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

SIGNALS INTELLIGENCE DIRECTORATE

SID MANAGEMENT DIRECTIVE NUMBER 422

Issue Date: 30 April 2007
Revised Date: 15 April 2008
POC: S02L1

(U) UNITED STATES SIGINT SYSTEM MISSION DELEGATION

(U) Purpose

(U//~~FOUO~~) In accordance with NSA/CSS Policy 1-3, "NSA/CSS Governance," this Signals Intelligence Directorate (SID) Management Directive provides policy and procedures for the formal delegation of mission responsibility and a consistent process to ensure adequate support and standup of SIGINT mission within the United States SIGINT System (USSS).

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

(U) Scope

(U//~~FOUO~~) This SID Management Directive applies to all missions formally delegated for 90 days or more to SIGINT production elements located outside of NSA Headquarters (NSAW) and the NSA/CSS Cryptologic Centers.

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) PURPOSE AND SCOPE

(U) Purpose

1. (U//~~FOUO~~) Mission delegation is a critical process in the creation of a single, global, distributed, net-centric collaborative SIGINT system. Mission delegation is the process used to delegate one or more SIGINT production functions--signals collection, processing (e.g., analysis, cryptanalysis, transcription, etc.), retention, and/or dissemination--to an existing USSS element and is the process by which SIGINT production functions are documented in relation to the SIGINT production chain. The mission delegation process will be used to delegate SIGINT Production Activities in specific SIGINT Production Chains, as defined in Section 3 of USSID CR1610.

(U) Scope

2. (U//~~FOUO~~) Only the DIRNSA/CHCSS, SIGINT Director or his Deputy, Deputy Director (DD) of Customer Relationships (CR), DD of Analysis and Production (A&P), DD of Data Acquisition (DA), Associate Deputy Director of SIGINT Development (SIGDEV), and Director of the NSA/CSS Threat Operations Center (NTOC) may assign/delegate a new SIGINT mission to any SIGINT production element of the USSS outside of NSAW or the Cryptologic Centers.

3. (U//~~FOUO~~) NSA/CSS Cryptologic Representatives (NCRs), when authorized by the SIGINT Director, may re-delegate mission formally assigned to the NCRs or assigned to the NCRs' Cryptologic Services Group, or the NCRs may delegate initial or additional SIGINT missions in support of local customer requirements, in communication with a DD or ADD, to traditional SIGINT production elements within the NCR's area of responsibility (AOR) with the exception of Computer Network Exploitation (CNE) mission. NCRs may also delegate mission to

cryptologic support teams (CSTs) and cryptologic services groups (CSGs) within their AORs. The overall NCR delegation authority may not be further delegated.

NOTE 1: (U//~~FOUO~~) The first time a mission requiring FISA data access is deployed to a new location outside of NSAW or a Cryptologic Center, the SIGINT Director must be the approving official.

NOTE 2: (U//~~FOUO~~) The DIRNSA/CHCSS, SIGINT Director, the DDs, ADDs, and authorized NCRs, are collectively referred to as Mission Delegation Authorities (MDAs).

4. (U//~~FOUO~~) Tactical units requesting mission should contact the appropriate NCR for their AOR if that NCR is authorized to delegate mission. If the NCR for the AOR is not authorized, then the tactical unit needs to contact their Service Cryptologic Element (SCE) Sponsor who will contact the appropriate MDA.

5. (U//~~FOUO~~) To ensure adequate support (connectivity, tools, resources, etc.), appropriate documentation must be initiated and coordinated with the appropriate DDs or ADD and other offices of primary concern (OPCs) (such as ITD or ADS&CI). Additionally, the documentation shall be included in the Mission Correlation Table (MCT) and shall serve as the official record for the delegation and movement of mission in the USSS.

6. (U//~~FOUO~~) Should a USSS element want to delegate mission to a non-USSS element, the USSS element will contact SIGINT Policy to initiate a Memorandum of Understanding (MOU) between NSA/CSS and the non-USSS element as a preliminary step.

