SECRET//~~COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

SIGNALS INTELLIGENCE DIRECTORATE

SID MANAGEMENT DIRECTIVE NUMBER 421

Issue Date: 30 April 2007
Revised Date: 25 March 2008
POC: S02L1

(U) UNITED STATES SIGINT SYSTEM DATABASE ACCESS

(U) Purpose

(U//~~FOUO~~) In order to best serve our customer, it is imperative that the Signals Intelligence (SIGINT) process for access to databases be executed as expeditiously as possible. In order to facilitate that, this document outlines a new process for providing SIGINT database access to SIGINT personnel throughout the U.S. SIGINT System (USSS), located outside of NSA Washington (NSAW) and the Cryptologic Centers, in support of assigned and delegated SIGINT missions. This SID Management Directive supercedes anything in United States Signals Intelligence Directive (USSID) CR1610 that conflicts with this document; however, all legal and intelligence oversight requirements in USSID CR1610 remain in effect. USSID CR1610 will be updated later to reflect this guidance.

NOTE: (U//~~FOUO~~) Underlined terms are defined under the Definitions section.

(U) Scope

(U//~~FOUO~~) This SID Management Directive applies to all SIGINT personnel and

SIGINT production elements located outside of NSA Headquarters (NSAW) and the NSA/CSS Cryptologic Centers.

(U) Policy

(U//~~FOUO~~) In accordance with NSA/CSS Policy 1-9, SIGINT information (metadata and payload) that has not been minimized nor assessed for foreign intelligence is eligible for sharing only with NSA/CSS SIGINT elements, with Foreign SIGINT Partners, and with other U.S. Government elements specifically approved pursuant to DIRNSA authority in accordance with applicable policies, directives, and minimization procedures. Access to raw SIGINT data is limited to traditional and non-traditional SIGINT production elements approved for a SIGINT mission and a related set of SIGINT databases at a given location. This is done through the mission delegation process as defined in SID Management Directive 422 and recorded in USSIDs and/or the Mission Correlation Table (MCT). The SIGINT production element must also:

- (U//~~FOUO~~) be operating in an accredited Sensitive Compartmented Information Facility (SCIF);

- (U//~~FOUO~~) have an approved SIGINT dissemination plan, if applicable; and

- (U//~~FOUO~~) have an established and documented intelligence oversight mechanism that ensures proper handling of information at site within the SIGINT production chain as well as a documented intelligence oversight reporting process.

(U//~~FOUO~~) Once these criteria are established and documented, the individual or his sponsor may then apply for database access as part of this SIGINT production element. Access will be granted, depending on the mission and position, to the databases and tools approved for the SIGINT production element at that location.

NOTE: (U//~~FOUO~~) Individual database access is not guaranteed unless all eligibility conditions have been met - e.g., assignees may not be granted access to unevaluated, unminimized Foreign Intelligence Surveillance Act (FISA) data; individuals not read onto a particular special access program (SAP) cannot access such SAP data; etc.

(U//~~FOUO~~) Individuals seeking database access must then:

- (U//~~FOUO~~) have a NSANet account;

- (U//~~FOUO~~) be part of a SIGINT production element that has a confirmed SIGINT mission with an associated set of databases and meets the other requirements of the above paragraph;

- (U//~~FOUO~~) be fully indoctrinated and cleared for TOP SECRET (TS) Sensitive Compartmented Information (SCI); and

- (U//~~FOUO~~) have completed an approved training and indoctrination program for the required mission, databases, and tools.

(U//~~FOUO~~) Approved missions and databases will be documented in the MCT as specified in SID Management Directive 422. It is imperative that site and element leadership ensure correct, approved, and complete missions are listed in the MCT because accesses to databases for individuals will be granted in accordance with this table.

(U//~~FOUO~~) The below paragraphs provide further guidance for each of the above requirements.

RICHARD P. ZAHNER
MG, USA
Signals Intelligence Director

DISTRIBUTION:
Signals Intelligence Directorate, All
SIGINT Enterprise, Field, All
Office of General Counsel
Office of Policy

(U) SIGINT PRODUCTION ELEMENTS

(U) Definition

1. (U//~~FOUO~~) Units or organizations that have confirmed SIGINT missions are listed in USSID CR1610 as traditional or non-traditional SIGINT production elements, usually with USSIDs.

(U) Individuals

2. (U//~~FOUO~~) To be considered a part of a traditional SIGINT production element, the individual must be:

- (U//~~FOUO~~) a civilian employee of NSA/CSS;
- (U//~~FOUO~~) a military member permanently posted to NSA/CSS and under the full direction and SIGINT operational control of DIRNSA/CHCSS;

- (U//~~FOUO~~) a military member of a cryptologic element or tactical SIGINT unit with an executed USSID or site profile;
- (U//~~FOUO~~) a NSA/CSS contractor;
- (U//~~FOUO~~) a U.S. integree at NSA/CSS;
- (U//~~FOUO~~) a U.S. assignee at NSA/CSS; or
- (U//~~FOUO~~) a Second Party SIGINT integree at NSA/CSS.

(U//~~FOUO~~) U.S. integrees, U.S. assignees, or their sponsors must ensure the completion of the document authorizing the integree/assignee as a member of a SIGINT production element (a memorandum of agreement (MOA) or memorandum of understanding (MOU), signed in accordance with NSA/CSS Policy 1-43).

3. (U//~~FOUO~~) Second Party Partner SIGINT personnel outside of NSAW may be considered as integrees provided they meet the requirements of NSA/CSS Policy 1-13. A SIGINT Deputy Director (DD) or Associate Deputy Director (ADD) responsible for the mission being worked by the Second Party SIGINT integree or designated NSA/CSS Representatives (NCRs) approved by the SIGINT Director may approve a Second Party SIGINT integree for access to databases containing NOFORN SIGINT data with the exception of FISA data. Second Party SIGINT personnel may not be approved for access to NOFORN databases when those databases contain information collected under other than DIRNSA's SIGINT authorities without approval from the agency originating the information.

