissemination of FAA data
- (S//SI//NF) Identify the procedures for sharing unminimized FAA Section 702 data with CIA and FBI

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

- ~~(S//SI//~~ [REDACTED]) Summarize the procedures for disseminating reports containing U.S. person information
- (U) Identify the different caveats in use
- (U//~~FOUO~~) Summarize the procedures for correcting dissemination errors
- (U//~~FOUO~~) Identify collaboration procedures with foreign governments

(U) KNOWLEDGE CHECKS:

~~(S//SI//NF)~~ Which of the following are authorized practices when sharing FAA 702 data with CIA and FBI? (check all that apply)

- a.
- b.
- c.
- d.

~~(S//SI//~~ [REDACTED]) Why does NSA use caveats on reports based on FAA Section 702 data?

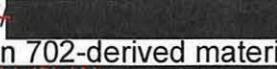
- a. ~~(b) (3) (A)~~
- b.
- c.
- d.

~~(S//SI//NF)~~ If NSA determines that an FAA Section 702 derived report or other dissemination improperly contains unminimized U.S. person information, which of the following is NOT a requirement?

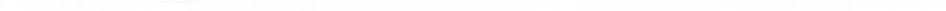
- a. ~~(b) (3) (A)~~
- b.
- c.
- d.

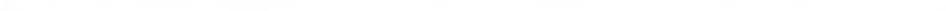
~~TOP SECRET//SI//NOFORN~~

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(S//SI//) What is the preferred method for disseminations of FAA Section 702-derived material to foreign governments?

- a. 

- b.

- c.

- d.


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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

(U) LESSON EIGHT: COMPLIANCE INCIDENTS and OVERSIGHT

(U//~~FOUO~~) This lesson will discuss the most common reportable events and how to properly report them. We'll also explore steps for remediation.

(U//~~FOUO~~) At the end of this lesson, you should be able to:

- (U//~~FOUO~~) Recognize what types of events are reportable through the internal and external FAA Section 702 oversight process
- (U) State what constitutes a compliance incident
- (U//~~FOUO~~) Summarize the steps that might be required to remediate a compliance incident or change in status event
- (S//~~██████████~~) Summarize the external oversight procedures for FAA Section 702 related to targeting, dissemination, and database queries

(U) WHAT IS A REPORTABLE EVENT?

(U//~~FOUO~~) NSA is required to report all incidents of non-compliance with the FAA Section 702 Targeting and Minimization Procedures to SV, OGC, and the NSA Inspector General (IG), as well as to our external overseers.

(C//~~██████████~~) NSA reportable events can occur at any point in the FAA Section 702 cycle of collection, processing, analysis, retention, and dissemination. Reportable events fall into two categories: a potential compliance incident or a change in the status of a user of a targeted selector. Let's discuss these types of events in more detail.

(U) COMPLIANCE INCIDENT

(S//SI//~~██████████~~) A compliance incident occurs when NSA's actions do not follow the FAA statute or the FAA Section 702 Targeting and/or Minimization Procedures because of something we do; something we fail to do; or something one of the electronic communication service providers who send us the communications does or fails to do.

(S//SI//~~██████████~~) For example, compliance incidents may occur when NSA avoidably collects on an inappropriate target, retains information outside of the procedures, or improperly disseminates a U.S. person identifier. Conversely, incidents

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

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

may also occur when NSA fails to take an appropriate action because an individual either made a mistake or failed to act upon information in a timely manner.

(U) Examples of reportable compliance incidents¹

¹~~(S//SI//NF)~~ An analyst mistyped a selector. As a result, NSA targeted the wrong e-mail account and, thereby, targeted an individual who does not meet the standards of the FAA Section 702 Targeting and Minimization Procedures.

~~(S//SI//NF)~~ (b) (3) (A)



(U) CHANGE IN STATUS

~~(S//SI//NF)~~ Remember that sometimes after appropriately targeting a selector, NSA learns that a change in status of the targeted user renders the targeting inappropriate. A change in status requires an immediate detargeting. For example, we discover a user of the selector has U.S. person status or is located in the U.S. Change in status implies that all of NSA's initial targeting actions were reasonable but once new information came to light, the targeted selector status changed, and we detargeted immediately.

