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

FOIA Case: 78711B
19 January 2016

ALAN BUTLER
EPIC
1718 CONNECTICUT AVE NW
STE 2000
WASHINGTON DC 20009

Dear Mr. Butler:

This is an interim response to your Freedom of Information Act (FOIA) request, which was received by this office on 1 August 2014, for:

"1. Any policies, regulations, white papers, final memoranda, guidelines, or training materials interpreting or addressing the retention, dissemination, or sharing of electronic communications or metadata under EO 12333.
2. The most recent version of IC member agency procedures adopted under EO12333, including DOD 5240 1-R, Army Regulation 381-10, and USSID-18.."

As noted in our previous responses, your request was assigned Case Number 78711.

As you may recall in our previous letter, dated 12 March 2015, we informed you that a number of documents have been reviewed and/or released in various other FOIA requests. After further review, we have located an additional document that we feel is responsive to your request, which is enclosed herein.

Also, as noted in our previous letter, your request has been placed in the first-in, first-out processing queue along with a similar FOIA request that contains one document responsive to your request. However, we inadvertently provided you with the incorrect FOIA Case number that your request is following. A portion of your request Case 78711, will piggbyback or follow Case 71488. As A review of the document in Case 71488 is completed, we will respond to you further.

FOIA Case: 78711B

Following any release in Case 71488, and as noted in our previous letter, one additional documents responsive *only* to your request will be processed in turn, based on the date of your request in our first-in, first-out backlog queue. Please be advised that there are significant number of cases ahead of yours in that queue. We appreciate your patience thus far.

Any other correspondence related to your request also should include the case number assigned to your request. Your letter should be addressed to National Security Agency, FOIA Office (DJ4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

CSBlacker FOR

JOHN R. CHAPMAN
Chief
FOIA/PA Office

OVSC1100

Lesson 1 - Introduction

(U//~~FOUO~~) Welcome to the Overview of Signals Intelligence (SIGINT) Authorities. I'm here to tell you about the course, what you're going to see and do, and what you will learn.

(U//~~FOUO~~) This course should take you about an hour to complete, and we hope it will give you a better understanding of the authorities that both enable and restrict the Agency's SIGINT activities.

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

- Identify the applicable surveillance authorities at a high level
- Define the basic provisions of these authorities
- Identify certain situations and circumstances that require additional authority

(U) Throughout this course, you will get information on relevant legal authorities. You will then have opportunities to check your knowledge about these authorities. These knowledge checks will not be graded. As you progress through the lessons, you will be able to compare and contrast the authorities to determine which might be applicable to a particular situation.

(U) Remember, this is an overview course. We don't intend for it to contain comprehensive information about all of the various legal authorities under which we conduct our foreign intelligence mission -- but we'll give you the links to more in-depth information if you need it.

(U) Throughout the course, the "Legal Readings" link in the left navigation pane will provide links to the authority documents.

(U//~~FOUO~~) If you need more assistance with understanding these authorities as they apply to your specific operational situation, please contact the SID's Office of Oversight and Compliance or the NSA Office of the General Counsel.

(U//~~FOUO~~) As we go through this course, you will see that NSA/CSS conducts its operations within the scope of some very specific authorities -- each having their own minimization procedures. NSA's EO 12333 minimization procedures, USSID SP0018, are divided into four major categories:

- Collection
- Processing
- Retention

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

- Dissemination

(U) We're going to examine each of these authorities at a high-level to see what they permit you to do, how you can use them, and which authority to seek in a given situation.

(U) The three lessons you are about to review explain the origin and derivation of NSA's authorities and how they're applied operationally. But before we begin, no discussion of SIGINT authorities would be complete without a quick mention of National Security Council Intelligence Directive 6 (NSCID 6).

(U//~~FOUO~~) NSCID 6 identifies SIGINT activities as national responsibilities used to satisfy the intelligence needs of the US Government and authorizes and directs how SIGINT activities are to be conducted for an efficient and economical use of available technical resources.