(U) Tethered Analysts and Elements

4. (U//~~FOUO~~) Analysts or groups of analysts may be tethered forward from a traditional SIGINT production element via a staff processing form (SPF) or a MOA/MOU signed by the SIGINT DD or ADD responsible for the mission being deployed. NCRs (as delegated by the SIGINT Director) may also approve, via an SPF or other written documentation, the deployment of analysts from traditional SIGINT production elements in their Area of Responsibility (AOR) to other Traditional and Non-traditional SIGINT production elements. These tethered analysts or tethered elements will take their home element missions and database accesses with them to work at the new location. (The continuation of access to databases that contain FISA or FISA-derived data or special source database, however, will require the SIGINT Director's approval if this is the initial access request for a given location.) The authorization document will justify the need for the tethered mission and accesses of the analysts at the new location and ensure that the oversight required for the activity is in place. The document authorizing the tethering must be sent to the DD or ADD who is responsible for the mission, the SID Oversight and Compliance Office (O&C), and the SIGINT Policy Office.

(U) SIGINT MISSION DELEGATION

(U) Missions in the MCT

5. (U//~~FOUO~~) To ensure expedited database access, SIGINT production element missions and the databases associated with those missions must be recorded in USSIDs, mission delegation forms (MDFs) or other documentation, or MOAs/MOUs, and, most importantly, in the MCT. The process in this directive is based on the assumption that the SIGINT production element to which an individual is attached has the appropriate mission recorded in the MCT.

(U) New Missions

6. (U//~~FOUO~~) Only the DIRNSA/CHCSS, the SIGINT Director, a SIGINT DD or ADD may assign/delegate a new SIGINT mission to a SIGINT production element. See SID Management Directive 422 for more information and details of the mission delegation process.

(U) SECURITY

(U) SCIF Accreditation

7. (U//~~FOUO~~) All SIGINT activities, including those conducted by tethered elements and analysts must be conducted in an accredited SCIF to house the SIGINT operation. The sponsor submitting an individual for database access or the individual who will receive it may contact the Associate Directorate for Security and Counterintelligence (ASD&CI) to verify SCIF accreditation.

(U) Polygraph Requirement

8. (U//~~FOUO~~) Any individual who requests SIGINT database access and who [redacted]

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

(U) Eligibility Determinations

9. (C//REL) Authority for making determinations regarding eligibility for USSS personnel access to raw SIGINT databases, [redacted] resides with the SIGINT DD or ADD who is responsible for the SIGINT mission. NCRs designated by the SIGINT Director as having SIGINT mission delegation authority also have authority for making eligibility determinations for USSS personnel in their AORs as outlined in the above paragraph.

(U) OVERSIGHT

(U) General Oversight Expectation

10. (U//~~FOUO~~) Individuals, managers, and designated Intelligence Oversight Officers (IOOs) must strive for the oversight for the data types involved as described in the Annex to this Directive which describes the risks associated with each type of data and the oversight to be implemented to manage that risk. In general, oversight must be in place to cover for all four phases of SIGINT production:

- (U) collection;
- (U) processing (e.g., analysis, cryptanalysis, transcription, etc.);
- (U) retention; and
- (U) dissemination.

(U//~~FOUO~~) and all five key areas of oversight:

- (U) complete rules for activity;
- (U) training on rules;
- (U) implementation of technical, physical, and managerial measures to ensure compliance;
- (U) IG reporting; and
- (U) a process for fixing compliance problems.

(U//~~FOUO~~) These intelligence oversight considerations must be taken into account, along with mission considerations, when determining whether to grant database access to a SIGINT element. Managers are expected to exercise due diligence in determining oversight regimes to ensure that the SIGINT activity is conducted in a way that properly balances the Government's need for foreign intelligence and the protection of the privacy rights of U.S. persons, and ensures compliance with the laws and regulations governing NSA's foreign intelligence mission. Due diligence in determining appropriate oversight means that every attempt is made to implement the required oversight; a lesser standard is only implemented when the standard described in the Annex cannot be reached for **clearly defensible and articulable reasons**. See the table in the Annex for levels of oversight to be implemented for data of different types (minimized versus unminimized, evaluated versus unevaluated, FISA versus non-FISA; and metadata versus payload).

(U) SIGINT DISSEMINATION PLAN

(U) Requirement

11. (U//~~FOUO~~) As noted above, SIGINT production elements must have an approved SIGINT dissemination plan for all missions except SIGINT Development. When an element or analyst is tethered forward, there must be an approved SIGINT dissemination plan that the MDA has worked out in coordination with Information Sharing Services (S12) and recorded with the SIGINT mission authorization that must be part of the MCT.

(U) TRAINING AND INDOCTRINATION

(U) Requirement

12. (U//~~FOUO~~) Prior to applying for or obtaining access to raw unminimized, unevaluated SIGINT databases, all individuals shall be certified in USSID SP0018/Database Access training provided by the Office of the General Counsel (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 USSID Database Systems" (USSID CR1610, Annex A).

NOTE 1: (U//~~FOUO~~) Individuals who do not request and use an unminimized, unevaluated database within six months of USSID SP0018 certification must be briefed again to ensure internalization and understanding of the restrictions on the data being granted.

