

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR,
NZL//20291123~~



~~UNITED
STATES
SIGNALS
INTELLIGENCE
DIRECTIVE~~

USSID CR1610

(U) SIGINT PRODUCTION AND RAW SIGINT ACCESS

ISSUE DATE: 25 August 2005

REVISED DATE:

(U) OFFICES OF PRIMARY CONCERN (OPCs):

SIGINT Directorate (SID)
Oversight and Compliance (SV),
SIGINT Policy (S02L1), and
Customer Relationships Directorate, Information Needs Division (S111)

(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION

**(U) Topic of
Promulgation**

~~(U//FOUO)~~ This USSID prescribes policies and assigns authorities for determining what elements and persons are considered United States SIGINT System (USSS) "SIGINT production personnel," operating under Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). Such personnel are eligible for access to USSS raw SIGINT as well as SIGINT

Approved for Release by NSA on 09-19-2014, FOIA Case # 70809 (Litigation)

databases based upon assigned missions. This USSID delineates the procedures for attaining such accesses.

(U) USSID Edition (U//~~FOUO~~) USSID CR1610 replaces Signals Intelligence Directorate (SID) Directive 406, "SIGINT Production and Raw Traffic Access," dated 13 March 2003, which must be destroyed.

(U) Legal Protection of Sensitive Information (U//~~FOUO~~) This USSID contains sensitive information that is legally protected from release to any member of the public and is to be used only for official purposes of the NSA/CSS.

(U) Handling of USSID (U//~~FOUO~~) Users must strictly adhere to all classification and handling restrictions (see NSA/CSS Classification Manual 1-52) when:

- (U) storing hard or soft copies of this USSID, or
- (U) hyperlinking to this USSID.

(U//~~FOUO~~) Users are responsible for the update and management of this USSID when stored locally.

(U) Location of Official USSID (U//~~FOUO~~) The SIGINT Policy System Manager will maintain and update the current official USSID on NSA WEBWORLD (go USSID). As warranted, the USSID will be available on INTELINK.

(U) Access by Contractors and Consultants (U) **For NSA/CSS elements to include the SIGINT Extended Enterprise:**

(U//~~FOUO~~) United States SIGINT System (USSS) contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT Extended Enterprise are pre-authorized for access to USSIDs via NSANet, INTELINK, or in hard-copy formats as needed to perform their jobs. However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.

(U) Outside NSA/CSS elements:

(U//~~FOUO~~) Non-USSS contractors or consultants working at external facilities are pre-authorized for soft-copy access to USSIDs via NSANet or INTELINK, if connectivity to those systems is allowed by the contractor's NSA/CSS sponsor. Where such connectivity is not established, any hard-copy provision of USSIDs must be authorized by the SIGINT Policy System Manager (NSTS: 963-3593, [redacted])

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

**(U) Access by
Third Party
Partners**

(U) This USSID is not releasable to any Third Party partner.

(U) To request a shareable version:

- (U) Refer to USSID SP0002, Annex B (formerly USSID 2, Annex B); and
 - (U) Contact the appropriate Country Desk Officer in the Foreign Affairs Directorate.
-

**(U) Executive
Agent**

(U) The executive agent for this USSID is:

//S//
RICHARD J. QUIRK, III
Major General, USA
Signals Intelligence Director

(U) TABLE OF CONTENTS

(U) Sections

SECTION 1 - (U) PURPOSE AND SCOPE

SECTION 2 - (U) POLICY

SECTION 3 - (U) PROCEDURES

SECTION 4 - (U) RESPONSIBILITIES

SECTION 5 - (U) REFERENCES

SECTION 6 - (U) DEFINITIONS

(U) Annexes

**ANNEX A - (U//~~FOUO~~) RAW SIGINT DATABASE ACCESS
ADMINISTRATION**

**ANNEX B - (U//~~FOUO~~) RAW SIGINT DATABASE ACCESS
PROCEDURES FOR EXTENDED ENTERPRISE SIGINT PRODUCTION
PERSONNEL**

SECTION 1 - (U) PURPOSE AND SCOPE

- (U) USSID Scope**
- 1.1. (U//~~FOUO~~) This USSID will be used to identify personnel and activities comprising a USSS SIGINT Production Chain (SPC). Such identification constitutes eligibility for access to USSS raw SIGINT and SIGINT databases in support of assigned NSA/CSS SIGINT missions and tasks.
- 1.2. (U//~~FOUO~~) This USSID applies to all elements of the USSS, and to those non-USSS elements authorized to conduct SIGINT enabling, production, or oversight activities under DIRNSA/CHCSS authorities.
- 1.3. (U) USSS tactical commanders, who conduct SIGINT activities under delegated standing SIGINT Operational Tasking Authority (SOTA), are authorized to grant access to any organic tactical SIGINT databases as required to other USSS units or elements in accordance with USSS SIGINT policy and directives.
- 1.4. (U) This USSID predominantly addresses eligibility for access to national-level USSS raw SIGINT and SIGINT databases.

-
- (U) Content and Format**
- 1.5. (U) This USSID prescribes the policies and procedures for the determination of eligibility for access to USSS raw SIGINT and SIGINT databases.
- 1.6. (U) Annex A describes the administrative and oversight requirements for access to national-level raw SIGINT databases.
- 1.7. (U) Annex B describes the process NSA/CSS Extended Enterprise SIGINT Production personnel must use to request access to national-level raw SIGINT databases.

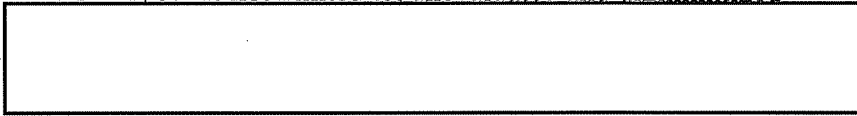
SECTION 2 - (U) POLICY

- (U) Policy**
- 2.1. (U//~~FOUO~~) Organizations and personnel that are assigned any SIGINT enabling, production, or oversight missions by DIRNSA/CHCSS or the SIGINT Director, and that are performing or managing associated SIGINT enabling, production, or oversight activities, including researching, developing, collecting, processing, analyzing, and reporting, are considered part of a SPC and are eligible for access to USSS raw SIGINT and SIGINT databases, as needed to support assigned SIGINT missions and tasks.