(U) Missions in the MCT

7. (U//~~FOUO~~) To ensure expedited database access to SIGINT databases, missions of SIGINT production elements and the databases associated with those missions must be recorded in, most importantly, the MCT, as well as USSIDs and supporting MOAs/MOUs and SPFs.

(U) MISSION DELEGATION CONSIDERATIONS

(U) General Mission Delegation Criteria

8. (U//~~FOUO~~) When a MDA is considering delegating a mission to a SIGINT production element, the MDA should consider carefully:

- (U//~~FOUO~~) the customer that the SIGINT production element is serving and the information needs of that customer;

- (U//~~FOUO~~) the skill level, operational tempo, and location of the SIGINT production element being considered for the mission;

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

- (U//~~FOUO~~) the nature of the mission and the skills and tools that the mission will require ([redacted] metadata analysis, reporting, collection, cryptanalysis, translation services, etc.); and

- (U//~~FOUO~~) the type of dissemination that the mission will require and the SIGINT production element's ability to perform that dissemination within the guidelines of NSA/CSS policy, guidance, and other applicable directives.

(U//~~FOUO~~) The MDA must also provide to the SIGINT production element receiving a mission a clear definition of exactly what part of a mission the element should work in order to reduce the possibility of duplication of effort across the USSS.

(U) Database Implications of Missions

9. (U//~~FOUO~~) When a MDA is considering Mission Delegation, the MDA must also consider:

- (U//~~FOUO~~) If the execution of the mission will require access to databases with sensitive content such as U.S. or Second and Third Party identities, the SIGINT production element must have the training and ability to handle such access, and may have to implement additional oversight, including designation of Intelligence Oversight Officers (IOO), query auditing, or other oversight as described in the Annex to this Directive.

- (U//~~FOUO~~) If the databases contain special source data in exceptionally controlled information (ECI) categories, the risks inherent in granting access to such data outside of NSAW and especially in a forward operation area must be carefully weighed.

- (U//~~FOUO~~) If a database contains FISA information, the MDA must be certain that the personnel are eligible for access to FISA data - i.e., under the full-time, direct operational control of DIRNSA to collect, process, analyze, and disseminate SIGINT data that supports the information needs validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. These databases entail special intelligence oversight and, depending on data type, auditing. There must be an Intelligence Oversight Officer (IOO) present with the appropriate training to oversee these responsibilities in accordance with national and NSA/CSS legal and policy guidelines. The MDA will need to coordinate these oversight requirements with O&C before delegating the mission.

(U) Information Requirements for Mission Delegations

10. (U//~~FOUO~~) Coordinating SIGINT production missions among SIGINT production elements is a crucial first step in the mission delegation process. To ensure that coordination is complete and expeditious, the MDA must have all the pertinent information gathered prior to initiating coordination. The required information includes the following categories:

- (U//~~FOUO~~) SIGINT Production Element (SPE) Attributes;
- (U) SIGINT Mission; and
- (U//~~FOUO~~) Intelligence Oversight.

(U) SIGINT Production Element (SPE) Attributes

11. (U) For the SPE gaining the mission:

a. (U//~~FOUO~~) SPE SIGINT Address (SIGAD) and PDDG (if applicable).

b. (U//~~FOUO~~) SPE Location (SCIF or T-SCIF #).

c. (U//~~FOUO~~) Is the element operating under only SIGINT authorities or will it have other authorities also? If dual authorities, what documentation authorizes this?

d. (U//~~FOUO~~) Does the element include Second Party Integrees?

(U) SIGINT Mission

12. (U) The SIGINT Mission:

a. (U//~~FOUO~~) What mission will the element be performing.

b. (U//~~FOUO~~) Sponsoring NSA Organization.

c. (U//~~FOUO~~) Effective Date of Mission Transfer.

d. (U//~~FOUO~~) Analytic Tools, Hardware, Software Requirements (include version # where applicable).

e. (U//~~FOUO~~) Databases Required (if applicable) and Auditors (if applicable).