NOTE 2: (U//~~FOUO~~) In conjunction with the new database access process, NSA/CSS is making available a computer-based training (CBT) course, CRSK 1800 "USSID SP0018 Orientation," which can be accessed via NSA Net and JWICS by typing "go vuport". This course is intended primarily for NSA/CSS deployers who require database access and cannot readily attend an interactive USSID SP0018 briefing either in person or via VTC. CRSK 1800 serves as an adjunct to reading USSID SP0018 and does not absolve individuals of the required annual intelligence oversight reading. Successful completion of the course certifies an individual for 24 months if they are accessing databases as part of their duties, and for 6 months if they are not accessing databases.

(U//~~FOUO~~) SIGINT personnel at Cryptologic Centers, Field Sites, and other U.S. and Second Party external elements must contact their local IOO or point of contact (POC) or sponsor for USSID SP0018 certification and account requests. Certification briefings are scheduled on an as-needed and as-possible basis with field elements through the video teleconference system and via a DVD formatted briefing if necessary. A short list of POCs is available at the following web page: http://sitepro.ops.s.nsa/index.cfm?p_id=853 but in no way should be taken as the only list. These are simply the most widely used. For elements not reflected in this list, or if personnel do not know who to contact at their site, an email should be sent to either your sponsor or dbaccounts@nsa.ic.gov.

13. (U//~~FOUO)~~Additional intelligence oversight training from OGC and O&C is required for SIGINT databases containing FISA or FISA-derived data.

~~(C//REL)~~ Special FISA Considerations

14.~~(C//REL)~~Only NSA/CSS personnel and integrees under the sole direction and operational control of the DIRNSA/CHCSS are eligible for access to databases that contain FISA or FISA-derived data to conduct SIGINT activities that support the information needs validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. The SIGINT Contact Center (SCC) process must ensure that the SIGINT personnel receiving the FISA data access authorization meet this requirement, especially when the personnel are integrees. When SIGINT personnel are a part of a SIGINT production element authorized for FISA data access, all personnel accessing databases that contain FISA or FISA-derived data must receive additional training by OGC and SID O&C on the minimization procedures and handling restrictions governing the type of FISA data specifically involved. Individuals must also read and remain familiar with the general and specific oversight documents governing NSA/CSS activities under FISA, including USSID SP0018, Annex A, "Procedures Implementing the Foreign Intelligence Surveillance Act;" Appendix 1, "Standardized Minimization Procedures for NSA Electronic Surveillances;" and any other documents that describe special handling procedures for the FISA data involved. Individuals must also read O&C's FISA Responsibilities Memo, which describes individual responsibilities regarding handling and use of FISA data. This memo is available at http://sitepro.ops.s.nsa/index.cfm?p_id=861. Parent organizations of integrees must relinquish all operational control of the integrees while they are integrated into NSA/CSS. This shall be documented in the MOU/MOA governing the integrees' presence at NSA/CSS and integrees shall sign statements indicating their understanding of these and other requirements as a precondition to gaining access to unevaluated, unminimized SIGINT data and conducting SIGINT activities. (See the Definitions section for additional requirements.) Assignees to NSA/CSS are not eligible for access to FISA data. FISA access for integrees who are at NSA/CSS on a part-time basis must be approved by the SIGINT Director or his delegated authority.

15.~~(C//REL)~~ FISA access is based on current mission need and does **not** follow an individual analyst from office to office within NSAW, nor to TDY or PCS locations or to forward-deployed or tethered locations unless specified in the document authorizing the assignment. Persons changing mission/job and/or location must provide re-justification to O&C through their management chain for FISA access or access to unminimized, unevaluated content (vice metadata) in the new position.

16. ~~(C//REL)~~ Any element requesting access to databases that contain FISA or FISA-derived data must contact the NSA organization that sponsored the relevant FISA application to ensure that roles and responsibilities vis-à-vis minimization obligations, management and renewal of the collection authorization, target deconfliction, and record-keeping on the use of the raw traffic are clearly delineated and agreed upon. This will ensure that FISA minimization and other required procedures are followed.

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

17. ~~(C//REL)~~ Access to FISA raw traffic is controlled through [redacted] the NSA clearance management system. In addition to approval for specific databases, analysts requesting FISA raw traffic database access must also be sponsored for the necessary access through [redacted]

(U) DATABASE ACCESS

(U) Summary of Procedures

18. (U//~~FOUO~~) The procedures table below summarizes the process for requesting access to raw SIGINT data and databases. All SIGINT production elements should begin the process for accessing databases as far in advance as possible to ensure that access is granted when needed in support of assigned SIGINT missions and deployments.

(U) Assumptions

19. (U//~~FOUO~~) This process is based on the assumption that the SIGINT production element to which the individual belongs has had its mission, dissemination plan, and database information recorded in the MCT and the required oversight is in place at the location where the data will be worked. If the information on the unit/organization is not in the MCT, the process will revert back to the one described in USSID CR1610. This process also assumes that the individual applying for access has received an NSANet account through the individual's sponsor.

(U) PROCEDURES TABLE

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Steps	POC	Activity
1	Sponsor	Submits a request for access to the SCC through the "Request for Access to Raw SIGINT Databases" website.
2	SCC	Checks the request against the MCT. (See paragraph 20 below). Ensures that the individual has an NSANet account. Also reviews the USSID SP0018 certification records for the individual and the IOO information for the SIGINT production element, and confirms receipt of the MDA's statement that oversight has been implemented per the requirements described in this USSID. This should take two business days.

