UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

USSID SP0019

(U) NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy

ISSUE DATE: 13 November 2012

REVISED DATE:

(U) OFFICE OF PRIMARY CONCERN:

National Security Agency/Central Security Service (NSA/CSS), Signals Intelligence Directorate, Office of Oversight and Compliance

(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION

(U) Topic of Promulgation

(U//~~FOUO~~) This USSID outlines the oversight and compliance policy and procedures governing Signals Intelligence (SIGINT) activities by elements of the United States SIGINT System (USSS) operating under the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). Oversight and compliance are the functions USSS elements perform to ensure that SIGINT activities comply with the laws, regulations, and policies governing those activities in a manner that protects the constitutional privacy rights of U.S. persons. All individuals, managers, and oversight personnel either conducting, performing research on or creating capabilities to support or perform collection, processing, analysis, production, retention, and dissemination of SIGINT throughout the USSS are responsible for following these laws, regulations, and

policies.

(U//~~FOUO~~) The Chief of the SIGINT Directorate's (SID) Office of Oversight and Compliance (SV) is the SIGINT Director's Senior Compliance Executive responsible for verifying USSS activities are conducted in a manner consistent with:

Executive Order 12333, as amended, "United States Intelligence Activities," dated 4 December 1981, revised 2008;

DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," dated 11 December 1982;

NSA/CSS Policy 1-23, "Procedures Governing NSA/CSS Activities That Affect U.S. Persons," dated 11 March 2004, revised 16 September 2011;

USSID SP0018, "Legal Compliance and U.S. Persons Minimization Procedures," dated 25 January 2011; the Foreign Intelligence Surveillance Act (FISA), as amended, 10 July 2008; Protect America Act (PAA);

USSID AP2231, "SIGINT Targeting of Maritime Vessels," dated 19 December 2008;

USSID SP0009, "Host Nation Collection," dated 28 October 2011; and

SID Management Directive (SMD) 424, "SIGINT Development Communications Metadata Analysis," dated 29 November 2010, revised 8 November 2012.

USSID FA6001, "Second Party SIGINT Relationships," dated 22 August 2012, and

USSID FA6101, "Third Party SIGINT Relationships," dated 31 October 2007, revised 15 April 2013.

(U) USSID Edition

(U//~~FOUO~~) This is the initial issuance of this USSID.

(U) Legal Protection of Sensitive Information

(U//~~FOUO~~) This USSID contains sensitive information that is legally protected from release to any member of the public and is to be used only for official purposes of the NSA/CSS, Service Partners, and USSS customers.

(U) Handling of USSID

(U//~~FOUO~~) Users must adhere to all classification and handling restrictions (see NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Manual," dated 23 November 2004, revised 8 January 2007) when:

(U) storing hard or soft copies of this USSID; or

(U) hyperlinking to this USSID.

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

(U) Location of Official USSID

(U//~~FOUO~~) The Chief, SIGINT Policy will maintain and update the current official USSID on NSANet (go USSID). As warranted, the USSID will be available on INTELINK.

(U) Access by Contractors and Consultants

(U) For NSA/CSS elements to include the SIGINT Extended Enterprise:

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

(U) Outside NSA elements:

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

[redacted] (b)(3)-P.L. 86-36

(U) Access by Third Party Partners

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

(U) If a shareable version of this USSID is requested:

(U) Refer to USSID SP0002, Annex B, "The USSID System," dated 14 October 2008; and

(U) Contact the appropriate Country Desk Officer in the NSA/CSS Foreign Affairs Directorate.

(U) Executive Agent

(U) The executive agent for this USSID is:

//s//

TERESA H. SHEA
Signals Intelligence Director

(U) USSID CHANGES

CHANGE 1	13	November 2012
CHANGE 2	26	November 2013
CHANGE 3	29	January 2014

(U) TABLE OF CONTENTS

SECTION 1 - (U) PURPOSE

(U) Purpose of USSID

1.1. (U//~~FOUO~~) This USSID applies to all SIGINT activities in the USSS conducted under the authorities of the DIRNSA/CHCSS. It provides guidance for everyone supporting, conducting, or engaging in the execution of SIGINT authorities in compliance with the laws, regulations, and policies designed to protect U.S. persons' privacy rights. Specifically, it:

(U//~~FOUO~~) Defines and explains the purpose of SIGINT oversight and compliance;

(U//~~FOUO~~) Provides guidance on the oversight roles and responsibilities of SIGINT personnel in the USSS based on the minimization policy and procedures required by USSID SP0018, to protect the privacy rights of U.S. persons;

(U//~~FOUO~~) Outlines the oversight and/or compliance responsibilities of all members of the USSS, regardless of location, i.e., anywhere in the Global Cryptologic Enterprise or tactical units. For guidance concerning Second Party personnel gaining access to raw SIGINT data, and the subsequent oversight and compliance responsibilities, refer to SMD 427, "Access to Data for Second Party Personnel Engaged in SIGINT Production," dated 1 August 2009; SMD 421, "United States SIGINT System Database Access," dated 30 April 2007, revised 25 March 2008, and USSID CR1610, "SIGINT Production and Raw SIGINT Access," dated 25 August 2005, revised 29 March 2012.

(U//~~FOUO~~) Describes the SIGINT compliance program to include the "Five Foundational Components of Compliance" and the procedures which, when implemented, provide reasonable assurance of adherence to specific authorities and policies governing SIGINT activities.

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

SECTION 2 - (U) BACKGROUND

(U) Oversight and Compliance

2.1. (U//~~FOUO~~) SIGINT oversight is the independent inspection of SIGINT activities for quality and performance. Independent oversight is conducted primarily by entities external to the SID, e.g., NSA/CSS Office of the Inspector General (OIG), Service Cryptologic Component (SCC) Inspector General, Service Partner Inspector General, NSA Office of the General Counsel (OGC), and Congressional overseers.