NOTE: ~~(C//SI//REL)~~ Raw SIGINT* is defined as any SIGINT acquired either as a result of search and development, or targeted collection operations

against a particular foreign intelligence target BEFORE the information has been evaluated for foreign intelligence AND minimization purposes. It includes, but is not limited to, unevaluated and unminimized

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



* This definition accommodates the most sensitive of the SIGINT disciplines - COMINT - but will not apply in its entirety to ELINT or Foreign Instrumentation Signals Intelligence (FISINT), where there is no expectation of privacy.

2.2. ~~(U//FOUO)~~ Any U.S. Government element assigned a valid SIGINT mission by DIRNSA/CHCSS or by the SIGINT Director must document the SIGINT enabling, production, or oversight activities in a unit USSID or in a site profile that is referenced in another USSID for field elements, or in a mission and activities statement for headquarters elements. Appropriate interim documentation, such as a NSA/CSS Staff Processing Form (SPF) will be sufficient in certain circumstances until such time as formal documentation is written and published.

2.3. ~~(S//SI//REL)~~ Per USSID SP0018, paragraph 6.2, "Access to raw SIGINT storage systems which contain identifiers of U.S. Persons must be limited to SIGINT production personnel." SIGINT production personnel are eligible for access as needed for and appropriate to their official duties. Before accessing or querying raw SIGINT databases, personnel must be briefed by the Office of General Council (OGC) on the Attorney General Minimization Procedures (USSID SP0018) that govern the handling of raw SIGINT and on relevant directives and Executive Orders.

2.4. ~~(C//REL)~~ SPC personnel accessing interactive raw SIGINT database systems will employ only those selection terms reasonably likely to produce foreign intelligence or foreign counterintelligence information in response to valid intelligence requirements levied in accordance with governing directives. Analysts will not employ selectors reasonably likely to result in the collection of U.S. or Second Party communications without appropriate authorization.

2.5. ~~(C//REL)~~ The use of a selection term designed to collect or select communications to, from, or about a U.S. person is prohibited without the prior written approval of the DIRNSA/CHCSS, the Attorney General, or the U.S. Foreign Intelligence Surveillance Court, as appropriate, in accordance with USSID SP0018, Section 4.

(U) Database Access Policy

2.6. ~~(U//FOUO)~~ SPC organizations and units requesting access to National-level raw SIGINT databases must employ fully indoctrinated personnel cleared for TOP SECRET (TS) Sensitive Compartmented Information (SCI) and operating in an approved SCI Facility (SCIF); and have a confirmed SIGINT mission, an approved dissemination plan, and an established and approved oversight mechanism that ensures proper handling of information at site within the SIGINT

production chain as well as a documented intelligence oversight reporting process.

2.7. (U//~~FOUO~~) SIGINT personnel at NSA/CSS Headquarters - Washington (NSAW) and at NSA/CSS Cryptologic Centers whose personnel security is already documented with CONCERTO and SEARCHLIGHT records may apply directly to the database Web sites for access, getting supervisor endorsement as needed. For purposes of security, oversight, and mission vetting, tactical elements hosted at these locations, and operating under tactical or dual tactical/national mission authorities, must submit applications for access in accordance with Annex B, paragraph B2.1, through paragraph B2.3.

**(U) Approval
Authorities**

2.8. (U//~~FOUO~~) The DIRNSA/CHCSS is the sole authority with Secretary of Defense (SECDEF) approval for the initial assignment of a SIGINT mission to a non-DoD element.

2.9. (U//~~FOUO~~) The SIGINT Director, SID Chief of Staff, SID Deputy Directors, and the SID Associate Deputy Director for SIGINT Development may assign initial or additional national SIGINT missions to established USSS elements or new SIGINT missions to non-USSS elements of the NSA/CSS.

a. (U//~~FOUO~~) The Deputy Director for Customer Relationships (DD/CRD) may assign a SIGINT mission for SIGINT product and service dissemination activities.

b. (U//~~FOUO~~) The Deputy Director for Analysis and Production (DD/A&P) may assign a SIGINT mission for SIGINT analysis and production, dissemination for analytic collaboration activities, and SIGINT Development relevant to A&P missions.

c. (U//~~FOUO~~) The Deputy Director for Data Acquisition (DD/DA) may assign a SIGINT mission for SIGINT collection or exploitation activities, and for SIGINT Development activities relevant to DA missions.

d. (U//~~FOUO~~) The Associate Deputy Director for SIGINT Development (ADD/SIGDEV) may assign a SIGINT mission for SIGINT Development relevant to the USSS.

SECTION 3 - (U) PROCEDURES

**(U//~~FOUO~~) Access
to National-Level
USSS Raw
SIGINT Databases**

3.1. (U//~~FOUO~~) The process for submitting requests for national-level USSS raw SIGINT database access is dependent upon the requester's unit/element, assignment, and the individual database requirements.

3.2. (U//~~FOUO~~) Requesters located at an NSAW location should follow the

procedures found on the respective database Web pages available on NSANet. Requesters located at NSA/CSS Cryptologic Centers outside the Washington area should also follow the procedures found on the respective database Web pages available on NSANet, though forms will be processed by the on-site oversight and compliance personnel or representatives.

3.3. (U//~~FOUO~~) All other requesters outside the elements noted in paragraph 3.2. should follow the procedures delineated in Annex B.

~~(U//FOUO)~~
**Traditional
SIGINT
Production
Elements**

3.4. (U//~~FOUO~~) A USSS element, hereafter identified as "traditional," is any element whose fundamental purpose is SIGINT production. A traditional element is, from its inception, assigned a SIGINT production or intelligence oversight mission, hereafter referred to as a "SIGINT mission." Those personnel assigned to traditional elements are inherently part of a SPC and, therefore, eligible for access to appropriate raw SIGINT databases. The following elements are considered traditional:

a. (U//~~FOUO~~) NSA SIGINT Directorate, NSA SIGINT/Information Assurance Centers, and NSA/CSS Cryptologic Center elements with a SIGINT mission.

b. (U//~~FOUO~~) USSS National Field Site elements [redacted] with a SIGINT mission.