		NOTE: If any of the information involved in Step 2 requires clarification or modification from the sponsor/individual, or if any SIGINT personnel require oversight briefings or the MDA has not yet confirmed that the required oversight is in place, the request is returned to the sponsor to be completed.
3	Database Administrators	Upon notification by the SCC that an access request has been approved, the administrators for each approved database will create the account and notify the individual, the sponsor, and the SCC so the SCC can close the request. This should take one business day.
4 (if needed)	Individual	If all steps have been completed, and the individual is not able to log in to the database, the SCC, the sponsor, and the individual will work with the database administrator to the problem.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) PROCESS FOR TERMINATION OF ACCESS

(U) When Access is No Longer Needed

20. (U//~~FOUO)~~Upon determining that an individual will no longer require access to raw SIGINT data, the SIGINT production element IOO will immediately notify the database System Administrators to remove the individual's accounts from their systems. This notification should be sent directly to the database System Administrators with a copy to O&C and the SCC. Failure to remove accounts may result in unlawful access, so managers and IOOs at the SIGINT production elements must pay careful attention to personnel changes and movement for their organizations.

(U) Individual Reassignments

21. (U//~~FOUO)~~If an individual is reassigned to another USSS organization and needs to retain access to an unminimized, unevaluated SIGINT (including FISA) database, the individual, through his or her new management, must submit a re-justification in an account request to O&C, with new justification and auditor information as it applies to the individual's new job. To avoid an interruption in access, this can be done prior to the individual's reassignment, provided the effective date for the new job is included in the request.

(U) Inactive Accounts

22. (U//~~FOUO)~~The database administrator will suspend, without prior notice, any account that has been inactive for a period of 90 days. The database administrator will subsequently notify the individual, who will then initiate action either to close

the account or provide the database administrator a reason for maintaining the account in an active status.

(U) DEFINITIONS

(U) Approved SIGINT Dissemination Plan

23. (U//~~FOUO~~) A plan to disseminate SIGINT information to customers in response to information needs, requests for information, and other requests validated by NSA/CSS. The plan must be approved by the MDA in close coordination with the Information Sharing Services Policy Office (S12P).

(U) Assignee

24. (U//~~FOUO~~) The term "assignee" in this document (vice "integree") refers to non-NSA/CSS personnel detailed or assigned to a traditional SIGINT production element under the direction and SIGINT operational control of the DIRNSA/CHCSS to conduct SIGINT activities that support information needs validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. Assignees may be civilians, military members, contractors, or Second Party partners. A MOU/MOA governing the assignee's presence at NSA/CSS--that states that the assignee will be under the direction and SIGINT operational control of the DIRNSA/CHCSS during his/her assignment to NSA/CSS--must be executed between NSA/CSS and the parent organization. An assignee is distinguished from an integree by the fact that the assignee's parent organization may retain some operational control of the assignee for non-SIGINT matters. Prior to seeking access to raw SIGINT data, assignees must sign a precondition memorandum that is part of the MOU/MOA documenting their presence at NSA/CSS. For contractor assignees, an authorized representative of the parent organization must additionally execute a memorandum certifying the terms and conditions under which the contractor services are being provided to NSA. (Liaison officers typically are not considered assignees.)

(U) Foreign Intelligence Surveillance Act (FISA) Data

25. (U) The Foreign Intelligence Surveillance Act (FISA) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. FISA requires that all "electronic surveillance" as defined by FISA be directed only at foreign powers or agents of foreign powers as defined by FISA and authorized by the United States Foreign Intelligence Surveillance Court, or, in certain limited circumstances, by the Attorney General. All data collected in accordance with this law is referred to as FISA data.

(U) Integree

26. (U) The term "integree" in this document (vice "assignee") refers to non-NSA/CSS personnel integrated into or detailed to a traditional SIGINT element (as defined in USSID CR1610) who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct SIGINT activities that support information needs

validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilians, military members, contractors, or Second Party SIGINT personnel. A MOU/MOA governing the integree's presence at NSA/CSS - that states that the integree will be under the full direction and operational control of the DIRNSA/CHCSS, and that the integree's parent organization relinquishes all operational control of the integree, during his/her assignment to NSA/CSS - must be executed between NSA/CSS and the parent organization. (Non-NSA/CSS personnel who are assigned to NSA/CSS to operate under the direction, authority, and SIGINT operational control--but not full operational control--of the DIRNSA/CHCSS, will be considered to be "assignees" under this Directive. Typically, liaison officers are not considered integrees or assignees.) Prior to seeking access to raw SIGINT data, integrees must sign a precondition memorandum that is part of the MOU/MOA documenting their presence at NSA/CSS. For contractor integrees, an authorized representative of the parent organization must additionally execute a memorandum certifying the terms and conditions under which the contractor services are being provided to NSA.

(U) Metadata

27. (U//~~FOUO~~) Refers to structured "data about data". Metadata includes all information associated with, but not including content, and includes any data used by a network, service, or application to facilitate routing or handling of a communication or to render content in the intended format. Metadata includes, but is not limited to, dialing, routing, addressing, or signaling information and data in support of various network management activities (e.g. billing, authentication or tracking of communicants).

(U) Mission Correlation Table

28. (U//~~FOUO~~) DDAP is the responsible official for the integrity and contents of the MCT. This table is a master list of all SIGINT analytic production elements that have been approved for SIGINT mission. The MCT, whose maintenance is the responsibility of A&P, facilitates the database access process by providing a record of databases needed to perform a given SIGINT mission. This table records the unit's SIGINT Address (SIGAD), the location, the mission, the intelligence oversight officer, authorized databases, dates, and other information necessary to authorize access to raw SIGINT data.

(U) Mission Delegation Authority (MDA)

29. (U//~~FOUO~~) The DIRNSA/CHCSS or SID official authorized to delegate a mission to a new organization and/or new location. This includes the SIGINT Director, a SIGINT Deputy Director, a SIGINT Associate Deputy Director, or a NSA/CSS Representative as approved by the SIGINT Director. The Director of NTOC is the delegation authority for SIGINT missions assigned to NTOC. MDAs and the mission delegation process is detailed in SID Management Directive 422.

