made progress in addressing some of these deficiencies, but found that processes had not been fully documented in the form of management directives, administrative policies, or operating manuals. The NSA OIG recommended that Program officials formally adopt rigorous, written operating procedures for the following key processes:

- Approvals for content collection by the appropriate named officials
- Reporting of violations of the Authority, similar to procedures for documenting violations of Legal Compliance and Minimization Procedures[5]
- Evaluation of dual FISA and PSP content collection
- Systematic identification and evaluation of telephone numbers and Internet identifiers for detasking.[6]

(U//~~FOUO~~) Corrective action was taken in response to the four recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 06 and HPSCI on 2 January 2008.

13 Sep 2004 ***~~(S//NF)~~ Need for Increased Attention to Security-Related Aspects of the STELLARWIND Program (ST-04-0025)***

(U//~~FOUO~~) This OIG report disclosed weaknesses in Program security. The Program was particularly vulnerable to exposure because it involved numerous organizations inside and outside NSA.

(U//~~FOUO~~) While the Program Manager placed a strong emphasis on personnel security, he did not take a proactive and strategic approach to physical and operational security. In particular, better use of the Program Security Officer would have helped to improve special security practices for handling Program material and strengthen operations security (OPSEC).

(U//~~FOUO~~) The Program Manager and the Associate Director for Security and Counterintelligence concurred with the findings and implemented corrective measures. In particular,

---

[5](U) U.S. Signals Intelligence Directive 18 or "USSID SP0018" (as of 27 July 2003).
[6](~~TS//SI//NF~~) [redacted]

the Staff Security Officer was freed from other responsibilities and took a more active and effective role in Program security. Management did not conduct a formal OPSEC survey as recommended; however, steps taken by management to implement OPSEC practices met the intent of the original recommendation.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

21 Nov 2005 ***~~(TS//SI//NF)~~ Review of the Tasking Process for STELLARWIND U.S. Content Collection (ST-04-0026)***

~~(TS//STLW//SI//OC/NF)~~ This report identified material weaknesses in the tasking and detasking process under the PSP. The process to task and detask telephone numbers for content collection under the Program was inherently fragile because it was based on e-mail exchanges and was not automated or monitored.

~~(TS//STLW//SI//OC/NF)~~ The OIG examined [redacted] telephone numbers and Internet identifiers approved for content collection on the date in November 2004 when the audit began and identified the following types of errors:

- [redacted] involved under-collection; identifiers were not put on collection quickly enough or were not put on collection until the OIG discovered the errors.
- [redacted] involved unauthorized collection caused by a typographical error.
- [redacted] involved over-collection; they were not removed from collection quickly enough.
- [redacted] record-keeping errors in the Program's tracking database

~~(TS//STLW//SI//OC/NF)~~ In the [redacted] of unauthorized collection caused by a typographical error, NSA personnel did not review the collected information before destroying it, nor did NSA issue any report based on, or otherwise disseminate, any information from the [redacted] of untimely detasking. However, without a robust and reliable collection and tracking process, NSA increased its risk of unintentionally violating the Authorization. NSA also increased the risk of missing

valuable foreign intelligence by failing to task telephone numbers and Internet identifiers in a timely manner.

(U//~~FOUO~~) NSA OIG recommended that all errors be swiftly resolved, that specific procedures be adopted to prevent recurrences, and that identifiers tasked for collection be promptly reconciled with identifiers approved for tasking, and repeated every 90 days. Management implemented the recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

31 May 2006 ***~~(TS//SI//NF)~~ Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027)***

~~(TS//STLW//SI//OC/NF)~~ This report determined that, based on a statistical sample, Program officials were adhering to the terms of the Authorization and the Director's delegation thereunder; that tasking was appropriately approved and duly recorded under the Authorization; and that tasking was justified as linked to al-Qa'ida or affiliates of al-Qa'ida. The report recommended improvements in record-keeping practices.

~~(S//NF)~~ Due to a lack of sufficient and reliable data, the NSA OIG could not reach a conclusion on the tasking approval process for two PSP-related collection programs. The OIG recommended that management responsible for the affected programs, design and implement a tasking and tracking process to allow managers to audit, assess timeliness, and validate the sequencing of tasking activities. Management agreed to install automated tracking of tasking and detasking.