NOTE: If mission requires access to special source collection; unminimized, unevaluated raw traffic in databases that are keyterm-searchable; and/or data resulting from Foreign Intelligence Surveillance Act (FISA) activities, please ensure this information is provided in the mission delegation documentation.

f. (U//~~FOUO~~) SPEs must have an approved SIGINT dissemination plan for all missions except SIGINT Development. The SIGINT dissemination plan should be worked out by the MDA in coordination with Information Sharing Services (S12).

(U) MISSION DELEGATION PROCESS

(U) Roles and Responsibilities

13. (U//~~FOUO~~) Once the above information has been gathered, it must be sent to the DD, A&P Global Capability Manager (GCM), or ADD who is responsible for the mission. If an authorized NCR is the MDA, the information will be used to coordinate the mission delegation with a DD, A&P GCM, or ADD prior to initiating the mission. The DDs, A&P GCMs, and ADDs are responsible for orchestrating the execution of and maintaining awareness of missions across national and tactical units throughout the global enterprise. In addition, the GCMs are responsible for appropriately connecting enterprise analytic elements in order to synchronize mission, align resources, understand and maintain analytic capabilities, and optimize prosecution of the SIGINT missions. GCMs are also tasked with building collaborative relationships with mission elements throughout the global enterprise.

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

NOTE: ~~(S//SI//REL)~~ The GCMs maintain cognizance of mission efforts across the extended enterprise, including the missions of the [redacted] [redacted] sites, which contribute to both local support and national missions. Therefore, the provisions of this Directive also apply to [redacted] sites' missions. [redacted] will work with the DDAP to ensure that the MCT accurately correlates [redacted] sites to their national and local support missions and to the applicable databases for each.

14. (U//~~FOUO~~) A&P GCMs will work with the NCRs who have been delegated mission authority to ensure that the appropriate connections are made to analysts at production centers within the global enterprise and to ensure that enterprise analysts have access to appropriate training on tools, data, and target sets. Connecting enterprise analysts with common mission interests will foster collaboration and will help the GCM to validate that the analytic processes--analysis, discovery, production--being performed under the NCR's authorities are consistent with standards established for all SIGINT analysts.

(U) The NCR Process

15. (U//~~FOUO~~) Given a SIGINT requirement for a supported customer (e.g., COCOM), the NCR with mission delegation authority will engage the appropriate NSAW element to determine if the requirement currently has NSA resources assigned to it and whether production is occurring that satisfies the requirement.

- (U//~~FOUO~~) If production is occurring, the NCR and GCM will ensure that the supported customer is on distribution for production, and will ensure that the customer's interest in that requirement is clearly understood by all relevant enterprise production elements.

- (U//~~FOUO~~) In the event that the customer determines that the NSA level of effort against the requirement does not satisfy its needs, the NCR could decide to dedicate additional (local) resources to that requirement, and the NCR will communicate this intention to the appropriate GCM for situational awareness and so that the MCT can be updated.