(U//~~FOUO~~) NSCID 6 begins by defining COMINT and ELINT activities within SIGINT:

(U//~~FOUO~~) "COMINT" or "Communications Intelligence" is the technical and intelligence information derived from foreign communications by other than the intended recipients. COMINT activities produce COMINT via the collection and processing of foreign communications passed by radio, wire or other electromagnetic means, and by the processing of foreign encrypted communications, however transmitted. Collection includes search, intercept and direction finding. Processing includes range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of the results.

(U//~~FOUO~~) COMINT activities, as defined by NSCID 6, do not include (a) any intercept and processing of unencrypted written communications, press and propaganda broadcasts, or (b) censorship.
(U//~~FOUO~~) "ELINT" or "Electronics Intelligence" is the technical and intelligence information produced from foreign, non-communications, electromagnetic radiations emanating from other than atomic detonation or radioactive sources.

(U//~~FOUO~~) NSCID 6 identified the Secretary of Defense as the Executive Agent of the US Government for conducting SIGINT activities. It established the roles of the Director and the Deputy Director of NSA and gave the Director of NSA (DIRNSA) responsibility to provide for the SIGINT mission of the US and to control all SIGINT collection and processing, except as otherwise stated in the directive.

(U//~~FOUO~~) NSCID 6 also established the Central Security Service (CSS), under DIRNSA in order to centralize and consolidate the performance of SIGINT functions. The CSS includes

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

SIGINT functions previously performed by various military organizations and other US Governmental elements.

(U//~~FOUO~~) As outlined in NSCID 6, DIRNSA is responsible for managing SIGINT resources, personnel, and programs, and is required to provide SIGINT to the Armed Forces and other agencies since they often require timely and effective SIGINT. DIRNSA is also authorized to conduct research and development to meet the SIGINT needs of the US.

(U//~~FOUO~~) NSCID 6 also set limits on SIGINT activities. For example, the directive specifically states that NSA may not produce all-source intelligence, often referred to as finished intelligence. Instead, NSA produces and disseminates finished SIGINT, which combines pertinent SIGINT information as well as collateral information and pertinent analytic comments, leaving the jobs of interpreting SIGINT reporting, producing finished intelligence, and persuading policymakers to the customer.

(U//~~FOUO~~) To summarize, the purpose of NSCID 6 was to provide a cohesive SIGINT analysis and processing effort within the Intelligence Community. As a result, NSA was explicitly given the responsibility to: (1) provide for the SIGINT mission of the US; (2) control all SIGINT collection and processing activities of the US; and (3) produce finished SIGINT in accordance with national objectives, requirements, and priorities.

(U) When you're ready to begin, select Lesson 2 from the course menu to continue.

(U) Good luck!

Lesson 2 - Conventional Collection

(U) Welcome to the Conventional Collection Lesson. This lesson deals with the authorities applicable to routine SIGINT operations at NSA and the limitations on those authorities.

(U) Here we are going to deal with the source of our authority and how we implement it. We will do this through a high-level examination of the relevant documents.

(U) As always, further information is available from SID's Office of Oversight and Compliance and the NSA Office of the General Counsel.

(U) This lesson examines Executive Order 12333, USSID SP0018, DoD Regulation 5240.1-R, and NSA/CSS Policy 1-23.

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

- Define and identify components of Executive Order 12333

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

- Identify implementing procedures--DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, and USSID SP0018

(U) This lesson should take approximately 15 minutes to complete.

(U//~~FOUO~~) Executive Order 12333 was issued by the President of the United States to provide for the effective conduct of US intelligence activities and the protection of the rights of US persons. It is the primary source of NSA's foreign intelligence-gathering authority.

(U//~~FOUO~~) Executive Order 12333 governs foreign intelligence activities across the Intelligence Community. Derivative documents such as DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, and USSID SP0018 establish policies and procedures consistent with Executive Order 12333.

(U//~~FOUO~~) Under Executive Order 12333, NSA collects, processes, analyzes, produces, and disseminates signals intelligence information and data. These activities are approved for foreign intelligence purposes, counterintelligence purposes, and for the conduct of military operations.