(U) Payload

30. (U//~~FOUO~~) Payload is the message substance [redacted] of the communication and may include but is not limited to the body or subject line of an email, [redacted] or the voice data of a phone call [redacted] [redacted]

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

(U) Polygraph Plan

31. (U//~~FOUO)~~ Director of Central Intelligence Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," administratively updated 3 May 2002, establishes the use of polygraphs for access to SCI material and this is further implemented in NSA/CSS Policy 5-2, "Security Investigations," dated 16 December 2003 and NSA/CSS Policy 5-1, "Personnel Security Policies and Procedures for Members of the Service Cryptologic Elements Assigned or Detailed for Duty with the NSA/CSS," dated 18 November 2004. [redacted] The information provided in these forms shall serve as a major factor in the MDA's determination of the eligibility for initial or continued access to NSA/CSS protected information.

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

(U) Raw SIGINT Data

32. ~~(C//SI//REL)~~ Raw SIGINT data is any SIGINT data 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, [redacted]

(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 determined to constitute foreign intelligence and minimized, it can then be considered for "native format" SIGINT dissemination or as Evaluated and Minimized SIGINT traffic (EMT) and is eligible for release in accordance with USSID SP0018 and other approved SIGINT dissemination means and processes established by policies governing SIGINT production.

(U) Service Cryptologic Elements (SCEs)

33. (U) The military cryptologic organizations of the Army, Navy, Marine Corps, Air Force, and Coast Guard with assigned SIGINT missions that comprise the Central Security Service (CSS) and operate under the direction and SIGINT operational control of the DIRNSA/CHCSS.

(U) SIGINT Databases

34. (U//~~FOUO~~) Databases that serve as the repositories for SIGINT data that are derived from USSS and foreign SIGINT partner collection against intelligence

priorities. These databases are generally accessible to SIGINT production personnel based on assigned mission and serve a broad analytic purpose. There are various categories of SIGINT Databases:

- (U) **FISA DATABASES** - SIGINT databases that contain FISA or FISA-derived data (see definition above). In practice, these databases usually include other data in addition to FISA, as there are no FISA-specific databases.

- (U//~~FOUO~~) **METADATA DATABASES** - SIGINT databases that contain metadata from communications transactions but no content from the communications. (Metadata--usually to/from information relating to specific communication events--is currently considered to be the same as message content and must receive the same USSID SP0018 protection. Metadata from FISA is governed by applicable FISA minimization procedures or the specific terms of the court order under which it was collected.)

- (U) **NATIONAL-LEVEL SIGINT DATABASES** - A national-level database contains information of interest across a broad section of targets or of interest to a broad section of USSS elements. It is usually populated by sources from more than one location.

- (U) **ORGANIC, TACTICAL SIGINT DATABASES** - Databases that are populated by an organization/element with a target limited to a specific location or area or a target with a limited membership.

- (U) **RAW SIGINT DATABASES** - SIGINT databases that contain raw SIGINT data (see definition above).

- (U//~~FOUO~~) **SPECIAL SOURCE SIGINT DATABASES** - Databases that contain SIGINT information originating from sources where knowledge about the source is contained in exceptionally controlled information (ECI) categories or special access programs (SAPs). Some of these database may also include information obtained under FISA.

(U) Sponsor

35. (U//~~FOUO~~) The sponsor refers to an individual who has been approved by his supervisor to submit other individuals for database access within the SCC process. It is often one of the SCE Liaison Offices at NSAW on behalf of deployed military or it could be a NSAW SIGINT production element working on behalf of an integree, forward deployed, or tethered element/individual. It might also be a NCR acting on behalf of a SIGINT production element within the appropriate AOR.

(U) Tethered

36. (U//~~FOUO~~) An analyst who is functioning as part of and under the direct

Analyst

SIGINT operational control and tasking of a traditional SIGINT production element (as defined in USSID CR1610), usually an element resident at NSAW or a Cryptologic Center. However, the analyst is located in a different SIGINT production element or a customer element location. The tethered analyst retains the mission and appropriate database accesses from that home element and the tethered mission is kept separate from and not added to the mission of the different (non-home element) SIGINT production element. The analyst relies on the home element for operational tasking and reporting authority and, if appropriate, administrative support and intelligence oversight support.

(U) Tethered Headquarters Element

37. (U//~~FOUO~~) A sub-element of a SIGINT production element, that is usually resident at NSAW or a Cryptologic Center, that is functioning under the direct SIGINT operational control and tasking of that home element but operating at different SIGINT production element or customer location. This tethered element retains the mission and appropriate databases accesses from that home element. The sub-element relies on the home element for operational tasking and reporting authority and, if appropriate, administrative support and intelligence oversight support.

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

38. (U//~~FOUO~~) **TRADITIONAL**: A USSS element whose fundamental purpose is SIGINT production under the direction of the DIRNSA/CHCSS is a "traditional SIGINT production element." A traditional SIGINT production 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 must be:

- (U) a civilian employee of NSA/CSS;
- (U//~~FOUO~~) a military member permanently posted to NSA/CSS and under the full direction and SIGINT operational control of DIRNSA/CHCSS;
- (U//~~FOUO~~) a military member of a cryptologic element or tactical SIGINT unit with an executed USSID or site profile;
- (U) a NSA/CSS contractor;
- (U) a U.S. integree at NSA/CSS;
- (U) a U.S. assignee at NSA/CSS; or
- (U) a Second Party SIGINT integree at NSA/CSS;

and are inherently part of a the SIGINT Production Chain (SPC) and, therefore, eligible for access to appropriate raw SIGINT databases. The following elements are considered traditional:

a. (U//~~FOUO~~) NSAW SIGINT Directorate and NSA/CSS Cryptologic Center elements with a SIGINT mission.