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

c. ~~(S//SI//REL)~~ [redacted] with a SIGINT mission.

d. ~~(C//REL)~~ Active Duty Service Cryptologic Organizations (SCOs) or Service Cryptologic Elements (SCEs) [redacted]

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

[redacted] with assigned SIGINT missions).

e. (U//~~FOUO~~) Service Partner (SP) tactical SIGINT elements - DoD tactical SIGINT units not assigned to an SCE/SCO - with assigned SIGINT missions.

f. (U//~~FOUO~~) DoD Reservist and National Guard elements assigned to a SIGINT unit/element and working an approved SIGINT mission.

g. ~~(C//REL)~~ Second Party partner SIGINT elements [redacted]. This includes U.S. persons integrated into Second Party partner SIGINT elements. Additional oversight requirements may be required, including any additional requirements of the Second Party partners, if integrated U.S. SIGINT personnel require access to data not already accessible by the Second Party.

h. ~~(C//REL)~~ Integrated personnel (integrees) from Intelligence Community

partners and customers and/or other organizations who are assigned to SIGINT elements or who are operating under DIRNSA/CHCSS SIGINT authorities in accordance with approved documented agreements (Memoranda of Understanding (MOUs)/Memoranda of Agreement (MOAs)).

i. (U//~~FOUO~~) NSA/CSS contractors who are assigned to SIGINT production elements and who operate under DIRNSA/CHCSS authorities (with contractual documentation).

(U//~~FOUO~~) Non-traditional SIGINT Production Elements

3.5. (U//~~FOUO~~) A number of NSA/CSS and external elements have been assigned SIGINT enabling or production missions by DIRNSA/CHCSS, even though their primary mission is not SIGINT production. (See paragraph 2.8., Approval Authorities). These entities are hereafter identified as "non-traditional" SIGINT production elements. When assigned SIGINT missions by DIRNSA/CHCSS, and when appropriate oversight channels have been established, these elements become part of the USSS. Personnel performing SIGINT enabling or production activities within these elements then become part of a SPC, and are therefore eligible for access to appropriate national-level raw SIGINT databases:

a. (U//~~FOUO~~) NSA/CSS Representatives (NCRs) and their staffs.

b. (U//~~FOUO~~) Cryptologic Services Groups (CSGs) and Cryptologic Services Teams (CSTs) including those employed as integral parts of National Intelligence Support Teams (NISTs).

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

c. (U//~~FOUO~~) Special U.S. Liaison Officers (SUSLOs) to Second Party SIGINT partners.

d. (U//~~FOUO~~) Research Associate Directorate (RAD), Information Assurance Directorate (IAD), SIGINT System Acquisition project/program personnel, and other elements supporting SIGINT missions.

NOTE 1: (U//~~FOUO~~) Given the distinct and ever-changing nature of research and development efforts, to adequately support SIGINT missions, RAD may require large volumes of, and differing accesses to, SIGINT information and raw SIGINT more so than other SIGINT enablers.

NOTE 2: (U//~~FOUO~~)

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

e. (U//~~FOUO~~) NSA/CSS contractors who are performing SIGINT enabling under DIRNSA/CHCSS authorities (with contractual documentation).

f. (U//~~FOUO~~) Other U.S. Government Executive Branch elements to whom DIRNSA/CHCSS has assigned, with SECDEF approval, SIGINT missions.

(U//~~FOUO~~) Non-SIGINT Production Elements

3.6. (U//~~FOUO~~) Unless specifically authorized by exception, personnel working in or for the following elements are not generally part of an SPC as they do not typically work under DIRNSA/CHCSS SIGINT authorities. Exceptions to this rule are made only under special circumstances and must be approved by DIRNSA/CHCSS or the SIGINT Director. (See paragraph 2.8., Approval Authorities).

a. (U) NSA/CSS Associate and Principal Directorates, unless directly enabling a SIGINT mission. See paragraph 3.5.d. for common exceptions.

b. (U) Customer organizations hosting NSA/CSS integreees operating under the host's authorities.

c. (U//~~FOUO~~) Other agencies' liaison personnel when assigned to NSA/CSS in a liaison rather than an integreee capacity, when the liaison is not working under DIRNSA/CHCSS authorities.

d. (U//~~FOUO~~) Non-SIGINT customer organizations (e.g., Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA); and non-SIGINT components of NSG, Marine Support Battalions, U.S. Coast Guard, INSCOM, and AIA), unless collaborating on SIGINT missions and operating under DIRNSA/CHCSS authorities.

e. (U//~~FOUO~~) Department of Defense, Department of Homeland Security, or Intelligence Community all-source intelligence organizations (e.g., joint/combined or interagency all-source intelligence centers), unless collaborating on SIGINT missions and operating under DIRNSA/CHCSS authorities.

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

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

(U//~~FOUO~~)

3.7. (C//REL)

[Redacted content for 3.7]

3.8. (C//REL)

[Redacted content for 3.8]

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

SECTION 4 - (U) RESPONSIBILITIES

(U) DIRNSA/CHCSS 4.1. (U//~~FOUO~~) DIRNSA/CHCSS shall assign or approve a request for a new SIGINT mission to any non-NSA/CSS element.

(U) SIGINT
Director

4.2. (U//~~FOUO~~) The SIGINT Director or his delegated authority shall:

- a. (U//~~FOUO~~) Assign or approve a request for a new SIGINT mission to an established USSS or non-USSS element of the NSA/CSS.
- b. (U//~~FOUO~~) Define specific activities for that SIGINT mission.
- c. (U//~~FOUO~~) Direct dissemination and accountability of SIGINT products.
- d. (U//~~FOUO~~) Certify that proper intelligence oversight is in place.
- e. (U//~~FOUO~~) Document the SIGINT Production mission.

(U) SIGINT
Production
Elements

4.3. (U//~~FOUO~~) Authorized SIGINT production elements as identified in paragraph 3.4. shall:

- a. (U//~~FOUO~~) Document and adhere to the database administration and intelligence oversight provisions noted in Annex A.
- b. (U//~~FOUO~~) Document and adhere to general intelligence oversight procedures.
- c. (U//~~FOUO~~) Document a request for any additional resources needed to conduct the assigned SIGINT mission using the process described in Annex B, if external to NSA or NSA/CSS Cryptologic Centers.