(U//~~FOUO~~) Executive Order 12333 permits collection, retention, and dissemination of the following types of information concerning US persons, such as:

- Information that is publicly available or collected with the consent of the person concerned
- Information constituting foreign intelligence or counterintelligence
- Information needed to protect the safety of any persons or organizations
- Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure
- Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws

(U//~~FOUO~~) We will now look at what documents provide for the implementation of EO 12333 authorities.

(U//~~FOUO~~) NSA's routine authority is implemented through DoD Regulation 5240.1-R, and NSA/CSS Policy 1-23, entitled Procedures Governing Activities of NSA/CSS that Affect US Persons.

(U//~~FOUO~~) Department of Defense Regulation 5240.1-R, sets forth procedures governing the activities of Department of Defense intelligence community agencies that affect US persons. A Classified Annex to the Regulation establishes the procedures NSA/CSS must follow while conducting SIGINT activities.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

(U//~~FOUO~~) These procedures cover a wide range of topics and permit broad powers for the collection of foreign intelligence. They detail collection, processing, retention, and dissemination of information about US persons.

(U//~~FOUO~~) Another key document is NSA/CSS Policy 1-23, Procedures Governing Activities of NSA/CSS that Affect US Persons.

(U//~~FOUO~~) The policy establishes procedures and assigns responsibilities to ensure that the NSA/CSS activities are conducted in a manner consistent with the privacy rights of US persons as required by law, executive orders, Department of Defense policies and instructions, and internal NSA/CSS policy.

(U) This document also defines the roles of the Office of the General Counsel and the Signals Intelligence Directorate with regard to intelligence oversight.

(U//~~FOUO~~) The USSID System is the mechanism through which the Director of the National Security Agency/Chief, Central Security Service exercises SIGINT operational control of the United States SIGINT System. USSIDs beginning with 'SP' are approved policies and doctrines for SIGINT Policy.

(U//~~FOUO~~) USSID SP0018 implements the provisions of Executive Order 12333, Department of Defense Regulation 5240.1-R, and NSA/CSS Policy 1-23. It covers policies and procedures for the collection of foreign intelligence information, while regulating collection, processing, retention, and dissemination of US person information. It assigns responsibilities to ensure that the missions and functions of the US SIGINT System are conducted in a manner that safeguards the privacy of US persons.

(U//~~FOUO~~) USSID SP0018 defines a US person as:

- a) A citizen of the United States
- b) An alien lawfully admitted for permanent residence in the United States, also known as a "Green Card" holder
- c) Unincorporated groups and associations a substantial number of the members of which constitute US citizens or "Green Card" holders
- d) Corporations incorporated in the United States, but not including those entities which are directed and controlled by a foreign government or governments. What's important to know is not who owns the corporation, but rather where the corporation is incorporated. For example, if corporation A is incorporated by a US Person outside the US, it is a foreign corporation and, therefore, it is not defined as a US person. On the other hand, if corporation Z is incorporated in the US by a non-US person, the corporation has US person status.
- e) Lastly, non-governmental US flagged ships and aircraft are legal entities and have the nationality of the country in which they are registered. So, even though ABC

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

airlines may be based out of the United Kingdom, if their planes are flagged, or registered in the US, their planes have US person status.

(U//~~FOUO~~) Practical application of USSID SP0018 for individuals requiring access to raw SIGINT data is contained in OVSC1800.

(U) The Supreme Court has ruled that the interception of non-public communications is a search and seizure under the Fourth Amendment. Therefore, Signals Intelligence operations must comport with the 'reasonableness' requirements of the Fourth Amendment to the Constitution.

(U) The limitations on NSA's ability to target, retain, and disseminate information on US persons stem from the U.S. Constitution. The Fourth Amendment protects all U.S. persons anywhere in the world from unreasonable searches and seizures by any person or agency acting on behalf of the US Government. The Fourth Amendment privacy protections are also afforded to everyone physically located within the United States and its territories regardless of citizenship or nationality.
(U//~~FOUO~~) Non-US persons who are visiting or living in the US are generally afforded privacy rights while they are located inside the US.
(U//~~FOUO~~) Elements of the intelligence community shall use the least intrusive collection techniques feasible within the United States or directed against US persons abroad.