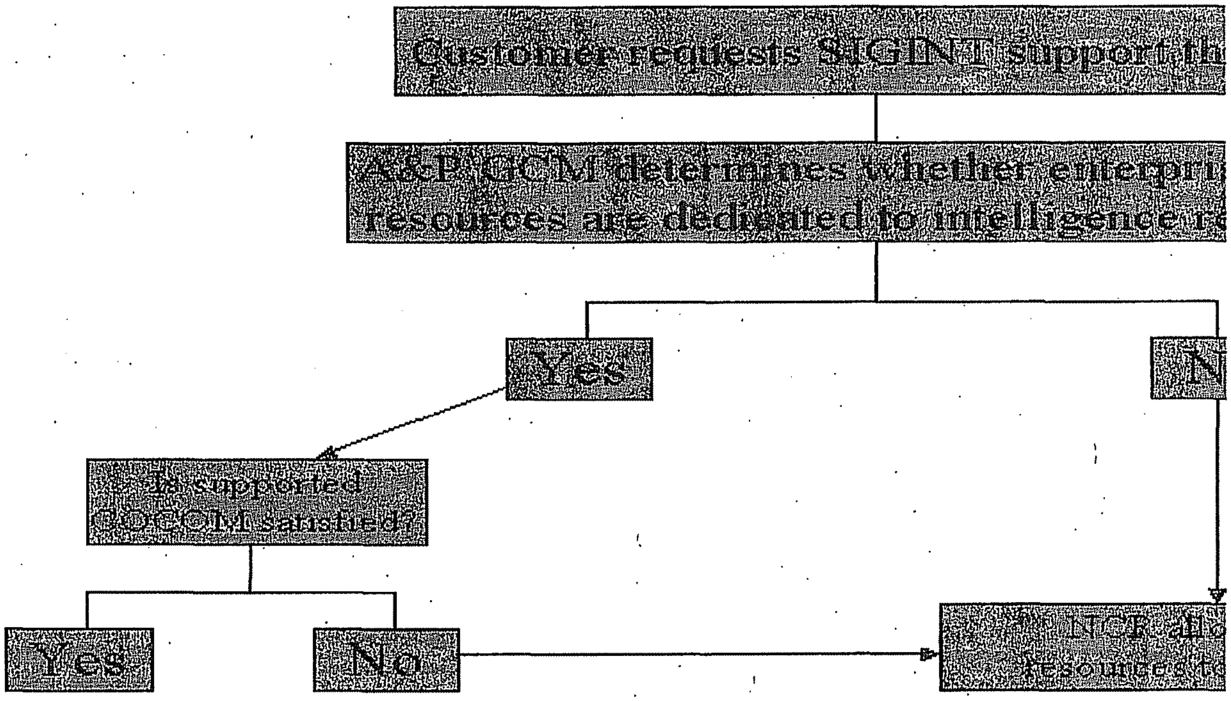
- (U//~~FOUO~~) Further, if there are no NSA resources dedicated to a customer's SIGINT requirement, the NCR could allocate local resources to that requirement and communicate that decision to the appropriate GCM for situational awareness and so that the MCT can be updated.

16. (U//~~FOUO~~) The following flowchart depicts the process for A&P-NCR engagement in determining allocation of analytic resources.

UNCLASSIFIED//~~FOUO~~

SEE SEPARATE PAGE

A&P-NCR Engager



Customer requests SIGINT support th

A&P GCM determines whether enterpri resources are dedicated to intelligence r

Yes

N

Is supported GOCCM satisfied?

Yes

No

NCR al resources t

GCM ensures linkages between all enterprise elements producir and services against intelligence requirements and negotiates witl local elements will assume enterprise responsibility for satisf

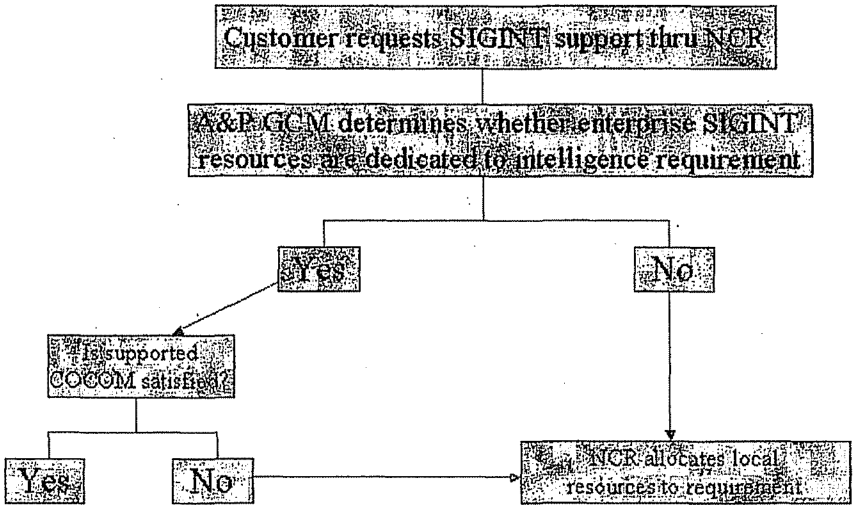
(U//~~FOUO~~) SIGINT Production Standards