SECTION 5 - (U) REFERENCES

(U//~~FOUO~~) USSID
SP0018

5.1. (U//~~FOUO~~) **Legal Compliance and Minimization Procedures**, dated 27 July 1993. This document prescribes the policies and procedures and assigns responsibilities to ensure that the missions and activities of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons. paragraph 6.2. states that access to raw SIGINT storage systems that contain identities of U.S. persons must be limited to

SIGINT production personnel.

(U//~~FOUO~~) Executive Order 12333, as amended 5.2. **(U//~~FOUO~~) United States Intelligence Activities**, dated 4 December 1981, as amended. This order states that the Intelligence Community agencies shall, in accordance with applicable United States law and with the other provisions of the order, conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

(U//~~FOUO~~) NSCID No. 6 5.3. **(U//~~FOUO~~) National Security Council Intelligence Directive (NSCID) Signals Intelligence**, dated 17 February 1972. This directive mandates that activities pertaining to SIGINT must be organized and managed so as to exploit to the maximum the available resources of the Government, to satisfy the intelligence needs of the National Security Council and the departments and agencies of the Government, and to provide for efficiency and economy in the use of technical resources.

(U//~~FOUO~~) Department of Defense (DoD) Directive 5100.20 5.4. **(U//~~FOUO~~) The National Security Agency and the Central Security Service**, dated 23 December 1971. This directive prescribes authorities, functions, and responsibilities of the NSA/CSS, and states that the SIGINT resources of the Department of Defense will be structured to accomplish most efficiently and effectively the SIGINT mission of the United States.

(U) National Cryptologic Doctrine 5.5. **(U//~~FOUO~~) Signals Intelligence Cryptologic Publications (CPs) 2.0, 2.1, 2.2, and 2.3**; dated 1 August 2004. These documents provide national cryptologic doctrine for the United States SIGINT mission, and offer additional details regarding the relationship between the NSA/CSS, the USSS, and the Service elements.

(U//~~FOUO~~) SID Management Directive Number 411, USSS Governance 5.6. **(U//~~FOUO~~) SID Management Directive Number 411, USSS Governance**, dated 19 November 2004. This management directive documents the governance of the USSS as a single global enterprise.

(U) DoD Regulation 5240.1-R 5.7. **(U) Activities of DoD Intelligence Components that Affect U.S. Persons**, dated December 1982.

(U) NSA/CSS Policy 1-23 5.8. **(U) Procedures Governing NSA/CSS Activities that Affect U.S. Persons**, dated 11 March 2004.

- (U//~~FOUO~~)
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.
- 5.9. (U//~~FOUO~~) Sections 1801-1811, Title I, **Electronic Surveillance within the United States for Foreign Intelligence Purpose**; and Sections 1821-1829, Title III, **Physical Searches within the United States for Foreign Intelligence Purpose.**
-
- (U) **NSA/CSS Policy 1-60**
- 5.10. (U) **NSA/CSS Office of the Inspector General**, dated 6 July 2005.
-
- (U) **NSA/CSS Personnel Management Manual, Chapter 366**
- 5.11. (U) **Personal Conduct**, dated 14 August 2001.
-
- (U) **NSA/CSS Policy 2-14**
- 5.12. (U) **Signals Intelligence Dissemination**, dated 13 September 2004.
-
- (U) **USSID CR1611(P)**
- 5.13. (U) **SIGINT Dissemination for Analytic Collaboration**, dated 13 September 2004.
-

SECTION 6 - (U) DEFINITIONS

- (U) **Foreign Intelligence**
- 6.1. (U//~~FOUO~~) Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons.
-
- (U) **Local-level Raw SIGINT Database**
- 6.2. (U) A raw SIGINT database that is generally accessible only to SIGINT Production Chain personnel of one specific NSA/CSS element and serves a narrow analytic purpose.
-
- (U) **Minimization**
- 6.3. (U//~~FOUO~~) Specific SIGINT procedures that, considering the purpose and technique of the particular surveillance, lessen the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. Persons consistent with the U.S. need to obtain, produce, and disseminate foreign intelligence and counterintelligence information.
-
- (U) **National-Level Raw SIGINT Databases**
- 6.4. (U//~~FOUO~~) Databases that serve as the repositories for raw SIGINT that is derived from USSS and foreign SIGINT partner collection against national intelligence priorities. These databases are generally accessible to all SIGINT Production Chain personnel and serve a broad analytic purpose.
-

**(U) NSA/CSS
Extended
Enterprise (Field)**

6.5. (U//~~FOUO~~) NSA/CSS personnel and facilities at locations other than NSAW.

(U) Raw SIGINT

6.6. (~~C//SI//REL~~) Raw SIGINT is any SIGINT acquired either as a result of search and development, or targeted collection operations against a particular foreign intelligence target BEFORE the information has been evaluated for foreign intelligence AND minimization purposes. It includes, but is not limited to,



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

NOTE: (~~C//SI//REL~~) After data has been minimized and has been determined to constitute foreign intelligence, it can then be considered "native format" SIGINT or Evaluated and Minimized SIGINT (EMT) and is eligible for release in accordance with approved SIGINT dissemination means and processes established by policies governing SIGINT production.

**(U) Service
Cryptologic
Elements (SCEs)**

6.7. (U//~~FOUO~~) The term Service Cryptologic Elements has evolved to designate the military cryptologic organization(s) comprising the CSS. There are five service elements - Army, Marine Corps, Navy, Air Force, and the Coast Guard - that comprise the CSS.

**(U) Service
Cryptologic
Organizations
(SCOs)**

6.8. (U//~~FOUO~~) References in paragraph 5.3 and paragraph 5.4 direct that the SIGINT activities previously performed by the Military Departments, referred to as Service Cryptologic Organizations, be organized into a Central Security Service.

6.9. (U//~~FOUO~~) Currently, based on governing directives, the three major commands within the Military Departments responsible for CSS personnel are:



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

**(U) Service
Partners (SPs)**

6.10. (U//~~FOUO~~) Military and Coast Guard (non-SCE) personnel, when performing SIGINT operations under authorities delegated by DIRNSA/CHCSS are considered members of the USSS. These mostly tactical units are more properly recognized as Service Partners.

**(U) SIGINT
Enabling Activities**

6.11. (U//~~FOUO~~) Any activity, technique, or technology that facilitates the exploitation of a SIGINT target. Such activities include research, development, acquisition (program or project development), and direct management.