2.2. (U//~~FOUO~~) SIGINT compliance is defined as verifiable conformance with the rules that govern SIGINT activities, as established in various executive orders, statutes, directives, and policies. The difference between oversight and compliance is that compliance is everyone's responsibility. Oversight is the review of SIGINT activities to verify they are conducted in a manner that protects the constitutional privacy rights of U.S. persons.

2.3. (U//~~FOUO~~) The NSA/CSS compliance program is intended to assist individuals to operate within the established mission compliance standards and to provide overseers with confidence that the USSS is conducting its activities within legal parameters. NSA/CSS' mission compliance standards are implemented through the Comprehensive Mission Compliance Program (CMCP), managed by the NSA/CSS Office of the Director of Compliance (ODoC).

(U) The SIGINT Compliance

2.4. (U//~~FOUO~~) The SIGINT compliance program is aligned with the CMCP and provides guidance specific to SIGINT functions, i.e., collection, processing, analysis,

Program

production, retention, and dissemination. The goal is to protect U.S. persons' privacy, while enabling the USSS to conduct its SIGINT mission to the fullest extent of the law. Underpinning the SIGINT compliance program are NSA/CSS' Five Foundational Components of Compliance (Section 4).

SECTION 3 - (U) RESPONSIBILITIES

(U) General

3.1. (U//~~FOUO~~) The DIRNSA/CHCSS is responsible for implementing an effective program for both oversight and compliance. Independent oversight is conducted by the NSA/CSS OIG and the OGC, while compliance is everyone's responsibility: individuals in every mission area and every work role in those mission areas, managers, Intelligence Oversight Officers (IOOs)/Compliance Leads/Compliance Officers (hereafter referred to as IOO), and for the SIGINT enterprise, SV. All locations conducting SIGINT activity, whether at NSA/Washington (NSAW), the extended enterprise, or at USSS elements globally dispersed, will implement appropriate physical protection measures to reduce the risk of personnel not authorized access to Raw SIGINT data from seeing, hearing, or otherwise gaining access to raw SIGINT data (see Annex A of this USSID).

(U) Offices of the Inspector General and General Counsel

3.2. (U//~~FOUO~~) The OIG is the agent for individual and organizational integrity within the Agency. It has the authority to conduct inspections, audits, investigations, special inquiries, and other reviews relating to the programs or operations of NSA/CSS. This oversight authority promotes economy, effectiveness, efficiency, and accountability within the Agency; ensures compliance with laws and regulations; and, assists in detecting and preventing fraud, waste, and mismanagement in NSA/CSS programs and operations.

3.3 (U//~~FOUO~~) OGC also has an oversight role with regard to providing legal interpretation and guidance. The OGC's Intelligence Law Practice Group is responsible for all legal matters relating to NSA/CSS' SIGINT activities. These responsibilities include providing legal advice and oversight on all matters relating to the collection, processing, analysis, production, retention, and dissemination of SIGINT information to ensure that operational activities are in compliance with legal and regulatory requirements.

3.4 (U//~~FOUO~~) The NSA/CSS OGC and NSA/CSS OIG will coordinate with similar elements of USSS organizations with regard to legal interpretations and guidance related to oversight of SIGINT operations performed under DIRNSA authority.

(U) SID Oversight and Compliance (SV)

3.5. (U//~~FOUO~~) SV is responsible for implementing the SIGINT component of NSA/CSS' CMCP. SV, in conjunction with ODoC, establishes standards for execution of SIGINT authorities with reasonable assurance of adherence to the laws, policies, and regulations that govern the handling of SIGINT with respect to the protection of U.S. persons privacy. SV's mission and functions are available on the SV home page.

(U) Individuals and Managers

3.6. (U) Every individual must comply with applicable laws, statutes, directives, and regulations by:

(U) Staying current on the governing documents and the compliance standards that implement them (Section 4.4);

(U) Staying current on individual accountability for the rules and standards;

(U//~~FOUO~~) Reporting any non-compliant activity to management, an IOO, SV, and OIG (Section 4.8);

(U) Taking measures to reduce the risk of non-compliant activity and to prevent future non-compliant activity (Section 4.9); and

(U) Exercising due diligence to remain compliant, i.e., make every reasonable attempt to adhere to the rules and standards.

3.7. (U//~~FOUO~~) Managers are accountable for the compliance within their organization and for implementing the Five Foundational Components of Compliance.

3.8. (U) Access sponsors are responsible for:

(U) Ensuring that there is an adequate number of trained auditors available to support their respective organizations;

(U) Knowing the rules and standards;

(U) Understanding what they and their employees are accountable for as identified in approved mission compliance standards;

(U) Verifying implementation of what they and their employees are accountable for;

(U) Evaluating results of root cause analysis and recommending institutional changes to compliance standards; and,

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

(U) Assessing the true need for additions or changes to local procedures and safeguards.

(U//~~FOUO~~) Additional [redacted] Roles and Responsibilities are contained in SIGINT POLICY MEMORANDUM 2012-02, "Management of Access to SIGINT Data in NSA Repositories."

(U) Intelligence Oversight Officers (IOO)

3.9. (U//~~FOUO~~) IOOs provide day-to-day oversight and compliance guidance for SIGINT activities. IOOs, who are essentially an extension of SV, serve as the "go-to" person for compliance implementation and advise local management on problems, risks, and mitigation procedures.

3.10. (U//~~FOUO~~) See Annex B to this USSID for more details on qualifications and responsibilities of the IOO, as well as the criteria for an off-site IOO.