17. (U//~~FOUO~~) All SIGINT products, target packages, responses to requests for information (RFIs), and SIGINT end-product reports must adhere to NSA corporate standards for SIGINT reporting as described in:

- (U//~~FOUO~~) USSID CR1400, "SIGINT Reporting";

- (U//~~FOUO~~) USSID CR1500, "Time-Sensitive SIGINT Reporting";

A&P-NCR Engagement



Customer requests SIGINT support thru NCR

A&P GCM determines whether enterprise SIGINT resources are dedicated to intelligence requirement

Yes

No

Is supported COCOM satisfied?

Yes

No

NCR allocates local resources to requirement

GCM ensures linkages between all enterprise elements producing SIGINT products and services against intelligence requirements and negotiates with NCR to determine if local elements will assume enterprise responsibility for satisfying requirement

UNCLASSIFIED//~~FOUO~~

- (U//~~FOUO~~) USSID CR1501, "Handling of Critical (CRITIC) Information";

- (U//~~FOUO~~) All standing and ad hoc NSA reporting guidance ("go reporting-policy" on NSANet); and

- (U//~~FOUO~~) Documented in the SIGINT dissemination plan.

18. (U//~~FOUO~~) All SIGINT collection must adhere to NSA Corporate standards for SIGINT collection as described in:

- (U//~~FOUO~~) USSID DA3110, "Collection Management Procedures";

- (U//~~FOUO~~) USSID DA3625, "The Plop Format for Raw Traffic Forwarding";

- (U//~~FOUO~~) USSID DA3620, "Collected Signals Data Format";

- (U//~~FOUO~~) Other USSIDs as noted in Table 3 of USSID DA3000; and

- (U//~~FOUO~~) All standing and ad hoc NSA collection guidance.

(U) Accessibility to SIGINT Products

19. (U//~~FOUO~~) In addition to adherence to corporate standards for SIGINT product, target packages, responses to RFIs, SIGINT end-product reports, and any other SIGINT dissemination product must be corporately archived so that they are accessible and retrievable across the SIGINT enterprise. This ensures that the results of SIGINT analytic efforts are known and available for viewing by others with similar mission responsibilities, and aids with target continuity. A corporate archive of the work already done will expedite the time needed to produce intelligence information on a target. A corporate archive will also provide a permanent record of SIGINT dissemination for accountability purposes.

(U) Developing and Maintaining Analytic Skill Sets

20. (U//~~FOUO~~) Access to SIGINT databases requires training, not only on the content of the databases, but on the tools used to manipulate and view the data and on the intricacies of the target that could impact on interpretation of the data. Given the rapidly changing target environments, new accesses, and the development of new analytic tools and capabilities, analysts must be afforded initial training on databases and continuing education and training to keep skills and capabilities current. All SIGINT producing organizations must adhere to the same analytic standards. The MDA must identify a plan to ensure the analysts have the proper training and maintenance of skills required to handle SIGINT to which they are being granted access. Additionally, the NCR must identify a plan to ensure proper training and maintenance of skills required to handle the SIGINT data to which it is being granted access. Additionally, the NSA forward element should evaluate if the supported customer's non-NSA SIGINT assets can contribute to an overall solution to gaps and limited resources, and if so, should so inform the appropriate A&P GCM. These analysts would also require the same

strict standards, oversight, accountability, transparency and training as NSA SIGINT analysts.

(U) Coordination

21. (U//~~FOUO~~) Coordination is in fact the key to success and transparency in our SIGINT Enterprise. The ability of SIGINT analysts working the same targets/topics to share analytic perspectives, challenge interpretations, and gain new insights is not only invaluable to strengthening analysis, but also is an imperative to optimizing mission effectiveness. Multiple SIGINT analytic entities following the same targets and researching the same data sets could result in conflicting reporting reaching customers, leaving the customer to determine which interpretation of the SIGINT is correct. The best way to minimize this is constant communication between the SIGINT elements performing the analysis. This will not, and should not, eliminate competing analysis, but it can provide a venue for resolution of analytic differences and anticipate questions in order to better serve the customer.