~~(TS//SI//NF)~~ Although the collection architecture was designed to produce one-end-foreign communications, inadvertent collection of domestic communications occurred and was addressed. The OIG recommended changes in management reporting to improve the tracking and resolution of inadvertent collection issues.

(U//~~FOUO~~) Corrective action has been completed for one of the two recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

11 Jul 2006 ***~~(TS//SI//NF)~~ Supplemental Report to Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027.01)***

~~(TS//STLW//SI//OC/NF)~~ After issuing the original report, the NSA OIG conducted further research to determine whether Program officials were approving content tasking requests based solely on metadata analysis. Using the statistical sample in the original audit, the OIG found no instances of metadata analysis as the sole justification for content tasking. In all cases tested, there was corroborating evidence to support the tasking decision.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

5 Sep 2006 ***~~(TS//SI//NF)~~ Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records (ST-06-0018)***

~~(TS//STLW//SI//OC/NF)~~ On 24 May 2006, the telephony metadata portion of the PSP was transferred to FISC Order BR-06-05, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [Telecommunications Providers] *Relating to* [redacted] The Order authorized NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data regarding [redacted]

~~(TS//SI//NF)~~ On 10 July 2006, in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*, the NSA OIG issued "a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." This report was issued with the Office of the General Counsel's concurrence as mandated by the Order.

~~(TS//SI//NF)~~ The "*Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance*

Court Order: Telephony Business Records (ST-06-0018)," 5 September 2006, provided the details of the findings of the 10 July memorandum and made formal recommendations to management.

~~(TS//SI//NF)~~ Management controls governing the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order were adequate and in several aspects exceeded the terms of the Order. However, due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, the NSA OIG recommended three additional controls regarding collection procedures, reconciliation of audit logs, and segregation of duties.

~~(TS//SI//NF)~~ Collection Procedures

~~(TS//SI//NF)~~ During an OIG review of collection procedures, Program management discovered that NSA was obtaining [redacted] data that might not have been in keeping with the Order: [redacted] OGC advised that [redacted] data should have been suppressed from the incoming data flow. Immediately, management blocked the data from analysts' view. Further, working with the providers, Program management completed suppression of the suspect data on 11 October 2006 and agreed to implement additional procedures to prevent the collection of unauthorized data.

~~(TS//SI//NF)~~ Reconciliation of Audit Logs

~~(TS//SI//NF)~~ Management controls were not in place to verify that telephone numbers approved for querying were the only numbers queried. Although audit logs documented the queries of the archived metadata, the logs were not in a usable format, and Program management did not routinely use them to audit telephone numbers queried. Management concurred with the recommendation to conduct periodic reconciliations; however, action was contingent on the approval of a Program management request for two additional computer Programmers.

[redacted]

~~(C//NF)~~ Lack of Segregation of Duties

~~(C//NF)~~ The seven individuals with the authority to approve queries also had the ability to conduct queries under the Order. Standard internal control practices require that key duties and responsibilities be divided among different people to reduce the risk of error and fraud. Although Program management concurred with the finding, it could not implement the recommendation due to staffing and operational needs. As an alternative, Program management agreed to develop a process to monitor independently the queries of the seven individuals. This action plan was contingent on the development of usable audit logs recommended above.

(U//~~FOUO~~) Corrective action has been completed for one of the three recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

20 Dec 2006

~~(S//NF)~~ Summary of OIG Oversight 2001-2006 STELLARWIND Program Activities (ST-07-0011)

~~(S//NF)~~ On 20 December 2006, the OIG issued a report summarizing OIG's oversight of the STELLARWIND Program after five years of implementation.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

~~(TS//SI//NF)~~ Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using Pen Register and Trap and Trace Devices (ST-06-0020)

~~(TS//SI//NF)~~ On [redacted] the OIG reported that the management controls governing the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the FISC Order authorizing NSA to collect Internet metadata using PR/TT devices were adequate and in several aspects exceeded the terms of the Order. Due to the risk associated with the processing of electronic communications metadata involving U.S. person information, additional controls were needed for processing and monitoring queries made against PR/TT data, documenting

ST-09-0002 ~~*TOP SECRET//STLW//COMINT//ORCON/NOFORN*~~

oversight activities, and providing annual refresher training on the terms of the Order.