SECTION 4 - (U) POLICY AND PROCEDURES

(U) Five Foundational Components of Compliance

4.1. (U//~~FOUO~~) The Five Foundational Components of Compliance which provide the framework for the policy and procedures necessary to remain compliant are:

1. (U) Familiarity with the current rules and standards;
2. (U) Awareness of individual accountability for the rules and standards;
3. (U) Verification of rules and standards implementation;
4. (U) Reporting of non-compliant activity; and
5. (U) Implementation of corrective measures, if necessary.

(U) Rules and Standards

4.2. (U//~~FOUO~~) The regulations governing SIGINT activity have been established in executive orders, directives, policies, and mission compliance standards, as well as in legal statutes. The following intelligence oversight (IO) documents are foundational for all NSA/CSS SIGINT mission activities to include research and development:

(U) **Executive Order 12333,** as amended 2008, "United States Intelligence Activities," establishes the overall framework for the conduct of intelligence activities by the Intelligence Community (IC), and specifies the scope of NSA/CSS' authorities to conduct its routine foreign intelligence mission;

(U) **DoD Regulation 5240.1-R,** "DoD Intelligence Activities," dated December 11, 1982. sets forth procedures governing the activities of Department of Defense (DoD) intelligence components that affect U.S. persons. These procedures include Attorney General-approved procedures for certain activities of intelligence components that affect U.S. persons, which are required to implement E.O. 12333 as amended. A classified annex establishes procedures specific to the conduct of SIGINT activities;

(U) **NSA/CSS Policy 1-23,** "Procedures Governing NSA/CSS Activities that Affect U.S. Persons," dated 16 September 2011, establishes procedures and assigns responsibilities to ensure that NSA's SIGINT mission is conducted in a manner consistent with the privacy rights of U.S. persons; and

(U) **Directive-Type Memorandum (DTM) 08-052**, "DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters," dated 17 June 2009 (incorporating change 2, 22 August 2011).

4.3. (U) In addition, the following IO documents are foundational for SIGINT activities including research and development and for those creating the tools for training:

(U) **USSID SP0018**, "Legal Compliance and U.S. Persons Minimization Procedures," dated 25 January 2011, prescribes policies and procedures and assigns responsibilities to ensure that SIGINT missions and functions are conducted in a

manner that safeguards the constitutional rights of U.S. persons; and

(U) **NSCID 6**: "National Security Council Intelligence Directive No. 6, Signals Intelligence," dated 17 February 1972, defines and prescribes the conduct of SIGINT activity among various intelligence agencies.

4.4. (U//~~FOUO~~) Other NSA/CSS policies, USSIDs, and SID Management Directives (SMDs) also provide guidance on implementing SIGINT authorities. Mission compliance standards contain the minimal criteria, procedures and safeguards for a given mission function which, when implemented, provide a reasonable assurance of adherence to specific authorities and governing documents. Roles and responsibilities for implementation, both human and machine, of these standards are identified as well. Mission compliance standards for SIGINT correspond to a set of identified SIGINT functions where the compliance risk is greatest.

(U) Training/ Individual/ Accountability

4.5. (U//~~FOUO~~) Every individual involved in a SIGINT activity – including those who conduct, manage, support and provide oversight to it – must be knowledgeable of the current rules governing SIGINT activities. Furthermore, these same individuals must be aware of their individual accountability for those rules, as identified in governing documents and mission compliance standards. The SV homepage provides Oversight and Compliance course information and enrollment instructions. These courses are available on NSANet and JWICS.

(U//~~FOUO~~) All personnel engaged in activities that include access to SIGINT or visibility of raw SIGINT data must successfully complete OVSC1100, "Overview of Signals Intelligence Authorities;" and either OVSC1800, "Legal Compliance and Minimization Procedures" or OVSC1806 "USSID SP0018 Training for Technical Personnel within 30 days of being assigned to a SIGINT mission and prior to access being granted, and annually thereafter (Reference Compliance Advisory 044).

(U//~~FOUO~~) **For Intelligence Oversight Officers**: In addition to the foundational IO training, IOOs are required to successfully complete OVSC2201, "Intelligence Oversight Officer Training," and any specific training pertinent to the data being accessed. All training requirements must be completed before any analyst at the IOO's location gains access to raw SIGINT.

(U//~~FOUO~~) **For auditors**: In addition to the foundational training, auditors must complete OVSC3101, "NSA Raw Traffic Database Auditor Training," and any specific training pertinent to the data being accessed.

(U//~~FOUO~~) **For specific accesses:** In some cases, additional training for access to some SIGINT data, such as Foreign Intelligence Surveillance Act (FISA), is needed. See the SV web pages under "training" for details on what training is required for specific accesses.

(U) Oversight

4.6. (U//~~FOUO~~) Compliance verification provides an independent examination to evaluate the effectiveness of safeguards implemented to enable compliance. Oversight evaluates the effectiveness of the implemented compliance safeguards. Oversight activities assist in uncovering shortcomings that may exist within the technical,

operational, and management safeguards implemented for SIGINT activities. Awareness of these shortcomings provides the mission element with the opportunity to recommend modifications to safeguards, where needed, to better manage compliance risks.

4.7. (U//~~FOUO~~) Within the SID, SV is responsible for carrying out the compliance verification mission, to include supporting IOOs in implementing SIGINT compliance programs. SV meets its responsibility by undertaking three broad categories of activities:

(U//~~FOUO~~) **Site Assistance Visits:** SV visits USSS locations with an authorized SIGINT mission to examine the procedures, processes, and safeguards implemented to enable the conduct of SIGINT activities in a compliant manner. SV assesses the effectiveness of these procedures against existing standards, confirms that safeguards are operating as intended, and recommends potential improvements. Site assistance visits also provide an opportunity for SV to educate USSS personnel on compliance goals and requirements;

(U//~~FOUO~~) **Super Audits:** It includes sampling reviews of queries against raw traffic databases to ensure compliance with U.S. laws and procedures that govern SIGINT activities and the protection of U.S. persons.