(U) Examples of reportable events due to changes in status²

²~~(S//SI//NF)~~ You had a reasonable belief that your target was a non-USP living and working overseas; however, after reviewing collected traffic, you discovered



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



~~(TS//SI//NOFORN)~~ So, to summarize, a "compliance incident" is the result of something we do or fail to do, while a "change of status" is based on facts about the target that weren't available for review despite our best efforts. They both need to be promptly reported.

(U) INTERNAL/EXTERNAL REPORTING AND NOTIFICATION

~~(S//SI//NOFORN)~~ If you suspect a reportable event:

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

- ~~(S//SI//~~ [REDACTED]) Immediately contact SV (at ~~(b) (3) (A)~~). SV will work with you to answer the "who, what, when, how, and why;" they will communicate these findings with OGC.
- ~~(S//SI//~~ [REDACTED]) If you know that a targeted selector is no longer eligible for FAA Section 702 collection, you must detarget it immediately--do NOT wait for confirmation from SV.

~~(S//SI//~~ [REDACTED]) Prompt internal resolution regarding the facts is critical because NSA is obligated to report compliance incidents and changes in status within five business days to the DOJ and the ODNI. Failure to meet the notification deadline is itself a compliance incident. Therefore, you must inform SV of potential reportable events immediately and respond promptly to questions as SV and OGC investigate the matter.

~~(U//FOUO)~~ If you have any questions, do not hesitate to call SV or OGC.

(U) REMEDIATION

~~(S//SI//~~ [REDACTED]) Depending on the circumstances of the reportable event, NSA may be required to take remediation steps. For instance, we may:

- Immediately detarget selectors
- Identify and purge data that turns out to be ineligible for retention and dissemination
- Recall disseminated reports

~~(S//SI//~~ [REDACTED]) NSA must account for any required purging and the final disposition of reports as part of its documentation of compliance-related events. SV, along with NSA's purge team, will work with TOPIs to identify the material to be remediated.

~~(S//SI//~~ [REDACTED]) NSA's Minimization Procedures (Section 5) provide limited exceptions to the requirement to purge data and recall reporting. Specifically, we may retain some domestic communications or communications related to a change in status under three circumstances:

- To notify the FBI of a target's presence in the U.S.;
- If we obtain a Destruction Waiver; or
- For collection avoidance purposes.

~~(S//SI//~~ [REDACTED]) Any of these circumstances must be carefully coordinated with SV and requires status change in ~~(b) (3) (A)~~.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(U) FBI NOTIFICATION

(S//SI//[REDACTED]) As indicated in Section 5 of the Minimization Procedures, if a domestic communication (or communication that must be treated as a domestic communication) indicates that a target has entered the United States, NSA may tip FBI of that fact. NSA may also provide to FBI information concerning where and when the target was assessed to be in the U.S. NSA would then place this communication on the Master Purge List (MPL) to restrict further use.

(S//SI//[REDACTED]) Absent a destruction waiver (or dissemination authority under DIRNSA approval of a 72-hour continuation of coverage in the situation of a threat to life or serious bodily harm), however, NSA cannot share additional information gleaned from the domestic communication, such as [REDACTED], [REDACTED].

(S//SI//[REDACTED]) Additional communications that only reiterate the already disseminated location should not be retained or disseminated.

(U) DOJ/ODNI BI-MONTHLY OVERSIGHT REVIEWS OF FAA SECTION 702 ACTIVITY

(U//FOUO) In addition to the daily oversight of reportable events, the FAA Section 702 Targeting Procedures provide for bi-monthly reviews by the DOJ and ODNI to evaluate the implementation of the procedures. The DOJ and ODNI currently review three categories of information:

1. (U//FOUO) Tasking/targeting
2. (U//FOUO) Dissemination of U.S. person information
3. (U//FOUO) Queries using U.S. person terms as selectors

(U) Let's examine each of these categories in more depth.

(U) TARGETING REVIEWS

(S//[REDACTED] For targeting reviews, representatives from the DOJ and ODNI working in conjunction with SV and OGC, review every tasking sheet for a two-month period in preparation for a bi-monthly onsite review. This includes both new selectors and those that NSA has re-targeted after a break in targeting.