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

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

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

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

d. ~~(C//REL)~~ Active Duty Service Cryptologic Elements (SCEs) [redacted] [redacted] with assigned SIGINT missions.

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

e. (U//~~FOUO~~) Military Service Partner tactical SIGINT elements - Department of Defense (DoD) tactical SIGINT units not assigned to an SCE - with assigned SIGINT missions.

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

---

39. (U//~~FOUO~~) **NON-TRADITIONAL**: 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. These entities are hereafter identified as "non-traditional" SIGINT production elements. When assigned SIGINT missions by DIRNSA/CHCSS, and when appropriate intelligence oversight channels have been established, these elements become part of the USSS. These conditions must be documented in a USSID, a MOU/MOA, a SPF, a MDF, or other formal documentation as appropriate. Personnel performing SIGINT enabling or production activities within these elements then become part of a SPC and are therefore eligible for access to appropriate raw SIGINT and national-level raw SIGINT databases:

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

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

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

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

d. (U//~~FOUO~~) The National Threat Operations Center (NTOC), a NSA/CSS organization [redacted] [redacted]

e. (U//~~FOUO~~) Special Cryptologic Partners [redacted] [redacted]

f. (U//~~FOUO~~) Cryptologic Services Groups (CSGs) with assigned SIGINT mission.

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

g. (U//~~FOUO~~) Research Associate Directorate (RAD), Information Assurance Directorate (IAD), [redacted] and other elements supporting SIGINT missions.

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

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

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

NOTE 1: (U//~~FOUO~~) Given the distinct and ever-changing nature of research and development efforts to adequately support SIGINT missions, RAD [redacted] that support SIGINT systems may require large volumes of, and differing accesses to, SIGINT information and raw SIGINT data.

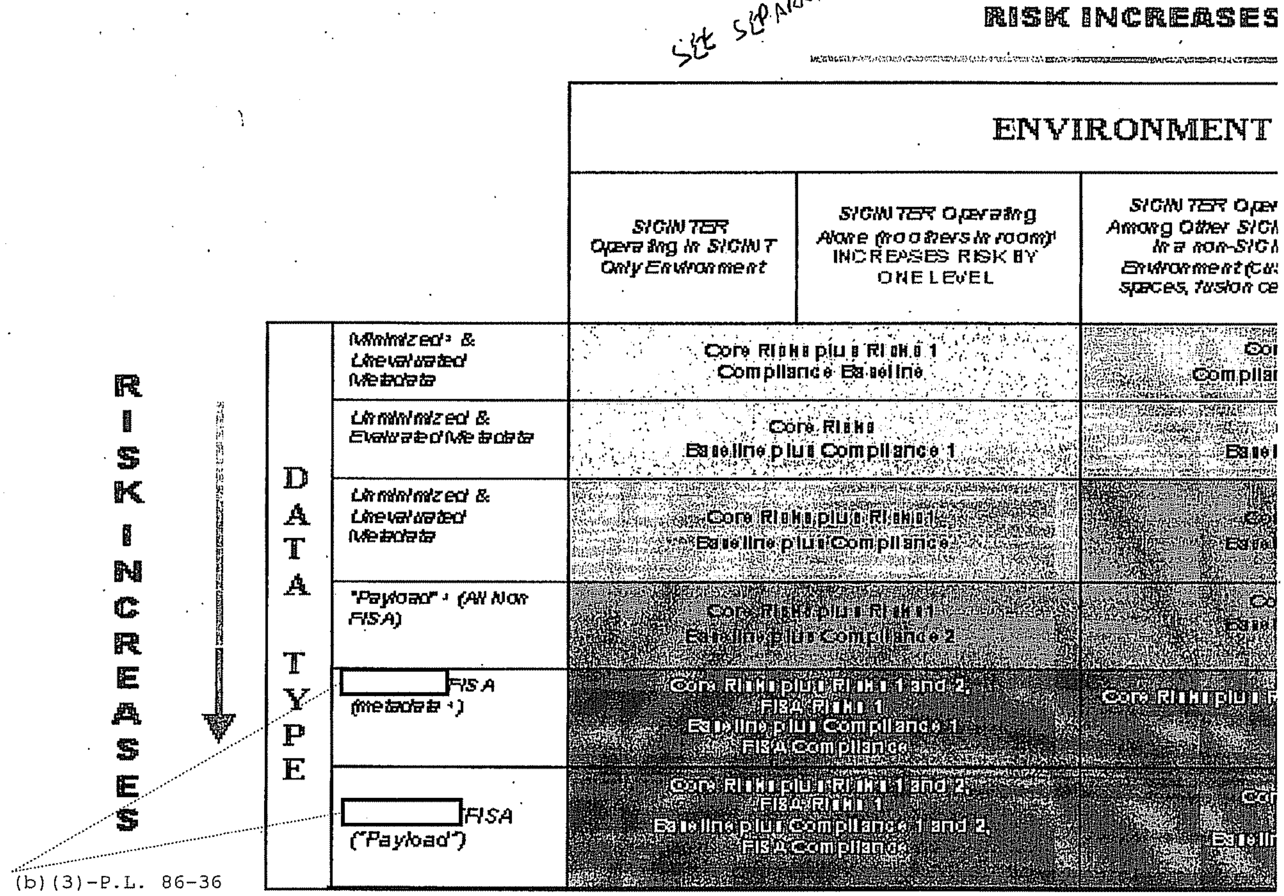
NOTE 2: (U//~~FOUO~~) IAD is increasingly collaborating with SID in SIGINT production activities through joint elements such as the NSA/CSS NTOC and through the integration of IAD personnel into SID elements. When collaborating with SID, certain IAD personnel may be designated and documented as working under DIRNSA/CHCSS' SIGINT authorities.