(U//~~FOUO~~) Because the US SIGINT System (USSS) has the ability to acquire an extraordinary amount of communications, NSA/CSS personnel may encounter incidentally acquired US person information when searching for data about valid foreign intelligence targets. For that reason, the SIGINT system must be used in a way that satisfies the Fourth Amendment.

(U//~~FOUO~~) The documents we have reviewed in this module - E.O. 12333, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, and USSID SP0018 - create the foundation for the appropriate conduct of SIGINT activities. They grant the authorities necessary for providing critical foreign intelligence information, while instituting the controls that are essential to protect US person privacy rights as guaranteed by the US Constitution.

(U) The detailed instructions for implementing any of the authorities are beyond the scope of this course.

(U//~~FOUO~~) You can get guidance from the NSA Office of the General Counsel, SID's Office of Oversight and Compliance, your supervisor, and Intelligence Oversight Officer. Information and guidance in routine operations and much more can be found in these organizations' websites.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

(U) We now begin a series of questions to check your knowledge of material from this lesson.

(U) The knowledge checks are not a test, and scores are not recorded. They should serve as guides to you, to help you to see if there are any parts of the lesson which you should review.

(U) Good luck!

1. (U//~~FOUO~~) EO 12333 is a directive to provide for the effective conduct of United States _____ and the protection of _____. Please select the correct answer to fill in the blanks.

a. foreign policy; US persons abroad
b. intelligence activities; rights of US persons
c. military activities; American warfighters
d. domestic economic policy; US markets

(U//~~FOUO~~) The correct answer is b, "intelligence activities; rights of US persons."

2. (U//~~FOUO~~) Which document covers policies and procedures for the collection of foreign intelligence information, while regulating collection, processing, retention, and dissemination of US person information?

a. FISA
b. USSID SP0018
c. EO 12333
d. Classified Annex Authority

(U//~~FOUO~~) The correct answer is b, "USSID SP0018."

3. (U//~~FOUO~~) Which of these would NOT be considered a US person?

a. citizen of Kenya granted lawful permanent resident status in the US
b. corporation headquartered in Bahrain and incorporated in the US
c. woman born in Ohio, who lives in Belgium, but who retains US citizenship
d. Venezuelan citizen in Venezuela

(U//~~FOUO~~) The correct answer is d, "Venezuelan citizen in Venezuela."

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

(U//~~FOUO~~) In this lesson, you have seen how Executive Order 12333, and its related documents, permit and control actions taken in the collection of information by the US SIGINT System.

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

- Define and identify components of Executive Order 12333
- Identify implementing procedures--DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, and USSID SP0018

(U) Select Lesson 3 from the course menu.

Lesson 3 - Additional Authorities

(U) Welcome to the Additional Authorities lesson.

(U) This lesson will introduce you at a high level to authorizations required under Executive Order 12333 procedures. Foreign Intelligence Surveillance Act (FISA) authorities will be covered in the next lesson.

(U) At the conclusion of this lesson you will be able to identify the following Executive Order 12333 situations which may require additional authorization. Students will:

- (U//~~FOUO~~) Identify collection or targeting situations of US persons using consensual collection, using emergency procedures, or for foreign intelligence purposes
- (U//~~FOUO~~) Recognize retention procedures and limitations using destruction waivers

(U//~~FOUO~~) List procedures for the dissemination of:

- US person information based on imminent threat situations
- US Congressional personnel information
- Second Party person information
- Communications acquired through inadvertent surveillance which has been retained using a destruction waiver

(U//~~FOUO~~) You will also be able to recognize some instances which would require Incident Reporting.

(U) This lesson should take twenty minutes to complete.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

(U) With regard to authorities it is important to understand the differences between collection, processing, retention, and dissemination.

(U//~~FOUO~~) Some of NSA's authorities have applicable components under more than one of these functions, while others are specific to one function.