**(U) SIGINT
Oversight
Activities**

6.12. (U//~~FOUO~~) Those activities conducted by the Office of the Inspector General (OIG), the OGC, and SID Oversight and Compliance (O&C) designed to ensure the proper handling and intelligence oversight of SIGINT data.

-
- (U) SIGINT Mission** 6.13. (U//~~FOUO~~) A SIGINT mission is any assignment that requires performance of activities to enable, produce, or oversee SIGINT production for a foreign intelligence or counterintelligence purpose. Personnel conducting such activities, by virtue of their assignments, are eligible for access to national-level raw SIGINT databases under the presumed requirement inherent in SIGINT missions.
-
- (U) SIGINT Production Chain (SPC)** 6.14. (U//~~FOUO~~) Any combination of organizations or personnel performing SIGINT enabling, production, or intelligence oversight activities against the same intelligence target. These elements are authorized to access or share raw SIGINT in support of assigned SIGINT missions only with individuals within their particular SPC. There is no single SPC; rather, there are many, each working distinct SIGINT missions assigned by the DIRNSA/CHCSS.
-
- (U) SIGINT Production Activities** 6.15. (~~C//SI//REL~~) Any activity, technique, or technology that facilitates the exploitation of a SIGINT target. Such activities include, but are not limited to, the following: SIGINT development, signals collection, collection management, data processing, cryptanalysis, language processing, minimization and evaluation, retention, analysis, reporting, and dissemination, and the overall management thereof.
-
- (U) Special Cryptologic Partner (SCP)** 6.16. (U//~~FOUO~~) Refers to the special cryptologic partnership between NSA/CSS and the U.S. Special Operations Command (USSOCOM). The establishment of this partnership improves SID and IAD abilities to support USSOCOM tactical requirements, while improving USSOCOM abilities to support NSA/CSS cryptologic requirements. The SCP arrangement provides for the integration of a USSOCOM liaison office at NSA/CSS Headquarters.
-
- (U) Support Organization** 6.17. (U) Any organization that provides for the technical health and maintenance of a raw SIGINT database.
-
- (U) United States SIGINT System (USSS)** 6.18. (U//~~FOUO~~) U.S. Government SIGINT activities worldwide under the direction of DIRNSA/CHCSS. The USSS comprises the NSA/CSS SIGINT Directorate, the SIGINT functions and elements of the military departments, and other governmental elements authorized to perform SIGINT activities under DIRNSA/CHCSS authorities.
-
- (U) User Organization** 6.19. (U) Any organization that has personnel who have been approved for access to raw SIGINT databases.
-

USSID CR1610

ANNEX A - (U//~~FOUO~~) NATIONAL-LEVEL RAW SIGINT DATABASE ACCESS ADMINISTRATION

SECTION 1 - (U) PURPOSE

(U) Purpose and Applicability

A1.1. (~~C//REL~~) This annex establishes procedures and assigns responsibilities to ensure that USSS raw SIGINT database systems and any other similar text retrieval systems used to access or search raw SIGINT are operated in accordance with applicable law, executive branch directives and orders, and Department of Defense (DoD) and NSA/CSS policy regulations and directives with proper procedural safeguards to protect the rights and privacy of U.S. persons.

A1.2. (~~C//SI//REL~~) The policy set forth in this annex applies to all users of interactive raw SIGINT databases or similar systems. It also applies to data downloaded from interactive raw SIGINT database systems to any other derivative database(s) when the downloaded data can be further manipulated for SIGINT-related production searches.

A1.3. (U//~~FOUO~~) This policy is also applicable in the use and/or development of any USSS system or tool that incorporates raw SIGINT.

A1.4. (U//~~FOUO~~) Restrictions on the use of the raw SIGINT database system and other similar systems set forth in this annex are intended to augment existing regulations and procedures governing SIGINT operations of the USSS and will take precedence over other USSS database access policies.

(U) Applicability

A1.5. (~~C//REL~~) The provisions set forth in this Annex apply to both national-level and local raw SIGINT databases through which users conduct keyword searches



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

SECTION 2 - (U) PROCEDURES

(U) Requirements for Users

A2.1. (U//~~FOUO~~) Prior to obtaining access to an interactive raw SIGINT database (for details and distinctions, see Section 6, Definitions, contained herein), users shall:

- a. (U//~~FOUO~~) Have received a USSID SP0018/Database Access briefing provided by OGC and SID O&C within the last two years and have on file,

with O&C, a current signed "Agreement for Users of Raw SIGINT Database Systems" (attached hereto); and

b. (U//~~FOUO~~) Read USSID CR1610, "SIGINT Production and Raw SIGINT Access" and its annexes.

A2.2. (U//~~FOUO~~) The user organization will ensure that personnel requesting accounts are included in the regularly scheduled USSID SP0018 briefings offered by OGC and O&C. If there are many account requests, arrangements for a separate USSID SP0018 briefing can be made through O&C. The originating organization will maintain account requests, justifications, and access approvals.

**(U//~~FOUO~~)
Oversight &
Compliance
Approval**

A2.3. (U//~~FOUO~~) Most national-level raw SIGINT databases are generally accessible to all SIGINT Production Chain personnel and serve a broad analytic purpose. Access request forms and procedures for these databases must be approved by O&C prior to their use and application and are generally found on the database's respective NSANet web page. O&C must also review and approve any access requests for these databases. In some cases, approval must be sought from SID senior management for accesses. Access request procedures are provided in Annex B.

A2.4. (U//~~FOUO~~) Local-level raw SIGINT databases are generally accessible only to SIGINT Production Chain personnel of one specific NSA/CSS element and serve a narrow analytic purpose. Access request forms, procedures, and review for these databases are established by the user organization and must be approved by O&C prior to their use and application. All databases, regardless of location or user, are subject to the same intelligence oversight requirements as NSA/CSS databases housing like data. Local-level raw traffic databases should have their oversight mechanisms vetted through SID Oversight and Compliance prior to system operation. Access requests for these databases must be reviewed and approved by the user organization in accordance with the guidelines in this USSID.

A2.5. (U//~~FOUO~~) The user will be notified by the database support organization, or the user organization when self-supported, when the access account is created.