(U) Completion of Mission Delegation

22. (U//~~FOUO~~) Once all information is identified and all coordination is complete, the mission delegation must be documented and signed by the MDA and copies sent to S2 for incorporation in the Mission Correlation Table, to SIGINT Policy for incorporation in appropriate USSIDs and site profiles, the Office of Oversight and Compliance and the SIGINT production element gaining the mission.

(U) OVERSIGHT

(U) General Oversight Expectation

23. (U//~~FOUO~~) Individuals, managers, and assigned 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 put in place to cover 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) Minimum Oversight Activity for Access

24. (U//~~FOUO~~) When a new mission requiring database access is assigned to an element, the mission and database access may be initiated once the following oversight steps have been taken:

- (U//~~FOUO~~) On-site IOOs have been identified to and trained by Oversight and Compliance.
- (U//~~FOUO~~) Individuals, managers, and IOOs have been trained on handling requirements for data involved and confirmation of the training has been forwarded to the A&P Operational Support Staff (DL s203_military) for recording in the MCT.
- (U/~~FOUO~~) MDAs have confirmed **in writing** to O&C that due diligence was performed and every effort was made to meet the standard of oversight required under the Annex, oversight requirements, the oversight identified was the best oversight possible for the situation, oversight is **in place** covering all four phases of production and all five key areas of oversight, and they acknowledge their commitment to remedy any oversight gaps identified by O&C.

(U) Subsequent Requirements

25. (U//~~FOUO~~) MDAs of the mission location will also provide the following within the times specified:

- (U//~~FOUO~~) ***within 30 days of mission activation***, the IOOs will submit to the MDA and O&C simultaneously a full written report on the oversight implemented at the location, including steps taken relative to all four phases of production and all five key areas of oversight. This report will include copies of any rules, policies, or procedures drafted to support the mission's intelligence oversight. If oversight does not meet the standards described in the Annex, the report must include defensible explanations for implementing less-than-optimal oversight conditions and the steps taken in attempting to achieve them.

NOTE: After reviewing the submitted report, should O&C have concerns regarding oversight implementation, especially regarding any activities where SIGINT is handled near non-SIGINT personnel or where FISA data is handled near non-FISA-cleared personnel, O&C will coordinate with the organization and the NCR to arrive at an appropriate solution.

(U//~~FOUO~~) O&C will use this report to suggest refinements, surface risks for SID leadership, or to compare against reality when the mission comes under review by O&C or the NSA Inspector General (IG). If the report is not received within the 30 days, O&C will notify the MDA who will then ensure that the report is submitted. Every individual in the leadership chain for the SIGINT mission location remains accountable for ensuring the compliance of the mission within their element; however the MDA is ultimately accountable for the intelligence oversight of the missions he authorizes.

- (U//~~FOUO~~) ***prior to the end of the quarter*** during which access is activated, IOOs will work with O&C to identify IG reporting path(s) for those participating in the mission.

(U) DEFINITIONS

(U) Approved SIGINT Dissemination Plan

26. (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) Cryptologic Center (CC)

27. (U//~~FOUO~~) The United States Cryptologic System (USCS) relies heavily on five major geographically dispersed enterprise locations, called Cryptologic Centers (CCs) to perform critical USCS mission operations which primarily focus on Analysis and Production. The five CCs (NSA/CSS Colorado, NSA/CSS Georgia, NSA/CSS Hawaii, NSA/CSS Texas, NSA/CSS Washington (Operations)) form the backbone of the NSA/CSS Global Net-centric Cryptologic Enterprise and are responsible for a full range of cryptologic operations as

assigned by the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) through the Signals Intelligence Directorate (SID) and the Information Assurance Directorate (IAD), with local support from integrated enabler elements.