(U//~~FOUO~~) **Compliance Verification:** Activities include, but are not limited to, independent verification and validation testing of established purge processes and procedures. SV may also undertake other verification activities to assess compliance.

(U) Reporting Incidents of Non-Compliance

4.8. (U//~~FOUO~~) All incidents of SIGINT mission non-compliance must be reported to SV (see section 4.9. for specific reporting guidance) and the OIG in accordance with established guidelines as follows:

(U) **Who should report an incident?**
(U//~~FOUO~~) Anyone who identifies a compliance problem should report the incident.

(U) **What is reportable activity?**
(U//~~FOUO~~) Any conduct that may be non-compliant with an Executive Order, Presidential Directive, or DoD policy/regulation, NSA/CSS Directives, SID Management Directives, and USSIDs governing SIGINT activities. Non-compliant activity includes, but is not limited to:

- (U) Mishandling of U.S. persons information;
- (U//~~FOUO~~) Queries against raw SIGINT data which are inadvertently, intentionally, or carelessly likely to target/retrieve United States or Second Party communications;
- (U) Actively searching against raw SIGINT data for purposes outside the scope of your mission or which serve no foreign intelligence purpose;
- (U) Access to raw SIGINT data without proper authority; and
- (U) Improper dissemination/handling of SIGINT.

(U) **When and how should the incident be reported?**
(U//~~FOUO~~) SIGINT mission incident reporting is the responsibility of every

individual across the SIGINT enterprise. An incident must be reported to local management, SV, and the OIG, with a copy sent to the sponsoring mission owner, upon recognition, or as soon as practicable, and quarterly as input to the IO Quarterly Report. Updates to the initial incident report must be filed as additional information becomes available. For FISA and FISA Amendments Act (FAA) incidents, NSA/CSS is responsible to also report incidents immediately upon recognition to the NSA/CSS OGC, which may report the information to external overseers.

4.9. (U//~~FOUO~~) Additional guidance, to include specific reporting requirements, procedures, and examples of reportable incidents, is available on both the SV home page ("go sv") under "Reporting Incidents" and on the OIG home page ("go ig") under "Intelligence Oversight." Those without JWICs access may use email on SIPRNet or the NSA/CSS Secure Telephone System (NSTS) to report incidents to their IO POC and the POC will submit the incidents via NSANet.

(U) Take Corrective Measures as Necessary

4.10. (U) When non-compliant activities are detected, the following actions must be taken:

(U//~~FOUO~~) The activity/action that caused the non-compliant situation must be stopped immediately and the situation closely monitored to verify that the problem has been resolved. Specific corrective actions depend on the situation, but may include de-tasking of selectors, stopping database queries, cancelling reports, etc.

(U//~~FOUO~~) If the incident is FISA-related, it must be reported to the OGC, which then handles reporting to external entities. See information in section 4.9. on details for reporting FISA incidents.

(U//~~FOUO~~) Adjustments to address non-compliance root causes or actions to correct or suspend non-compliant outcomes.

SECTION 5 – (U) GLOSSARY

(U) Auditing

(U//~~FOUO~~) The process USSS elements and overseers use to review queries made against unevaluated, unminimized (raw) SIGINT data or repositories to ensure that the queries are compliant with U.S. laws and procedures that govern SIGINT activities. The types of auditing are:

(U//~~FOUO~~) **Active Auditing:** The review of queries against raw SIGINT data or repositories that offer a significant risk of violating the privacy rights of U.S. persons (also known as post-query review). Any system, tool, database, or process which enables a user to conduct alpha-numeric searches against raw SIGINT content is actively audited. This function is performed by the elements of a SIGINT mission;

(U//~~FOUO~~) **Passive Logging (also known as Passive Auditing)**: The baseline auditing requirement imposed on raw SIGINT data and repositories to record information concerning their use. Passive logging tracks a user's queries of raw SIGINT on a given

system and may include a variety of information ranging from simple sign-in, sign-out times to the specific details of mouse clicks on a screen. The logs are not actively reviewed but are stored for potential compliance review at the discretion of SV. This function is performed by the system;

(U//~~FOUO~~) **Spot Checking:** Process of auditing a portion or sampling of the queries executed within specific raw SIGINT data or repositories that have been approved for this type of auditing. This function is performed by the elements of a SIGINT mission; and

(U//~~FOUO~~) **Super Auditing:** The independent review of activities conducted against raw SIGINT systems, tools, or databases. This function is performed by SV.

(U) Auditor

(U) See Post-Query Reviewer.

(U) Collection

(U) The intentional tasking or selection of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record (USSID SP0018).

(U) Compliance

(U) Verifiable conformance with a set of clearly defined rules.

(U) Compliance Standards

(U) The minimal criteria, procedures, and safeguards for a given mission function which, when implemented, provide a reasonable assurance of adherence to specific authorities and governing documents.

(U) Due Diligence

(U) Making every attempt to ensure that all compliance measures have been implemented during all phases of SIGINT Production.

(U) FISA Amendments Act (FAA)

(U) Amendments to the FISA that define additional procedures regarding certain persons outside the United States for electronic surveillance with a foreign intelligence purpose.

(U) Foreign Intelligence

(U) Information that relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons (USSID SP0018).