(U) When Access is No Longer Needed A2.6. (U//~~FOUO~~) Upon determining that a user will no longer require access to raw SIGINT, the user organization will immediately notify O&C, which then will instruct the appropriate support organization to remove the user's account.

**(U) User
Reassignments**

A2.7. (U//~~FOUO~~) If a person is reassigned to another USSS organization and needs to retain access to a general access interactive database, the person, through his or her new management, may submit a rejustification in an account request to O&C, with new justification and auditor information as it applies to the person's new job. To avoid an interruption in access, this can be done prior to the person's reassignment, provided the effective date for the new job is included in the

request.

**(U) Inactive
Accounts**

A2.8. (U//~~FOUO~~) The support organization will suspend, without prior written notice, any account that has been inactive for a period of 90 days. The support organization will subsequently notify the user organization, which will then initiate action either to close the account or provide the support organization a reason for maintaining the account in an active status.

**(U) Auditing
Requirements**

A2.9. (U//~~FOUO~~) User organizations are responsible for designating a primary and a secondary auditor to review daily the queries made on the interactive raw SIGINT databases by personnel assigned to their organization. These auditors must be branch level or above or be a senior analyst knowledgeable of the target. Auditors for military SIGINT elements must be at least a second echelon manager, and must be at least one echelon higher than the person being audited. New auditors are required to have had a USSID SP0018 briefing within the last year and attend O&C's auditor responsibilities training. Alternatively, if time permits, new auditors may meet with O&C personnel and receive an interim auditor responsibilities briefing prior to assumption of auditing duties. Frontline auditors are the SIGINT Director's designees for compliance with USSID SP0018, Section 5 through the daily audit of selection terms used for interactive raw SIGINT database retrievals.

A2.10. (U//~~FOUO~~) Oversight and Compliance will provide training for new auditors on their responsibilities; will visit frontline auditor organizations to promote understanding of auditor and analyst responsibilities, answer questions and ensure compliance with USSID SP0018, this USSID, and its references; will conduct a periodic super audit of all interactive raw SIGINT database systems; and, will provide the NSA/CSS OGC and the NSA/CSS OIG with a report detailing USSID SP0018 incidents incurred during the use of the systems.

A2.11. (U//~~FOUO~~) The support organizations will provide each database user with a full-screen reminder of USSID SP0018 requirements with every log-on.

(U) Audit Files

A2.12. (U//~~FOUO~~) For audit purposes, the support organizations will maintain a non-editable system file of all interactive raw SIGINT database queries for a minimum of one year. They will also maintain a 120-day on-line record of the above referenced queries. The support organizations will ensure that the designated auditor forwards audits of system queries to the user organizations on a daily basis for organizational review. All organizations will retain the reviewed audit trails of the interactive raw SIGINT database queries for a minimum of 120 days. These records will be available to the NSA/CSS Office of the Inspector General upon request.

**(U//~~FOUO~~) On-
going Review**

A2.13. (U//~~FOUO~~) Review of selection terms is an essential part of ensuring compliance with USSID SP0018 requirements designed to ensure the

constitutionality and legality of NSA/CSS operations with respect to protecting privacy interests of U.S. persons. Access to raw SIGINT databases occurs through an interactive retrieval system, which enables users to construct queries from individual terminals and apply them on-line against any database of raw SIGINT. When conducting retrievals, users will comply with the following procedures:

- a. (U//~~FOUO~~) Each interactive query against raw SIGINT databases will be driven by a foreign intelligence or foreign counterintelligence purpose, and will take reasonable measures to eliminate the collection of U.S. and Second Party communications.
- b. (U//~~FOUO~~) Each interactive request will create an audit record of the selection terms used that will be reviewed on a daily basis by the originating organization and maintained as detailed in paragraph A2.12. These audit records must also be provided to O&C for review.
- c. (U//~~FOUO~~) Whenever doubt exists regarding whether use of a particular selection term would be consistent with the requirements of USSID SP0018, an analyst should consult with his or her supervisor, auditor, or O&C prior to use of the particular selection term.

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

(U//~~FOUO~~) Sensitive Information Categories

A2.14. (U//~~FOUO~~) The NSA/CSS OGC may designate specific categories of queries as containing sensitive information.



(U) Incident Reporting

A2.15. (U//~~FOUO~~) The auditor/analyst will report through their organizational chain to SID O&C any use of a U.S. selection term or use of selectors that intentionally or inadvertently collect communications to, from, or about U.S. persons, or selectors with no foreign intelligence or foreign counterintelligence purpose discovered by user organizations during daily review of the audits. O&C will evaluate the incident and, if necessary, prepare a report to the NSA/CSS OIG and the OGC. If an incident is reported to the NSA/CSS OIG and OGC, SID O&C will alert the organization involved and that organization is responsible for including the incident in their organization's input to the NSA/CSS IG Quarterly Report which details NSA/CSS's compliance with Executive Order 12333, as amended, USSID SP0018, and related directives.

(U) Annual Reviews of Terms

A2.16. (U//~~FOUO~~) User organizations are also responsible for the annual review of selection terms. All violations and suspected violations of U.S. person's privacy rights discovered during this annual review will be reported immediately upon recognition to SID O&C, which will be responsible for detailing the incident to the NSA/CSS OIG and OGC. Document referenced in paragraph 5.9., document referenced in paragraph 5.12., and document referenced 5.13. (listed below) require that all violations or suspected violations of documents

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

referenced in paragraph 5.7. through paragraph 5.11. shall be reported immediately to the NSA/CSS OIG for investigation and recommended corrective action, and to the OGC.

(U) Availability of Records A2.17. (U//~~FOUO~~) Audit records, supervisory reviews, and samples of products generated using raw SIGINT database systems will be made available upon request to the OGC and the Office of Intelligence Policy and Review of the Department of Justice for periodic review. Violations or suspected violations discovered during a periodic review by the Office of Intelligence Policy and Review of the Department of Justice, in conjunction with the OGC, will be reported immediately upon recognition to the OIG.