(U) Foreign Intelligence Surveillance Act (FISA) Data

28. (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) Global Capabilities Manager (GCM)

29. (U//~~FOUO~~) The focus of the GCM is on developing/implementing an end-to-end analytic and production strategy for his mission area that optimizes and leverages the entire cryptologic enterprise. The GCM's role is to ensure that the missions area strategy is comprehensive, includes and leverages Intelligence Community (IC) and foreign partners, and optimizes Production Center and other cryptologic resources to maximum effectiveness to produce SIGINT products and services in satisfaction of customer needs. Additionally, the GCM will preserve and promote the technical health of the workforce. The GCM acts under the oversight of the appropriate Group Chief to assign missions, define mission authorities, and work with relevant organizations to establish policies, processes, and standards for the mission area that are in accordance with corporate goals and criteria. The GCM shall designate the Primary Production Center Manager (PPCM), another Production Center Manager (PCM), or a member of the Production Center to act on his or her behalf during an absence.

(U) Metadata

30. (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 (MCT)

31. (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 units SIGINT Address (SIGAD), the location, the mission, the intelligence oversight auditor, authorized databases, dates, and other information necessary to authorize access to raw SIGINT data.

(U) Mission Delegation Authority (MDA)

32. (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.

(U) Payload

33. (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) Service Cryptologic Elements (SCEs)

34. (U//~~FOUO~~) 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

35. (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 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. (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

36. (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) Traditional and Non - Traditional SIGINT Production Elements

37. (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.

(U//~~FOUO~~) 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. (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.

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

d. ~~(C//REL)~~ Active Duty Service Cryptologic Elements (SCEs) [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.

---

38. (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 or Third Party SIGINT partners.

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

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

e. (U//~~FOUO~~) Special Cryptologic Partners (components of the U.S. Special Operations Command (SOCOM)).

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

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

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

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.

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.

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

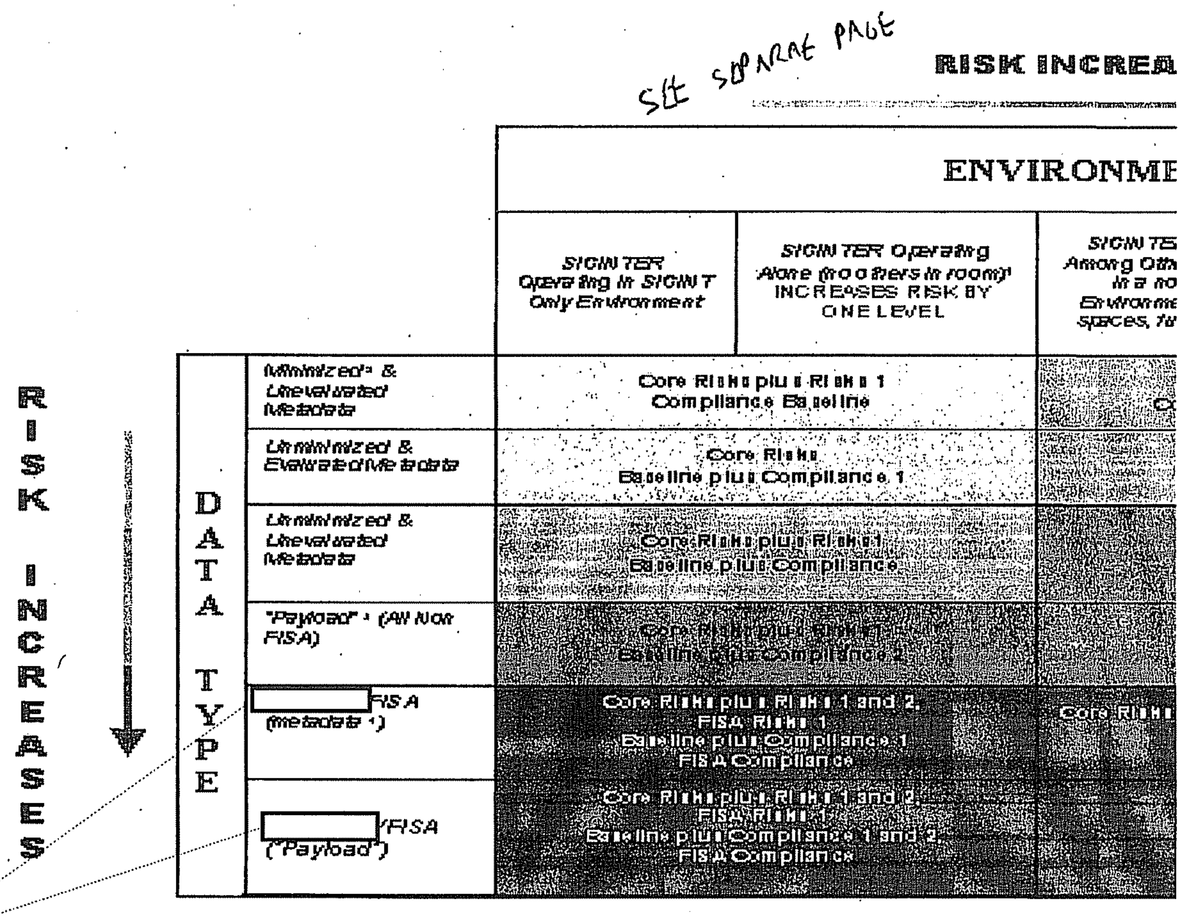
NOTE 2: (U//~~FOUO~~) IAD is increasingly collaborating with SID in SIGINT production activities through joint elements such as the NSA/CSS NTOC and through the integration of IAD personnel into SID elements. When collaborating with SID, certain IAD personnel may be designated and documented as working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