(U) Foreign Intelligence Surveillance Act (FISA) as amended, 10 July 2008

(U) Governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. The Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States, all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy.

The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General (USSID SP0018, Annex A).

(U) Intelligence Oversight Officer (IOO)

(U//~~FOUO~~) Individual who conducts day-to-day oversight of SIGINT activities on behalf of management at a location where a SIGINT mission is being conducted. The IOO advises management on compliance problems and risks, oversight implementation, and risk mitigation.

(U) Intelligence Oversight Quarterly Report (IO Quarterly Report - formerly known as the IG Quarterly Report)

(U//~~FOUO~~) A quarterly report summarizing any SIGINT activity that is conducted without necessary authority, in violation of a specific authority, or in violation of the general authorities, restrictions, directives, and policies that govern SIGINT activities. SID Oversight and Compliance submits the Intelligence Oversight Quarterly Report to the NSA/CSS OIG based on input from all organizations directly subordinate to the SIGINT Director.

(U) Minimization

(U//~~FOUO~~) Specific SIGINT procedures that, considering the purpose and technique of the particular surveillance, lessen the acquisition and retention, and prohibit the dissemination of non-publicly available information concerning unconsenting U.S. persons consistent with the United States need to obtain, produce, and disseminate foreign intelligence and counterintelligence information (USSID CR1610).

(U) Oversight

(U) The review of SIGINT activities to verify they are conducted in a manner consistent with the laws, regulations, and policies designed to protect the constitutional privacy rights of U.S. persons. Oversight is conducted primarily by independent entities, e.g., the Office of Inspector General and Congressional overseers, to ensure objectivity when assessing the performance of compliance efforts.

(U) Passive Logging (also known as Passive Auditing)

(U) See Auditing

(U) Post Query Reviewer

(U//~~FOUO~~) A civilian or military person working a SIGINT mission carrying all required compliance training and accesses who is familiar with the targets and types of queries executed within a SIGINT mission. The query reviewer will verify that queries executed by their assigned analysts are in compliance with the laws and policies governing SIGINT targeting. The query reviewer ensures the documentation and forwarding of non-compliant query activity through appropriate incident reporting channels.

(U) Query

(U//~~FOUO~~) Using selectors to search repositories, which may include U.S. persons'

information, to find data of potential intelligence value for follow-on analysis.

(U) Questionable Activity

(U) Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive Order or Presidential directive, including E.O. 12333 as amended or applicable DoD policy and regulations. Any activity that is believed to be unlawful or contrary to Executive Orders, Presidential Directives, or DoD policies and regulations.

(U) SIGINT Personnel

(U) Personnel operating under DIRNSA's SIGINT authorities.

(U) Sourcing for Dissemination and/or Application

(U//~~FOUO~~) Tracking and maintaining the source for SIGINT items that will be used in dissemination and/or applications submitted to the FISA Court.

(U) Spot Checking

(U) See Auditing.

(U) Super Auditing

(U) See Auditing.

(U) U.S. Person

(U) A citizen of the United States, an alien lawfully admitted as a permanent resident in the United States (also known as a Green Card Holder), unincorporated groups and associations whose members are primarily either citizens of the United States or aliens lawfully admitted for permanent residence in the United States, and corporations incorporated in the United States, including United States flag non-governmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them (USSID SP0018).

ANNEX A

(U) Physical Protection for Unevaluated and Unminimized SIGINT Data and/or ECI Programs/Material in Government-controlled and NSA/CSS-Approved Contractor SCIF Locations

(U) Purpose and Applicability

A1.1. (U//~~FOUO~~) In addition to the compliance responsibilities of all personnel involved in SIGINT activities (Section 3 of this USSID) and the compliance standards for each SIGINT function, additional measures must be taken to physically protect raw SIGINT data. This annex defines physical protection measures and describes how these measures are implemented to prevent unauthorized access to unevaluated, unminimized SIGINT data.

(U) Definition

A1.2. (U//~~FOUO~~) A physical protection measure is an environmental control put in place to reduce the risk of unauthorized personnel seeing, hearing, or otherwise gaining access to SIGINT data and/or Exceptionally Controlled Information (ECI). Such measures help ensure compliance with EO12333 and Foreign Intelligence Surveillance Act (FISA)/FISA Amendments Act (FAA) restrictions on sharing and dissemination of SIGINT data. The ultimate goal is to protect U.S. persons' privacy rights, minimize NSA violations and avoid compromise to unauthorized individuals.

(U) Risk Factors

A1.3. (U//~~FOUO~~) Personnel conducting SIGINT activities within Government-controlled or NSA/CSS-approved contractor sensitive compartmented information facility (SCIFs) should implement appropriate physical protection measures. Different environments present different levels of risk and, therefore, require different physical protection measures. Risk factors include:

(U//~~FOUO~~) The mix of personnel (e.g., SIGINT personnel and non-SIGINT personnel, United States citizens and foreign partners);

(U) The type of data being accessed (e.g., E.O. 12333, as amended, FISA/FAA); and

(U//~~FOUO~~) The location and physical characteristics of the facility (e.g., NSAW, Cryptologic Centers, Second Party headquarters, field sites, IC partner organizations, mobile units in a war zone, or open space, compartmented rooms, TEMPEST level).

(U) Risk Mitigation

A1.4. (U//~~FOUO~~) The best case scenario for mitigating (avoiding) the risk is to conduct SIGINT activity in separate rooms accessible only to personnel authorized and/or eligible for SIGINT data. However, in a joint environment – where SIGINT personnel are co-located with personnel who are not working under DIRNSA's SIGINT authorities or where SIGINT personnel with FISA/FAA access are co-located with SIGINT personnel without FISA/FAA and/or ECI access – this arrangement is not always possible.