(U//~~FOUO~~) Corrective action has been completed for two of the six recommendations.

(U//~~FOUO~~) This report was sent to SSCI on [redacted] and HPSCI on [redacted]

5 Jul 2007 ***~~(TS//SI//NF)~~ Domestic Selector Tasking Justification Review (ST-07-0017)***

(U//~~FOUO~~) The OIG conducted this review to determine whether tasking justification statements were supported with intelligence information consistent with sources cited in the justifications. The OIG identified some justifications containing errors, but there was no pattern of errors or exaggeration of facts or intentional misstatements.

(U//~~FOUO~~) This report was sent to SSCI on 28 January 2008 and HPSCI on 28 January 2008.

30 June 2008 ***~~(TS//SI//NF)~~ Advisory Report on the Adequacy of STELLARWIND Decompartmentation Plans (ST-08-0018)***

~~(TS//SI//NF)~~ At the request of the SID Program Manager for CT Special Projects, the OIG assessed the adequacy of NSA's plans to remove data from the STELLARWIND compartment, as authorized by the Director of National Intelligence. On 30 June 2008, the OIG reported that NSA management had a solid foundation of planning for decompartmentation. In particular, the content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of successfully removing data from the STELLARWIND compartment, while complying with laws and authorities. Management was also diligent in assessing the scope and complexity of this undertaking. Although the OIG made no formal recommendations, it suggested improvements to develop more detailed plans, set firm milestones, and establish a feedback system to ensure that plans were successfully implemented.

(U//~~FOUO~~) This report was not sent to SSCI or HPSCI.

APPENDIX F

(U) Presidential Notifications

This page intentionally left blank.

(U) Presidential Notifications

~~(TS//STLW//SI//OC/NF)~~ Executive Orders 12333 and 12863 require intelligence agencies to report to the President, through the President's Intelligence Oversight Board, activities they have reason to believe may be unlawful or contrary to executive order or presidential directive. Knowing that Board members were not cleared, however, the NSA Director or Deputy Director reported the following violations of the Presidential Authorization and related authorities to the President through his Counsel, rather than through the Board. Each notification was approved if not actually drafted by OIG. Some of the notifications were not the subject of the OIG reviews or investigations discussed in Appendix E.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes violations regarding (1) the [redacted] and (2) [redacted]
[redacted]	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes a delay of about 90 days in detasking a telephone number [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes the investigation mentioned above regarding metadata collection violations that occurred under FISA Court Order *In Re* [redacted] FISA Court [redacted] The complete OIG report was issued [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes [redacted] instances in which cleared NSA analysts mistakenly accessed data [redacted] In one instance, a report based on such data went out, but it was not cancelled because the same information was available elsewhere. In the other [redacted] instances, no reports were issued. [redacted]

(U) Date	(U) Summary of Notification
	[redacted]
[redacted]	(~~TS//STLW//SI//OC/NF~~) Describes one instance of inadvertent collection of a call with both ends in the U.S. – a fact that could not have been known until it was listened to because [redacted] showed the call as having a foreign origin. [redacted]
[redacted]	(~~TS//SI//NF~~) Describes three incidents: The first involved a one-digit typo resulting in one incorrectly tasked number. The second involved a number improperly tasked for metadata analysis. The operator discovered it almost immediately and promptly removed it from tasking. The third involved [redacted] numbers that were not detasked in a timely fashion.
2 Aug 2005 [redacted]	(~~TS//SI//NF~~) Describes the evolving [redacted] a practice that may have resulted in over-collection. The notification refers to NSA's work in developing more rigorous [redacted]
[redacted]	(~~TS//STLW//SI//OC/NF~~) Describes an incident in which bulk telephony metadata was actively collected in spite [redacted] At that time NSA limited collection of bulk telephone records to [redacted] as permitted by statute. The collection resulted when [redacted] The error was not discovered for 18 months. (~~TS//STLW//SI//OC/NF~~) Although most of the metadata improperly collected was also properly acquired [redacted] pursuant to statute, the dataflow was terminated immediately upon discovery. Also, because the improperly collected metadata had been forwarded to non-STELLARWIND databases, the Agency removed non-compliant metadata from all affected databases, including those in which STELLARWIND data is normally stored.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which an [redacted] This resulted [redacted] of non-target data. The error was discovered within hours, when personnel responsible for monitoring [redacted] The error was corrected, and all inadvertently collected records were deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an instance where a [redacted] Although no reports were generated, and there was no evidence that U.S.-to-U.S. communications were collected, we could not certify that the files were all one-end foreign without reviewing [redacted] The [redacted] files were deleted, and procedures used by [redacted] were being reviewed. ~~(TS//STLW//SI//OC/NF)~~ A second incident was reported in which a typographical error resulted in contact chaining on a U.S. telephone number with no [redacted] affiliation. The telephone number was rechecked, and the error was corrected.