(U) Now let's dive right in and look at additional authorities for targeting US persons.

(U//~~FOUO~~) Communications of or concerning a US person may be intentionally intercepted under three circumstances.

- If the US person has signed a consent form (USSID SP0018, Annex H) and DIRNSA has approved collection.
- In hostage or threat-to-life or physical safety situations. (USSID SP0018 Section 4.1) or
- When targeting US persons for foreign intelligence purposes such as when the US person is acting as an agent or employee of a foreign power (FAA 703/704/705(b)). FISA/FAA authorities will be covered in the next lesson.

~~(S//SI//REL)~~ NSA is not permitted to engage in reverse-targeting. Reverse-targeting is collecting against an authorized target for the purposes of gathering information on a non-authorized target. For example, if an analyst is targeting badguy@provider.com in order to gather those communications with USbadguy@provider.com, this is not permitted because it is reverse-targeting.

(U//~~FOUO~~) A US person can authorize his or her foreign communications to be collected, and disseminated by NSA. This is commonly referred to as "consensual collection." SID's Office of Oversight and Compliance manages the process, Office of the General Counsel must review the consent form for legal sufficiency, and the Director or Deputy Director of NSA must approve an individual's request before collection can begin.

(U//~~FOUO~~) With DIRNSA approved consent, no further authority is required for collection. For detailed information about consensual collection, contact SID's Office of Oversight and Compliance through the alias, "DL Consensual."

(U//~~FOUO~~) If a US person located outside of the United States is reasonably believed to be held hostage or in imminent threat, there are two provisions where authorization for targeting can be granted.

- (U//~~FOUO~~) Under Classified Annex Section 4.A.1(a)(3) the Director of NSA or the Senior Operations Officer can authorize collection in hostage situations involving a foreign power or a group engaged in international terrorism. In such cases, NSA's Office of the General Counsel will notify the Attorney General of the authorization.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

- (U//~~FOUO~~) Under Department of Defense Regulation 5240.1-R Procedure 5 Section D.1.b. the Attorney General authorizes collection when a person's life or physical safety is reasonably believed to be in immediate danger. In an emergency, the Director of NSA or the Senior Operations Officer may authorize this collection for up to 72 hours. The NSA OGC will seek AG authorization to continue collection beyond 72 hours.

~~(S//SI//REL)~~ The targeting of non-US persons located inside the US is addressed in the Classified Annex Authority under Executive Order 12333. The Classified Annex Authority can be used in certain limited situations, including the limited continuation of targeting of non-US persons located in the United States.

(U//~~FOUO~~) A target is considered to be located inside of the United States when he or she is in US territory, airspace, or waters. If you have questions about targeting non-US persons inside the United States, [redacted] (b)(3)-P.L. 86-36 contact SID's Office of Oversight and Compliance.

(U//~~FOUO~~) During the course of collection, we may inadvertently intercept US Person data which must be destroyed or requires additional authority to retain. A destruction waiver waives the requirement to destroy the data.

(U//~~FOUO~~) (U//FOUO) Two individuals are empowered to sign destruction waivers: the Attorney General and the Director of NSA.

(U//~~FOUO~~) The Attorney General may waive the requirement to destroy electronic communications solely between persons located inside the United States if the contents indicate threat of death or serious bodily harm to any person.

(U//~~FOUO~~) The Director of NSA may approve destruction waivers to retain electronic communications with one or both ends located outside of the United States if the communication:

- contains significant foreign intelligence, or
- contains evidence of a crime or threat of death or serious bodily harm to any person, or
- reveals a potential vulnerability in US communications security.

(U//~~FOUO~~) For additional guidance on whether a destruction waiver applies to a given target circumstance, review the Destruction Waiver Template available on the Oversight and Compliance homepage, and contact SID's Office of Oversight and Compliance.

(U//~~FOUO~~) Rules regarding dissemination of inadvertently collected US person information depend on the situation. For example, in imminent threat to safety situations, NSA SIGINT

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

production personnel may disseminate the identity of the US person, other than those of Congressional members or staff, and must then notify SID's Office of Oversight and Compliance and Information Sharing Services.