SECTION 3 - (U) USER AGREEMENT

(U) AGREEMENT FOR USERS OF INTERACTIVE RAW SIGINT DATABASE SYSTEMS

1. (~~C//REL~~) The use of a selection term designed to collect communications to, from, or about U.S. persons is prohibited without the prior written approval of the DIRNSA/CHCSS, the Attorney General, or the U.S. Foreign Intelligence Surveillance Court, as appropriate, in accordance with USSID SP0018, Section 4.
2. (U//~~FOUO~~) There are stringent restrictions regarding generation of selection terms and serious potential legal consequences for failure to observe these restrictions. Users will retrieve information from interactive raw SIGINT database systems only in accordance with the provisions of Annex A to this USSID. User organizations will review raw SIGINT database audit trails to ensure compliance with this USSID and appropriate governing authorities, including Executive Order 12333, as amended, NSA/CSS Policy 1-23, and USSID SP0018. Any evidence of unauthorized or improper retrievals will be reported to SID Oversight and Compliance, which will be responsible for reporting to the NSA/CSS Office of General Counsel and to the NSA/CSS Office of Inspector General for a determination of appropriate action. Any potential violation of this document and appropriate governing directives may result in withdrawal of access to such databases until the issue is resolved.
3. (U//~~FOUO~~) Executive Order 12333, as amended, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, and USSID SP0018 establish policy and procedures for safeguarding the rights of U.S persons and are fully applicable to data contained in raw SIGINT database systems and to the use of text retrieval systems.
4. (~~C//SI//REL~~) I acknowledge that I have read and understand the policies and responsibilities outlined in this USSID, Annex A to this USSID, and the references therein. I agree to abide by these restrictions on retrieval of data from

any interactive raw SIGINT database system. I acknowledge that a foreign intelligence purpose must exist for the timeframe searched in all queries.

Signature

Date

NAME:

ORGANIZATION:

EMPLOYMENT STATUS (e.g., integree, contractor, NSA Civilian/Military):

NSANet SID:

CURRENT INTERACTIVE RAW SIGINT DATABASE ACCESS(ES):

DATE OF LAST USSID SP0018 BRIEFING:

PRIMARY AUDITOR'S NAME:

SECONDARY AUDITOR'S NAME:

PRIVACY ACT STATEMENT

(U) This statement is provided in compliance with the provisions of the Privacy Act of 1974 (P.L. 93-579, 5 U.S.C 552a), which require Federal agencies to inform individuals of the following facts concerning requested information:

~~(C//REL)~~ PRINCIPAL PURPOSE: To identify users of interactive raw SIGINT database, or similar, systems.

~~(C//REL)~~ ROUTINE USE: Maintenance of record of authorized users of interactive raw SIGINT database, or similar, systems.

~~(C//REL)~~ DISCLOSURE OF INFORMATION: Voluntary. If the individual does not provide the above requested information, access to interactive raw SIGINT database, or similar, systems may be denied.

(U) AUTHORITY: P.L. 86-36 reprinted in 50 U.S.C. 402 (Note), E.O. 12333, as amended, reprinted in 50 U.S.C. 401 (Note).

USSID CR1610
ANNEX B - (U//~~FOUO~~) RAW SIGINT DATABASE ACCESS

PROCEDURES FOR EXTENDED ENTERPRISE SIGINT PRODUCTION PERSONNEL

SECTION 1 - (U) PURPOSE

- (U) Purpose** B1.1. (U) To establish processes and procedures to efficiently grant accesses to raw SIGINT databases to personnel performing SIGINT missions within the NSA/CSS Enterprise.
- (U) Applicability** B1.2. (U) The processes described herein are applicable to all SIGINT Production Chain personnel assigned to NSA/CSS Extended Enterprise locations, including tactical elements hosted at NSAW or NSA/CSS Cryptologic Centers, and operating under tactical or dual tactical/national mission authorities.
-

SECTION 2 - (U) PROCEDURES

- (U) New Requests** B2.1. (U//~~FOUO~~) Initial requests for database access for a proposed or existing SIGINT Production organization other than those covered in paragraph 2.7. of this USSID require the completion of a new request form, which can be found at the "Request for Access to Raw SIGINT Database" webpage, available through the SIGINT Contact Center (SCC) web page by typing "go scc" in the URL window of your Web browser. Any organization or unit making an initial application must have the elements listed in paragraph 2.6. of this USSID completely vetted prior to gaining access. Information about completing these requirements can be found at the "How Do I Request Access to National-Level SIGINT Raw SIGINT Database?" webpage.
- (U) New Databases** B2.2. (U//~~FOUO~~) Existing Missions. If the requester requires a new database in support of a previously approved mission, a new request must be submitted. The requester may insert mission and oversight details from the previous request; however, the requester must confirm that the mission, location, and oversight details entered into the application are correct and up to date. References to a prior request will not be accepted.
- (U) New Personnel** B2.3. (U//~~FOUO~~) New personnel who are assigned to an organization or unit that is already approved for certain SIGINT production responsibilities need only meet the personnel security and USSID SP0018 requirements to gain accesses to raw
-

SIGINT database(s) already approved for that location. However, all questions in the request form must be complete to confirm that the details are accurate and up to date. The original request that established the unit's authorization for the mission and accesses may be replicated to the extent that it is still accurate.

SECTION 3 - (U) SIGINT CONTACT CENTER PROCESS

(U) SUMMARY OF PROCEDURES

(U) Summary of Procedures B3.1 (U) The procedures table below summarizes the SIGINT Contact Center (SCC) process for requesting access to raw SIGINT databases. More detailed information follows.

(U) PROCEDURES TABLE

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

STEPS	POC	ACTIVITY
1	Requester	Submits a request for access to the SCC through the " <u>Request for Access to Raw SIGINT Databases</u> " website. In addition to submitting this request, requestors will use existing or new NSANet accounts to visit each individual website and apply for that specific database.
2	SCE, Sponsor, Customer Liaison Officer	Validates the request.
3	SCC	Routes request to Dissemination (S12P1), S2, S3, Oversight & Compliance, Physical Security, System Security, and Personnel Security.
4	S12P1	Reviews the proposed dissemination plan for the information to be accessed.
4 (cont.)	S2 and/or S3	Reviews the mission justification for the proposed accesses, to include the establishment of new mission.
4 (cont.)	Oversight & Compliance	Reviews the oversight training records of personnel proposed for access, and arranges for training for those who have not completed it. Also reviews and validates the designation of an Intelligence Oversight Officer for the proposed access, and a clear oversight reporting path.
4 (cont.)	Physical, System,	Review the request against NSANet connectivity requirements.