A1.5. (U//~~FOUO~~) Below are some suggested guidelines to protect SIGINT and ECI data in Government-controlled facilities. It is important to remember that any changes that potentially impact space, to include reconfiguration of space, must be coordinated/approved by Associate Directorate for Installations and Logistics (ADIL) and the site Installations and Logistics (I&L) personnel to assess the feasibility, impact to power, space, and cooling, as well as the financial impact. Here are some guidelines:

(U//~~FOUO~~) **Cluster** SIGINT personnel (including those with FISA/FAA access) **in a secluded portion** of a room (e.g., in a row of cubicles grouped together) away from aisles and doorways, if possible;

(U) **Turn desks and computer screens** away from entryways, doorways, and aisles so that they cannot be seen by those not authorized for access;

(U//~~FOUO~~) **Use monitor filters or shields** to prevent casual viewing of computer screens;

(U//~~FOUO~~) **Limit displays**, e.g., briefing slides projected on a screen, to evaluated/minimized SIGINT with appropriate markings as required;

(U//~~FOUO~~) **Discuss SIGINT and/or ECI data only in isolated secure areas,** on a secure telephone, and/or in separate meeting spaces as necessary to ensure the discussions are not overheard by personnel not working under DIRNSA's SIGINT authorities;

(U) Provide all employees with **lockable storage** appropriate for the classification level of the material to be stored (drawer, flipper, cabinet, or safe);

(U//~~FOUO~~) In locations where the Associate Directorate for Security and Counterintelligence (ADS&CI/Q) has approved modified open storage of SCI material to include FISA data, classified information, with certain exceptions, is approved for storage within key-lockable containers including systems furniture;

(U//~~FOUO~~) Information protected in ECI compartments, GAMMA and GAMMA sub-compartment reports, certain other Controlled Access Program information, and Special Access Program (SAP) information must be stored in GSA-approved security containers (safes) unless approved by ADS&CI in coordination with the office of primary interest (OPI) and the Cover, Controlled, and Special Access Programs Office (S024). Additional, more stringent physical protection measures may be required for some Controlled Access Program information and SAP information.

A1.6. (U//~~FOUO~~) In locations where modified open storage has not been authorized by ADS&CI/Q, all classified information must be secured in GSA approved security containers.

A1.7 (U//~~FOUO~~) Provide a **dedicated printer** co-located with the SIGINT (or FISA/FAA) personnel and accessible only to personnel with access to SIGINT (or FISA/FAA) data or a programmable printer set to ensure that SIGINT personnel can limit access to SIGINT data printouts. If a dedicated or programmable printer is not available, the "2-man" system can be employed (in other words, one SIGINT analyst prints the document and one stands at the printer while it is being printed out).

A1.8 (U//~~FOUO~~) It is imperative that more stringent measures be implemented in NSA/CSS-approved contractor SCIFs to protect SIGINT and ECI material because contractor SCIFs are not SIGINT production environments and frequently are co-utilized by non-SIGINT personnel. Therefore, a "Compartmented Access Area" must be established to house SIGINT and ECI materials/activities to limit access to appropriately authorized and trained personnel. The requirements for a Compartmented Access Area are set forth in Chapter 2, Paragraph C, "Compartmented Area" of the IC Tech Spec-for ICD/ICS 705, "*Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*," dated 5 May 2011, and as amended. This section reflects that compartmented areas are designed to enforce need-to-know by ensuring that the areas afford visual, acoustical and access protection to the compartmented information contained therein. In the event facility issues preclude establishment of a compartmented area, alternative physical protection measures can be

utilized based upon Q13 survey results, and with the concurrence of the designated government Intelligence Oversight Officer, the government Contracting Officer/Contracting Officer Representative and the NSA/CSS Authorizing Official.

ANNEX B

(U) Guidelines for Intelligence Oversight Officers (IOO)

(U) Purpose and Applicability

B1.1. (U//~~FOUO~~) This annex establishes qualifications for, and assigns responsibilities to, IOOs to verify that SIGINT activities of the USSS (i.e., those with access to raw SIGINT) are conducted in a manner consistent with the laws, regulations, and policies that govern these activities. IOOs serve as the SIGINT intelligence oversight experts. They provide compliance guidance, implementation procedures, and partner with SV to advise local management of compliance problems, risks and mitigation procedures, thereby supporting the mission and promoting lawful conduct of SIGINT activities worldwide. The SIGINT Director requires that SIGINT elements with access to raw SIGINT data identify an IOO before SIGINT mission and database access are initiated.

B1.2. (U) The policy set forth in this annex applies to all IOOs operating throughout the USSS.

(U) General

B1.3. (U//~~FOUO~~) With the increase in missions and personnel requiring raw SIGINT access throughout the IC, comes greater risk that non-compliant activity could occur. The role of the IOO was created to fill the critical need for oversight in order to ensure that SIGINT activities everywhere are compliant with the laws, regulations, and policies that govern these activities.

B1.4. (U//~~FOUO~~) The IOO is designated by the Mission Owner/Mission Owner staff for all missions involving raw SIGINT access. In cases of delegated mission, the NSA Mission Owner may delegate the authority to assign an IOO to the Chief of the SIGINT organization to which the mission is delegated.

B1.5. (U//~~FOUO~~) A commander with delegated SIGINT Operational Tasking Authority (SOTA) is considered the Mission Owner for any SIGINT mission worked under SOTA – this does not include any NSA/CSS delegated mission and does not include computer network exploitation.