This page intentionally left blank.

APPENDIX G

(U) United States Signals Intelligence Directive SP0018, Legal Compliance and Minimization Procedures

This page intentionally left blank.

~~SECRET~~

AUTHORIZED REPRODUCTION NUMBER 00R0043

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES
SIGNALS INTELLIGENCE
DIRECTIVE
18

27 July 1993

INCLUDES CHANGES 1 and 2

See Letter of Promulgation for instructions on reproduction or release of this document.

~~OPR: D2~~
~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES ~~(FOUO)~~

LETTER OF PROMULGATION

(U) This USSID prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18, and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 19.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS, NSTS 963-3121 or [redacted]

J.M.McCONNELL
Vice Admiral, U.S. Navy
Director

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

USSID 18
27 July 1993

CHANGE REGISTER

No	Date	CHANGE Authority (Msg Cite/DTG, Hard Copy (HC))	ENTERED Date	By
1	28OCT97	HARDCOPY CHANGE	29OCT97	RS
2	11Dec98	P0211–0307–98, 111600Z Dec 98	11Dec98	WF
2	11Dec98	P0211–0309–98, 111640Z Dec 98 (correction to above)	11Dec98	WF

This page intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

27 July 1993

USSID 18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES (U)

SECTION 1 – PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

SECTION 2 – REFERENCES

2.1. (U) References

a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.

b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

SECTION 3 – POLICY

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS. The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

SECTION 4 – COLLECTION

4.1. ~~(S-CCO)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] will not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [redacted], or

(c) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(4) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) Technical devices (e.g. [redacted]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted] and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]:

(a) A non-U.S. PERSON located outside the UNITED STATES [redacted]

(b) [redacted]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process),

sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and abets a person engaging in such activities.

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. ~~(S-CCO)~~ [redacted]

a. [redacted]

b. [redacted]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

4.4. ~~(S-CCO)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that the DIRNSA/CHCSS is advised immediately and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [redacted]

b. If Attorney General approval is obtained, the COLLECTION may continue for the length of time specified in the approval.

c. If it is determined that [redacted] COLLECTION may continue at the discretion of the operational element.

d. If [redacted] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [redacted] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

4.5. ~~(C-CCO)~~ U.S. PERSON TARGETS Entering the UNITED STATES.

a. If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Attorney General approval described in Section 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. ~~(S-CCO)~~ Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [redacted], must be submitted through the DDO and the General Counsel to the DIRNSA/CHCSS for review.

4.7. ~~(C-CCO)~~ Direction Finding. Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for

communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5 – PROCESSING

5.1. ~~(S-CCO)~~ Use of Selection Terms During Processing.
When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located) [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the DDO or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(C-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. ~~(S-CCO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) Establish or maintain intercept, or

(b) Minimize unwanted intercept, or

(c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P02.

5.5. ~~(S-CCO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES [redacted] communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to

warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

SECTION 6 – RETENTION

6.1. ~~(S-CCO)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-CCO)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

SECTION 7 – DISSEMINATION

7.1. ~~(S-CCO)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P02.

7.2. ~~(S-CCO)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made

by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P02 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P02 should be in the form of a CRITICOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

7.3. ~~(S-CCO)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P02, the Deputy Chief, P02, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(1) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P02 within 24 hours of discovery of the error.

SECTION 8 – RESPONSIBILITIES

8.1. (U) Inspector General.
The Inspector General shall:

a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.

b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.

c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.

d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).