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

(S//~~SI//NF~~) Specifically, the overseers evaluate the documentation cited in the [REDACTED] to assess whether the information supports NSA's fore [REDACTED] the documentation is applicable to the Certification.

(S//~~SI//NF~~) If DOJ and ODNI have questions about the propriety of tasking (i.e. target's foreignness or the targeting analyst's rationale), SV works with the targeting analyst to supply any additional information. If NSA isn't able to produce sufficient additional information, NSA will likely need to detarget the selector and purge any collected data. It's important to mention that a Destruction Waiver would not be appropriate to retain data collected on a selector that was not validly target.

(S//SI//NF) NSA's review includes all selectors targeted as nominations from CIA and FBI also. DOJ and ODNI also make separate reviews at CIA and FBI of activities that are conducted under FAA Section 702.

(U) DISSEMINATION REVIEWS

(S//SI//~~NOFORN~~) In addition to targeting, the DOJ and ODNI also review NSA disseminations of material collected under FAA Section 702. The overseers evaluate NSA's minimization of U.S. person information and check for appropriate use of caveats, such as the IPO caveat.

(S//SI//~~NOFORN~~) makes available all serialized reports based on FAA Section 702 and informs DOJ and ODNI of any U.S. person information that's disseminated from FAA Section 702 collection through the "U.S. Idents Release" process.

(S//SI//~~NOFORN~~) In cases where a product line has SID Director approval (with a documented SPF) to disseminate [REDACTED] to a foreign partner or U.S. Intelligence Community agency, that product line must ensure that SV gets a copy [REDACTED] to include in the DOJ and ODNI reviews.

(U) U.S. PERSON QUERY REVIEWS

(TS//SI//NF) The third category covered at each bi-monthly review is NSA's queries of collected data using U.S. person identifiers as query terms. Remember--you must design all queries to return foreign intelligence information, and you may NOT use U.S. person identifiers as query terms in UPSTREAM data.

(TS//SI//NF) At each bi-monthly review, DOJ and ODNI review metadata queries using U.S. person identifiers, including the articulated foreign intelligence purpose. Remember

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

OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL

that content query terms currently require pre-approval from SV and OGC. DOJ and ODNI review the documented justification for the pre-approval.

(U) EMERGENCY DEPARTURES

(U) Section 1 of the NSA Minimization Procedures notes that if NSA determines it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (such as in the case of force protection or hostage situations), and that it's not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the ODNI and the National Security Division (NSD) of the DOJ. OGC should be consulted to ensure that any deviation from the procedures is otherwise lawful.

(U) Here are some examples of where emergency departure from the NSA Minimization Procedures might apply if there is an immediate threat to human life:

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

~~(TS//SI//NF)~~ Emergency situation or not, it is NEVER appropriate to target a selector used by a U.S. person in the U.S. under FAA Section 702 or to do anything else in violation of the statute.

(U) SUMMARY

~~(U//FOUO)~~ In this lesson we discussed the most common reportable events and how to properly report them. We also explored steps for remediation.

~~(U//FOUO)~~ You should now be able to:

- ~~(U//FOUO)~~ Recognize what types of events are reportable through the internal and external FAA Section 702 oversight process
- (U) State what constitutes a compliance incident

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

**OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818
FINAL**

- (U//~~FOUO~~) Summarize the steps that might be required to remediate a compliance incident or change in status event
- (S// Summarize the external oversight procedures for FAA Section 702 related to targeting, dissemination, and database queries

(U) KNOWLEDGE CHECKS:

(S//~~SI//NF~~) Which of the following is NOT a reportable event or compliance incident?

- a. (b) (3) (A)
- b.
- c.
- d.

(TS//~~SI//NF~~) Which of the following is NOT an appropriate remediation to a compliance incident or change in status event?

- a. (b) (3) (A)
- b.
- c.
- d.

(TS//~~SI//NF~~) NSA's external overseers perform bi-monthly reviews to assess compliance with the following procedures? (check all that apply)

- (b) (3) (A)
-
-
-