B1.6. (U//~~FOUO~~) Mission Owners are responsible for assigning the appropriate number of IOOs to effectively conduct intelligence oversight of the assigned missions. At least one IOO must be assigned for each mission. The total number of missions an IOO is assigned will depend on the complexity of the missions and the number and affiliation of personnel (USSS government, contractors, Second Party personnel, integrees/detailees from non-USSS organizations, part-time personnel, etc.) assigned to those missions.

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

B1.7. (U//~~FOUO~~) The IOO is responsible to the Mission Owner for Intelligence Oversight of the assigned missions, and is prohibited from serving in any [redacted] role that provides raw SIGINT access for the same mission (Mission Owner staff, Senior Sponsor, Access Sponsor, etc.).

NOTE: (U//~~FOUO~~) Until [redacted] software is developed to prevent IOOs from being assigned to other [redacted] roles that provide raw SIGINT access (within the same mission), the IOO (and the personnel who assigned the IOO) are responsible for ensuring compliance with this requirement.

B1.8. (U//~~FOUO~~) In most cases, an IOO is physically located with the SIGINT mission (on-site IOO). An IOO that is physically located in the same room, or interconnected rooms, as the personnel for whom he/she is responsible is considered an on-site IOO. An IOO that has personnel in nearby rooms he/she walks to on a daily basis is also considered an on-site IOO. There are specific conditions where an off-site IOO is permitted by the Chief of SV. The rare instances where an off-site IOO is permitted are detailed in Section B1.11 of this annex. All IOOs, whether on-site or off-site, have the same responsibilities and follow the same procedures to ensure compliancy at their mission location.

(U) IOO Qualifications

B1.9. (U//~~FOUO~~) IOOs must meet the following qualifications:

1. (U) Be a United States citizen;
2. (U) Be a United States government employee (civilian or military) operating under the SIGINT authority of Director, NSA/CSS;
3. (U) Be capable of, and have the ability to, effectively conduct IOO duties;
4. (U//~~FOUO~~) Complete foundational NSA/CSS and SID IO training requirements, SID Intelligence Oversight Officer Training (OVSC2201), and training for any authorities required for the assigned mission under the IOO's purview (OVSC1201/1203, etc.). Training must be completed before the IOO's location receives access to raw SIGINT; and,
5. (U//~~FOUO~~) For all missions to which assigned, be familiar with organizational technical capabilities, SIGINT mission, mission regulatory requirements, intelligence oversight requirements, and mission personnel and their affiliation.

(U) IOO Responsibilities

B1.10. (U//~~FOUO~~) In order to establish and/or maintain a robust intelligence oversight program for the mission to which they are assigned, the IOO will:

1. (U//~~FOUO~~) Know their locations' personnel, missions, SIGINT authorities (i.e., E.O. 12333, as amended, and/or FISA/FAA), governing documents (Staff

Processing Form (SPF), Mission Delegation form, Memorandum of Agreement/Memorandum of Understanding, or any other type of document that authorizes the element/location's mission), regulatory requirements, technologies, and SIGINT repositories utilized.

2. (U) Maintain current awareness of individual accountability for all personnel conducting or supporting SIGINT activities across their area of responsibility. The IOO will be aware of where their personnel are located when accessing raw SIGINT; routinely remind personnel they are limited to accessing raw SIGINT only at locations for which they have been approved based on their (b)(3)-P.L. 86-36 [redacted] mission entry; and routinely remind personnel of the need to suspend/remove access/authorities, as applicable, in cases of TDY, PCS, extended leave, etc.

3. (U//~~FOUO~~) Notify the Mission Owner/Mission Owner staff of any planned IOO absence to allow them sufficient time to assign a trained replacement IOO as needed.

4. (U) Notify local management of any intelligence oversight issues or compliance risks relevant to the IOO's location.

5. (U//~~FOUO~~) Understand applicable rules and standards: The IOO will be familiar with and be able to point personnel to the laws, executive orders, directives, and policies that apply to SIGINT activities in general (E.O. 12333, DoD 5240.4-R, NSA/CSS Policy 1-23, DTM 08-052, NSCID6, USSID SP0018, CR1610 as needed, etc.) and to their mission/location in particular. For SIGINT activity where access to NSANet is not available, the IOO will keep hard copies for reference. If personnel have questions the IOO cannot answer, the IOO will contact SV for assistance.

6. (U//~~FOUO~~) Emphasize individual accountability for the rules and standards: The IOO will provide guidance on IO training and will partner with management to enable personnel to remain current with required training. The IOO does not provide the training, but will be familiar with what is required and how to enroll. Specifically, the IOO will:

   a. (U) Answer questions on required annual core IO training (E.O. 12333, as amended, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, DTM-08-052, NSCID 6, and USSID SP0018) and other related training (OVSC courses); and

   b. (U) Document IO training for personnel whose access is not tied to CASPORT.

7. (U) Maintain cognizance of how personnel handle raw SIGINT data (USSID CR1610) and provide guidance as needed to reduce the likelihood of

unauthorized dissemination.