	Personnel Security	
5 (if needed)	Requester	When all security approvals are received, if a new NSANet account is required, the requester will submit a ticket to the Information Technology Directorate (963-6600s) requesting the creation of this account.
6 (if needed)	SCC/Requester	If any of the parties involved in Step 4 require clarification or modification of information from the requester, the SCC will convey the additional requirement to the requester who should attempt to provide the clarification within 10 working days.
7	Database Administrators	Upon notification by the SCC that an access request has been approved for a confirmed NSANet account holder, the administrators for each approved database will create the account and notify the SCC so the SCC can close the request.
8 (if needed)	Requester	If all steps have been completed, and the requester is not able to log in to NSANet or to the database, the SCC will notify the requester's SCE or sponsor to assist with troubleshooting to rectify the problem.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Initial Validation and Request Verification

B3.2. (U//~~FOUO~~) Based on the information provided in the request, the application is routed to a designated Point of Contact (POC) for initial review and verification. Appropriate SCE liaison officers, foreign affairs officers, and, if no POC can be identified, the SCC are responsible for the initial verification. These individuals have three business days to review/verify the request.

(U) Security and NSANet Connectivity

B3.3. (U//~~FOUO~~) If no confirmed records exist for the requester in the security database, or if the requester does not already have access to NSANet, the unit will need direct NSANet or proxy (JWICS) connectivity. The SCC Database Access form contains the necessary NSANet connectivity questions to complete connectivity requirements; therefore, a separate application is not necessary. The NSA/CSS Associate Directorate for Security and Counterintelligence will notify the SCC when NSANet access has been granted.

B3.4. (U//~~FOUO~~) Once all security reviews have been approved, the requester must submit a ticket with the Information Technology Directorate (ITD) to create an NSANet account. ITD notifies the requester via email when the account has been created. Security reviews are approved or denied within three business days, and ITD account creation is completed in approximately nine business days.

B3.5. (C//REL) Authority for making security determinations regarding eligibility for USSS personnel access to the following raw SIGINT databases, to include personnel [redacted] resides with the SIGINT Deputy Directors as follows:

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




Deputy Director for Analysis and Production (S2)



Deputy Director for Data Acquisition (S3)



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

B3.6 (U//~~FOUO~~) Any person who requests database access 

 consent form prior to gaining access. Additionally,  compliance plan approved by the Associate Directorate for Security and Counterintelligence and the sponsoring mission element must be on file prior to access.

(U) Mission Approval

B3.7. (U//~~FOUO~~) The SCC forwards the application to the A&P Operations Staff or to database owners within DA for review. The POCs within A&P and DA have five business days to review and approve or deny the request. A&P production center approval is sent to the A&P Operations Staff if the requested database requires additional review.

B3.8. (U//~~FOUO~~) If the request is denied or modifications to the request are needed, the SCC will notify the requester, the SCE, or other designated liaison to coordinate and resubmit the request. The A&P or DA staff requesting changes must detail the types of changes required for approval. The applicant should provide SCC the required amplifying information within 10 business days of notification. Once the changes are made, the request is resubmitted for mission approval within five business days.

(U) Dissemination

B3.9. (U//~~FOUO~~) The requested dissemination method must be routed to Information Sharing Services for review and approval. This may require coordination within the relevant product line. Only special circumstances require Chief of Information Sharing Services review and approval. Information Sharing Services has five business days to review and approve or deny the request. If the request is denied and changes must be made, the SCC will notify the requester, the SCE, or other designated liaison to coordinate and resubmit the request. After changes, the request must be reviewed again within three business days.

(U) Oversight and Compliance (O&C)

B3.10. (U//~~FOUO~~) The application is reviewed by SID O&C for USSID SP0018 and physical location requirements. The O&C POC will contact the Intelligence Oversight Officer for the SCIF to verify that the specified guidelines are being followed. O&C will inform the SCC when it has completed validation of the oversight requirements.

(U) Training Validation

B3.11. (U//~~FOUO~~) When all approvals have been received by the main participants of the process, the SCC will validate individual names on the request against training records or will contact the training POC's to determine if the individuals have completed the required training. Results are recorded within the SCC system. SCC has two business days to determine if training has been completed for a particular request.

(U) Account Development

B3.12. (U//~~FOUO~~) Once all approvals and NSANet account information are received in the SCC system, database administrators are notified that the request was approved and to create the accounts. A request form must be completed for each account to comply with database project requirements. The database administrator has two business days to create the account (this includes providing the user with a login and password) and to notify the SCC that the account was created.

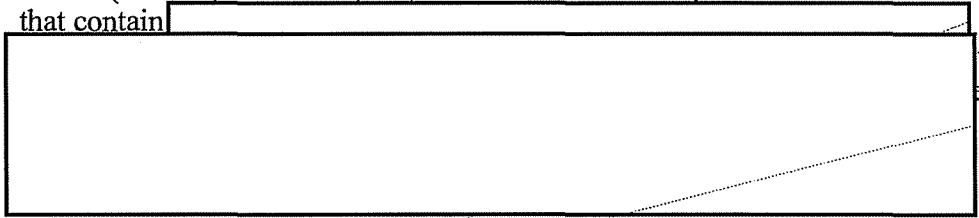
(U) Timeline

B3.13. (U//~~FOUO~~) If all questions are complete at submission, the application timeline shall not exceed twelve business days. This timeline includes the security and NSANet connectivity processes when required. The timeline for requests from individuals deployed to or deploying to a war zone or life-endangering location shall not exceed seven business days.

NOTE: (U//~~FOUO~~) All USSS elements should begin the access to raw SIGINT and SIGINT databases approval process as far in advance as possible to ensure that access is granted when needed in support of assigned SIGINT missions.

(U) Follow-on Training

B3.14. (S//~~REL~~) As the majority of database access requests include databases that contain



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

Proceed To:

[Director](#) | [SIGINT Directorate](#) | [SIGINT Policy](#) | [Reporting Policy & Guidance](#) | [Office of Policy](#)

Oversight and Compliance | Office of General Counsel | USSID Index

Derived From: NSA/CSSM 1-52

Dated: 8 January 2007

Declassify On: 20320108

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR,
NZL//20291123~~