(U//~~FOUO~~) For other non-imminent threat hostage situations, analysts must follow normal dissemination procedures. Note that a Blanket Dissemination Authority may be issued by the "USSID SP0018 Reporting and Dissemination Team" in Information Sharing Services.

(U//~~FOUO~~) All recipients must have a mission need for the US person identity.

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

(U//~~FOUO~~)

(U//~~FOUO~~) Requests for dissemination or retention of Signals Intelligence information about Congressional members or staff must be requested through NSA and approved by the Director of NSA or, depending on the requestor, the Director of National Intelligence.

(U//~~FOUO~~) As a matter of SID policy and in accordance with agreements between NSA and Second Party partners, Second Party persons - those from Australia, Canada, New Zealand, and Great Britain - are generally treated like US persons to the extent consistent with our national security interests. This applies to collection and targeting, processing, dissemination, and retention of communications of or about Second Party persons. For dissemination purposes, as a general rule, use generic terms to identify Second Party persons and organizations in serialized reports. Consult the US Identities in SIGINT Manual for specific procedures referencing Second Party identities in reports.

(U//~~FOUO~~) Second Party identities in SIGINT reports are not distributed to parties other than US users or the proper Second Party SIGINT headquarters. Information Sharing Services maintains distribution lists that identify Second Party recipients.

(U//~~FOUO~~) Any compliance incidents or violation of or contrary to Executive Order, Law, Regulation, or Directive must be reported.

(U//~~FOUO~~) Examples of such incidents include:

- Unintentional collection or dissemination of US person information
- Sharing unevaluated and unminimized (or raw) SIGINT outside of the SIGINT production chain
- Any other instance of unauthorized access to unevaluated and unminimized (or raw) SIGINT
- Unintentional collection and dissemination that occurs pursuant to FISA
- Any illegal, improper, or otherwise questionable activity not covered by the previous categories

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

(U//~~FOUO~~) Intelligence oversight programs and incident reporting ensure that NSA can conduct its foreign intelligence and counterintelligence missions while protecting the statutory and constitutional rights of US persons.

(U//~~FOUO~~) It is everyone's duty and responsibility to report questionable SIGINT activities that may involve information to, from, or about US persons.
(U//~~FOUO~~) Additional information regarding incident reporting can be obtained from SID's Office of Oversight and Compliance.

(U) We now begin a series of questions to check your knowledge of material from this lesson.

(U) The knowledge checks are not a test, and scores are not recorded. They should serve as guides to you, to help you to see if there are any parts of the lesson which you would do well to review.

(U) Good luck!

1. ~~(S//SI//REL)~~ _____ can approve a Destruction Waiver for inadvertently collected private radio communications between persons inside of the US and _____ can approve a Destruction Waiver for inadvertently collected foreign communications between US persons?

a. DIRNSA, Attorney General
b. Attorney General, DIRNSA

(U//~~FOUO~~) The correct answer is b, "Attorney General, DIRNSA."

2. ~~(S//SI//REL)~~ True or False: A non-US citizen, non-resident alien located in the US may be identified in SIGINT product.

a. True
b. False

(U//~~FOUO~~) The correct answer is True. See USSID SP0018.

(U//~~FOUO~~) You should now be able to:
(U//~~FOUO~~) Identify collection or targeting situations of US persons using consensual collection, using emergency procedures, or for foreign intelligence purposes
(U//~~FOUO~~) Recognize retention procedures and limitations using destruction waivers
(U//~~FOUO~~) List procedures for the dissemination of:

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

- US person information based on imminent threat situations
- US Congressional personnel information or
- Second Party person information

(U//~~FOUO~~) You should now also be able to recognize instances which would require Incident Reporting.

(U) Select Lesson 4 from the course menu.

Lesson 4 - FISA

(U//~~FOUO~~) In this lesson you will see how the Foreign Intelligence Surveillance Act (FISA) and its amendments, regulate certain actions taken in the collection of information by the US Signals Intelligence System.