(U) United States SIGINT System (USSS)

39. (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 INCREA

R I S K I N C R E A S E S

		ENVIRONME		
		SIGINTER Operating in SIGINT Only Environment	SIGINTER Operating Alone (no others in room)¹ INCREASES RISK BY ONE LEVEL	SIGINTE Among Oth in a no Environme spaces, fu
D A T A T Y P E	Minimized² & Unevaluated Metadata	Core Risks plus Risks 1 Compliance Baseline		C
	Unminimized & Evaluated Metadata	Core Risks Baseline plus Compliance 1		
	Unminimized & Unevaluated Metadata	Core Risks plus Risks 1 Baseline plus Compliance		
	"Payload" ³ (All Non FISA)	Core Risks plus Risks 1 Baseline plus Compliance 2		
	[redacted] FISA (metadata ⁴)	Core Risks plus Risks 1 and 2. FISA Risks 1 Baseline plus Compliance 1 FISA Compliance		Core Risks
	[redacted] /FISA ("Payload")	Core Risks plus Risks 1 and 2. FISA Risks 1 Baseline plus Compliance 1 and 2. FISA Compliance		

(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, the text of an [redacted] [redacted] or the voice data of a phone call [redacted]

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

[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; rather, every situation and data type also has nuances that involve additional risk

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 Risks plus Risks 1 Compliance Baseline		Core Risks plus Risks 1 and 2 Compliance Baseline plus Compliance 3	
Unminimized & Evaluated Metadata	Core Risks Baseline plus Compliance 1		Core Risks plus Risks 2 Baseline plus Compliance 1 and 3	
Unminimized & Unevaluated Metadata	Core Risks plus Risks 1 Baseline plus Compliance		[illegible]	
"Payload"[4] *(All Non FISA)*	[illegible]		[illegible]	
[redacted] *FISA (metadata*[4]*)*	Core Risks plus Risks 1 and 2, FISA Risks 1 Baseline plus Compliance 1 FISA Compliance		Core Risks plus Risks 1, FISA Risks 1 and 2 Baseline plus Compliance 1 and 3, FISA Compliance	
[redacted] *FISA ("Payload")*	Core Risks plus Risks 1 and 2, FISA Risks 1 Baseline plus Compliance 1 and 2, FISA Compliance		Core Risks plus Risks 1 and 2, FISA Risks 1 and 2 Baseline plus Compliance 1, 2 and 3, FISA Compliance	

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

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~~