(U) United States SIGINT System (USSS)

40. (U//~~FOUO~~) The United States SIGINT System (USSS) is the SIGINT part of the United States Cryptologic System (USCS) and refers to the U.S. Government SIGINT activities worldwide under the direction of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). The USSS is composed of the NSA/CSS SIGINT Directorate, the SIGINT functions and elements of the military departments, and other governmental elements (other than the Federal Bureau of Investigation) authorized to perform SIGINT activities under the direction and authority of the DIRNSA/CHCSS.

(U) ANNEX - OVERSIGHT RISK MANAGEMENT CHART

SEE SEPARATE PAGE



RISK INCREASES

ENVIRONMENT

		SIGINTER Operating in SIGINT Only Environment	SIGINTER Operating Alone (no others in room)[1] INCREASES RISK BY ONE LEVEL	SIGINTER Oper Among Other SIGI in a non-SIGI Environment (cu spaces, fusion ce
DATA TYPE	Minimized[2] & Unevaluated Metadata	Core Risks plus Risk 1 Compliance Baseline		Co Complia
	Unminimized & Evaluated Metadata	Core Risks Baseline plus Compliance 1		Base
	Unminimized & Unevaluated Metadata	Core Risks plus Risk 1 Baseline plus Compliance		Co Base
	"Payload"[3] (All Non FISA)	Core Risks plus Risk 1 Baseline plus Compliance 2		Co Base
	[redacted] FISA (metadata[4])	Core Risks plus Risks 1 and 2, FISA Risk 1 Baseline plus Compliance 1 FISA Compliance		Core Risks plus R
	[redacted] FISA ("Payload")	Core Risks plus Risks 1 and 2, FISA Risk 1 Baseline plus Compliance 1 and 2, FISA Compliance		Co Baselin

RISK INCREASES

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

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

[1] (U//~~FOUO~~) Carries listed requirements and risks with additional risk of having insufficient oversight to know if activities are legally compliant.

[2] (U//~~FOUO~~) Minimized databases still carry risks of unmasked and unmarked U.S. Person data.

[3] (U//~~FOUO~~) Payload is defined as the message substance [redacted] of the communication and may include but is not limited to the body or subject line of an email [redacted] or the voice data of a phone call [redacted]

[4] (U//~~FOUO~~) Metadata collected under FISA is considered "contents" of a communication.

(U) Explanation of Table: (U//~~FOUO~~) Access to raw SIGINT presents a number of risks, many of which can be mitigated by implementing active compliance measures. The table above illustrates the risks and the compliance measures that must be implemented for each data type/environment combination. All access situations carry a core set of risks (identified as Core Risks, described below) and all access situations must meet the compliance baseline (Compliance/Risk Mitigation Baseline below). There are no situations that are limited to core risks and the compliance baseline;

RISK INCREASES

RISK INCREASES

DATA TYPE	ENVIRONMENT			
	SIGINTER Operating in SIGINT Only Environment	*SIGINTER Operating Alone (no others in room)*[1] INCREASES RISK BY ONE LEVEL	*SIGINTER Operating Among Other SIGINTERS in a non-SIGINT Environment (customer spaces, fusion cell, etc)*	*SIGINTER Operating as Sole SIGINTER in a non-SIGINT Environment*[1] INCREASES RISK BY ONE LEVEL
Minimized[2] *& Unevaluated Metadata*	Core Risk plus Risk 1 Compliance Baseline		Core Risk plus Risk 1 and 2 Compliance Baseline plus Compliance 3	
Unminimized & Evaluated Metadata	Core Risk Baseline plus Compliance 1		Core Risk plus Risk 2 Baseline plus Compliance 1 and 3	
Unminimized & Unevaluated Metadata	Core Risk plus Risk 1 Baseline plus Compliance		Core Risk plus Risk 1 and 2 Baseline plus Compliance 1 and 3	
"Payload"[3] *(All Non FISA)*	Core Risk plus Risk 1 Baseline plus Compliance 2		Core Risk plus Risk 1 and 2 Baseline plus Compliance 2 and 3	
[redacted] *FISA (metadata*[4]*)*	Core Risk plus Risk 1 and 2, FISA Risk 1 Baseline plus Compliance 1 FISA Compliance		Core Risk plus Risk 1, FISA Risk 1 and 2 Baseline plus Compliance 1 and 3, FISA Compliance	
[redacted] *FISA ("Payload")*	Core Risk plus Risk 1 and 2, FISA Risk 1 Baseline plus Compliance 1 and 2, FISA Compliance		Core Risk plus Risk 1 and 2, FISA Risk 1 and 2, Baseline plus Compliance 1, 2 and 3, FISA Compliance	

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

rather, every situation and data type also has nuances that involve additional risk and/or additional compliance measures. The table lists the risks and compliance measures that also apply to the situation over and above the core risks and baseline compliance measures. Note that additional risks do not always require additional compliance measures; in these cases, the Baseline may be enough to mitigate the additional risk in a given situation.

(U) Note on risks and risk mitigation:

(U//~~FOUO~~) Although training on applicable rules, solid security practices (passwords and access controls) and physical/aural separation are all integral parts of a signals intelligence oversight mechanism, there is no amount of risk mitigation that will eliminate the risks of inadvertent, accidental or intentional release of U.S. identities or improper queries. The only reasonable method to ensure that SIGINT elements follow the rules is to back up the mitigating factors with a strong, well-trained on-site oversight presence with an eye on developing a solid culture of compliance as has developed at NSAW.