8. (U) Verify implemented rules and standards: IOOs serve as an extension of SV by verifying compliance at their locations. Verification responsibilities are as follows:

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

a. (U) Acknowledge IOO responsibilities through the automated IOO verification form in [redacted] initially, and annually, thereafter;

b. (U//~~FOUO~~) Verify the process used by the Access Sponsor to routinely remove/suspend from mission any unauthorized personnel (personnel who have left the mission, are on temporary duty elsewhere, etc.); routinely verify process effectiveness by confirming unauthorized personnel are removed from mission; review all missions routinely, and at a minimum quarterly, to verify approved documentation is in place, if applicable, for those entries for which he/she is responsible as an IOO. Examples of missions that require approved documentation are delegated mission, Partner mission using NSA data, mission worked at a location other than the Mission Owner's location, etc.)

c. (U//~~FOUO~~) Verify all assigned personnel are operating under appropriate SIGINT authority. Examples of personnel whose authority needs to be checked prior to an Access Sponsor submitting them against a mission requiring raw SIGINT access are non-permanently- assigned personnel, integrees, assignees, detailees from other agencies, tethered analysts, and personnel from other NSA organizations that do not have a SIGINT mission, etc. The types of documents that can assist in verifying SIGINT authority are MOAs/MOUs, SPFs, Second Party integree SPFs, unit USSIDs/Site Profiles, etc. The IOO will interface with the Access Sponsor(s) to identify which personnel require SIGINT authority documentation (integrees, assignees, Second Party, etc.). The IOO will verify the Access Sponsor(s) understand(s) the requirement to verify a user's SIGINT authority, and how to verify that authority, prior to granting access. The IOO will conduct spot checks to ensure appropriate SIGINT authority documentation is in place as needed.

d. (U//~~FOUO~~) As appropriate based on location, verify implementation of, and recommend as needed, appropriate physical protection measures (as described in Annex A of this USSID) to reduce the risk of personnel not authorized access to raw SIGINT data from seeing, hearing, or otherwise gaining access to the data;

9. (U//~~FOUO~~) Advise the Mission Owner Staff, Senior or Access Sponsor as appropriate to suspend access based on compliance verification findings

concerning documentation or issues regarding mission authorization for those entries for which he/she is responsible as an IOO.

10. (U//~~FOUO~~) Report or support reporting of non-compliant activity: The IOO will serve as a resource to provide guidance on, and assist with, reporting incidents of non-compliant activity, i.e., any conduct that constitutes or is related to an intelligence activity that may violate laws, executive orders, directives, and policies that govern SIGINT activities, as defined by DoD Regulation 5240.1-R. To support the reporting of non-compliant activity, the IOO will:

    a. (U) Know the reporting path(s) for incidents of non-compliance and provide guidance to personnel at his/her location;

    b. (U//~~FOUO~~) Report any non-compliant activity (or confirm that someone at his/her location is reporting the incident) to management, SV and OIG immediately upon recognition and also quarterly in the IO Quarterly Report;

    c. (U//~~FOUO~~) Work with local management and/or the responsible individual(s) to confirm that the results of non-compliant activities are destroyed unless authority to retain and/or disseminate the information has been obtained from the proper authority; and

    d. (U//~~FOUO~~) Provide updates, as applicable, to initial incident reports if additional information is obtained until the incident has been completely resolved (i.e., fully researched, impacts identified, and corrective measures taken).

11. (U//~~FOUO~~) Implement corrective action: When non-compliant activities/incidents are detected, the IOO will take the following steps, working with the applicable compliance directorate(s) (SV, TV, IV, V7, etc.) as needed:

    a. (U) Assist with immediate implementation of available measures to stop the non-compliant activity;

    b. (U//~~FOUO~~) Provide guidance appropriate to the situation, e.g., de-tasking of selectors, stopping database queries, cutting off data flows, turning off collection equipment, deleting database accounts, and reviewing applicable policies with the relevant individuals; and

    c. (U) Closely monitor the situation to verify that the problem has been resolved.

(U) Off-Site IOO

B1.11. (U//~~FOUO~~) The Chief of SV may authorize in writing an off-site IOO if the mission element agrees to accept the increased risk. The following are the most likely

situations where an off-site IOO is acceptable:

1. (U//~~FOUO~~) A SIGINT analyst operating alone or as the sole SIGINT person in a non-SIGINT environment [redacted]; and
2. (U//~~FOUO~~) Locations approved for the use of U.S. SIGINT, but with no U.S. presence, [redacted] (b)(3)-P.L. 86-36

B1.12. (U//~~FOUO~~) A mission element/site request for an off-site IOO is submitted via a Staff Processing Form (SPF) to SV. This is usually done through the SPF templates in [redacted] This request must include a justification, as well as an acknowledgement from the mission element that it accepts the increased risk of an off-site IOO.

B1.13. (U//~~FOUO~~) If an off-site IOO is approved, the site will name an IOO point of contact (POC), if possible, who works on-site with the analyst(s) on a daily basis, is familiar with the mission, and can interact with the off-site IOO via phone or email. The on-site POC for the off-site IOO may be a non-NSA/CSS employee, but must be someone familiar with the mission and the personnel working the mission.

B1.14. (U//~~FOUO~~) Although the responsibilities for on-site and off-site IOOs are the same, off-site IOOs will have to perform many of their duties virtually. SV highly recommends the off-site IOO virtually interact with the on-site POC at least weekly. Additionally, the off-site IOO is required to visit the site(s) on a quarterly basis. Although it is possible for an IOO to serve more than one location, budget constraints should be considered prior to accepting off-site IOO responsibilities.

(U) Additional Guidelines:

B.15. (U//~~FOUO~~) For mission(s) with one SIGINT analyst (no other SIGINT personnel on-site): the Mission Owner or delegate will submit an SPF requesting an off-site IOO and document justification and acceptance of risk for Chief SV approval. The Access/Senior sponsor roles reside with the sponsoring org.

B.16. (U//~~FOUO~~) For mission(s) with two SIGINT analysts: Each analyst will be trained as an IOO and conduct oversight over the other. Other roles, same as above.

B.17. (U//~~FOUO~~) For mission(s) with three SIGINT analysts: Same as above; third analyst (non-IOO) could fill an additional non-IOO [redacted] role if required by the Mission Owner. (b)(3)-P.L. 86-36

Proceed To:
NSA | Director | SID | SID Staff | SID Policy | USSID Index