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

- (U) Describe the purpose of FISA
- (U) List the 4 types of electronic surveillance defined by FISA
- (U) Distinguish between Section 702 and Sections 703, 704, and 705(b) of the FISA Amendments Act (FAA) of 2008
- (U//~~FOUO~~) Discriminate between how NSA uses FISA (to include FAA)
- (U) Identify whether Executive Order 12333 alone or additional FISA authorities are needed

(U) This lesson should take approximately twenty minutes to complete.

(U) In the 1970's the Church and Pike Committees investigated alleged abuses by the Intelligence Agencies. As a result of the activities unearthed, FISA was passed in 1978 to ensure the protection of privacy rights during the conduct of certain foreign intelligence collection activities.

(U) So what exactly is FISA?

(U) The Foreign Intelligence Surveillance Act, as enacted in 1978, is designed to regulate four specific categories of electronic surveillance which, in the judgment of Congress, were most likely to adversely impact privacy rights.

(U) FISA was most recently updated in July 2008.

(U) FISA (to include the FAA) establishes:

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

- Standards and definitions for electronic surveillance and physical search
- Two types of authorities (court orders and certifications)
- The US Foreign Intelligence Surveillance Court (FISC) and its jurisdiction
- The role of the Attorney General under FISA
- Emergency procedures for obtaining an authorization, and
- The requirement for minimization procedures

(U) In addition, FISA provides both judicial and Congressional oversight.

(U//~~FOUO~~) FISA defines four categories of electronic surveillance and requires FISC authorization before engaging in the following:

1) Collection against US persons located inside the United States

2) Collection off of a wire inside the United States with one end terminating in the United States

3) Collection of private domestic radio communications, or

4) Use of any other device from inside the United States for which a warrant would be required for law enforcement purposes

~~(S//SI//REL)~~ [redacted]

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

(U) Following the terrorist attacks of 9/11, Congress modified the FISA to grant the Intelligence Community additional authorities to protect national security.

~~(TS//SI//REL)~~ Most recently, the FISA Amendments Act (FAA) of 2008 provided a means under FISA to obtain the assistance of communications service providers to target non-US persons outside of the United States.

~~(TS//SI//REL)~~ FAA Section 702 applies to targeting non-US persons located outside of the United States using communications service providers to assist in the collection. More information on FAA Section 702 can be found in OVSC1203.

(U//~~FOUO~~) Other sections of the FAA (sections 703, 704, and 705(b)) apply to targeting US persons located outside of the United States and with limited exceptions require a FISA Court order regardless of the collection technique [redacted] (b)(3)-P.L. 86-36 Further information on FAA Sections 703, 704, and 705(b) can be found in OVSC1800.

((U//~~FOUO~~) NSA's standard minimization procedures are contained in USSID SP0018 but activity occurring pursuant to the FISA, to include FAA, is subject to FISC approved

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

minimization procedures. Each FISA authorization specifies the target set and the minimization procedures that must be followed.

(U//~~FOUO~~) Let's look at applying authorities for targeting.

(U//~~FOUO~~) We will look at applying Executive Order 12333, FISA Amendments Act Section 702, and FISA Amendments Act Sections 703, 704, and 705(b).

(U//~~FOUO~~) Section 1.7 (c) of Executive Order 12333, as amended, authorizes NSA to engage in SIGINT activities.

(U//~~FOUO~~) Executive Order 12333 is usually the only authority necessary when:

- the target is a non-US person and
- the target is located outside of the United States and
- the collection site or technique is located or used outside of the United States

~~(TS//SI//REL)~~ When the target is a non-US person, and the target is located outside of the United States, and the collection is effected with the assistance of a communications service provider, an FAA Section 702 certification may apply.

(U//~~FOUO~~) FISA Amendments Act Section 703, 704, and 705(b) Authorizations are required to engage in intentional, non-consensual collection against US Persons outside of the United States who are agents or employees of a foreign power.

(U//~~FOUO~~) When targeting a US person located outside of the United States, the type of collection will determine which type of FISA or FAA authority NSA must obtain.