CORE RISKS AND COMPLIANCE/RISK MITIGATION BASELINE:

(U//~~FOUO~~) The Core Risks and Compliance/Risk Mitigation Baseline described below apply to every access situation. The risks described relate to the type of data involved and the risks related to granting access. Additional risks relating to specific situations are described in the footnotes to the table above.

CORE RISKS:

- (U//~~FOUO~~) Undocumented dissemination of SIGINT.
- (U//~~FOUO~~) Targeting of U.S. and Second Party person identifiers in violation of USSID SP0018, DoD 5240.1-R and its Classified Annex, and the UKUSA Agreement.
- (U//~~FOUO~~) Inadvertent Dissemination of U.S. and Second Party person identifiers in violation of USSID SP0018, DoD 5240.1-R and its Classified Annex, and the UKUSA Agreement.
- (U//~~FOUO~~) Intentional Dissemination of U.S. and Second Party person identifiers in violation of USSID SP0018, DoD 5240.1-R and its Classified Annex, and the UKUSA Agreement.
- (U) Database queries could violate FISA.
- (U) Retention of SIGINT containing U.S. person information in violation of USSID SP0018.

COMPLIANCE BASELINE:

- (U//~~FOUO~~) Ad-hoc incident/violation reporting to SID Oversight and Compliance.

- (U//~~FOUO~~) Passive Auditing that records account usage.

- (U//~~FOUO~~) Non-compliance carries the need for remedial training and/or updates to site or element procedural documentation.

- (U//~~FOUO~~) Trained IOO on-site (by definition, IOO is not present in situations with footnote1 in table above).

- (U) Completion of yearly core intelligence oversight reading (E.O.12333, DoD 5240.1-R and its Classified Annex, USSID SP0018, NSA/CSS Policy 1-23, and NSCID 6).

- (U) USSID SP0018 Database Access Certification.

- (U//~~FOUO~~) Documented E.O.12333 Quarterly Reporting Path Tied into NSAW.

- (U//~~FOUO~~) Approved SCIF and Traditional SIGINT Production Element with approved mission.

- (U//~~FOUO~~) All situations governed by applicable rules: E.O.12333, DoD 5240.1-R and its Classified Annex, USSID SP0018, NSA/CSS Policy 1-23, NSCID 6, Foreign Intelligence Surveillance Act, Department of Justice Guidance, and Special and Additional Rules based on the situation.

ADDITIONAL RISK FACTORS

(U//~~FOUO~~) In addition to the Core Risks, some data has additional risks associated with access. Additional risk groupings are described below and are referenced in the table. Note that these risks are not grouped by type or seriousness; they are grouped for easy reference in the table.

RISKS 1:

- (U//~~FOUO~~) Targeting of non-foreign intelligence information in violation of E.O.12333 and FISA.

- (U//~~FOUO~~) Inadvertent Dissemination of non-foreign intelligence information in violation of E.O.12333 and FISA.

- (U//~~FOUO~~) Intentional Dissemination of non-foreign intelligence information in violation of E.O.12333 and FISA.

RISKS 2:

- (U//~~FOUO~~) Incidental Dissemination of U.S. and Second Party person identifiers in violation of USSID SP0018, DoD 5240.1-R and its Classified Annex and the UKUSA Agreement.

- (U//~~FOUO~~) Incidental Dissemination of non-foreign intelligence information in violation of E.O.12333 and FISA.

FISA RISKS 1:

- (U//~~FOUO~~) Violations of FISA minimization procedures and court-ordered handling requirements relating to processing and retention (all reported to DoJ and Congress).
- (U//~~FOUO~~) Inadvertent violations of FISA minimization procedures and court-ordered handling requirements relating to dissemination (all reported to DoJ and Congress).
- (U//~~FOUO~~) Intentional violations of FISA minimization procedures and court-ordered handling requirements relating to dissemination (all reported to DoJ and Congress).
- (U//~~FOUO~~) Inability to produce FISA dissemination records for DoJ review.
- (U//~~FOUO~~) Destruction of NSA and Declarant Credibility with Foreign Intelligence Surveillance Court.

FISA RISKS 2:

- (U//~~FOUO~~) Incidental violations of FISA minimization procedures and court-ordered handling requirements relating to dissemination (all reported to DoJ and Congress).

ADDITIONAL COMPLIANCE/RISK MITIGATION MEASURES

(U//~~FOUO~~) In addition to the Compliance Baselines, some data requires additional compliance measures to mitigate risk. Additional compliance groupings are described below and are referenced in the table. Note that these measures are not grouped by type; they are grouped for easy reference in the table.

COMPLIANCE 1:

- (U//~~FOUO~~) Technical means to prevent unauthorized contact chaining (targeting) from/through U.S. persons, or active auditing.

COMPLIANCE 2:

- (U//~~FOUO~~) Active Auditing of Query Terms Per USSID CR1610, Annex A.
- (U) Database Auditor Training.

COMPLIANCE 3:

- (U//~~FOUO~~) Reasonable Visual Separation of SIGINT Activity from Non-SIGINT Personnel.
- (U//~~FOUO~~) Reasonable Aural Separation of SIGINT Activity from Non-SIGINT Personnel.
- (U//~~FOUO~~) Restricted Access to raw SIGINT through use of dedicated printer and storage accessible only to SIGINT production chain personnel.

FISA COMPLIANCE:

- (U//~~FOUO~~) Restricted Access to FISA data through use of dedicated printer and storage accessible only to FISA-cleared SIGINT production chain personnel.
- (U//~~FOUO~~) User/Auditor/IOO: Training on Specific Applicable Higher Authorities Including data-specific FISA Training.

Proceed To:
NSA | Director | SIGINT | SIGINT Staff | SIGINT Policy

Derived From: NSA/CSS Manual 123-2
Dated: 24 Feb 1998
Declassify On: X1

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~