((U) It is mandatory for anyone using data obtained under FISA to be trained properly.

(U//~~FOUO~~) NSA analysts are the first line of defense for preventing and reporting compliance incidents. Every analyst is required to self-report all recognized incidents. All incidents should be reported at the time they are detected, in order to reduce the impact of an incident and allow quick mitigation and determine if notice to the FISC is required.

(U//~~FOUO~~) Other SIGINT personnel who work to prevent violations or minimize damage from incidents include: auditors, mission managers, supervisors, and Intelligence Oversight Officers.

(U//~~FOUO~~) All SIGINT incidents and compliance incidents are reported to one or more external overseers, to include, but not limited to:

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

- The Foreign Intelligence Surveillance Court
- Congress
- The Assistant to the Secretary of Defense for Intelligence Oversight
- Office of the Director of National Intelligence
- The Department of Justice

(U) If you have questions that are not clearly covered in this course material, please contact the Office of the General Counsel and SID's Office of Oversight and Compliance.
(U) Remember, if you are not sure, it is best to ask.

(U) We now begin a series of questions to check your knowledge of material from this lesson.

(U) The knowledge checks are not a test, and scores are not recorded. They should serve as guides to you, to help you see if there are any parts of the lesson which you should review.

(U) Good luck!

1.(U) FISA and its amendments are NOT needed to authorize the intentional targeting of:

a. A US Person located in the United States
b. International radio communications between foreign communicants located outside the United States
c. A US Person located outside the United States
d. Collection from inside the US that requires a FISC order

(U) The correct answer is b, "International radio communications between foreign communicants located outside the United States."

2.(U//~~FOUO~~) True or False? FISA defines intentional acquisition by electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent to or from a known US person as electronic surveillance.

a. True
b. False

(U) The correct answer is True.

3.(U//~~FOUO~~) Which one of these modifies the Foreign Intelligence Surveillance Act (FISA)?

a. FISA Amendments Act
b. Stand Against Terrorism Act

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

(U) The correct answer is a, "FISA Amendments Act."

4. (U//~~FOUO~~) Which of these is required in order to conduct targeting under FAA 702 certifications? (Select all that apply)

a. 'Target X' is a non-US person
b. 'Target X' is located outside of the United States
c. Targeting is performed under an FAA Section 702 certification
d. All of the above

(U) The correct answer is d, "all of the above."

(U//~~FOUO~~) You have now completed the lesson. In this lesson, you have seen how FISA prescribes procedures related to electronic surveillance.

(U//~~FOUO~~) Much more information regarding FISA is available in other courses. Future courses relating to the FISA are also under development.

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

- Describe the purpose of FISA
- List the 4 types of electronic surveillance defined by FISA
- Distinguish between Section 702 and Sections 703, 704, and 705(b) of the FISA Amendments Act of 2008
- Discriminate between how NSA uses FISA, to include FAA
- Identify whether Executive Order 12333 alone or additional FISA authorities are needed

(U//~~FOUO~~) You have now completed the Overview of Signals Intelligence Authorities course. Be sure to look for links to the original documents, as well as documents which provide comparisons between the authorities.

(U//~~FOUO~~) As always, it is important to remember that SID's Office of Oversight and Compliance and the Office of the General Counsel are available to answer any specific questions you may have relating to these authorities. Remember that this is the Overview of Authorities course and does not replace training on specific FISA authorities.

(U//~~FOUO~~) SID's Office of Oversight and Compliance can be contacted by typing : 'go SV'

(U//~~FOUO~~) The Office of the General Counsel can be contacted by typing: 'go GC'

(U) This concludes the course.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401

Legal Readings

- AG 25 Information.doc
- DoD 52401R.pdf
- EO 12333 2008.pdf
- FISA 1978.pdf
- FISA Amendments Act of 2008.pdf
- Policy 1-23 29 May 09.pdf
- USSID AP2231
- USSID SP0002
- USSID CR1252
- ussidSP0018.pdf

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380401