~~SECRET~~

USSID 18

Guide (~~FOUO~~)

Derived From: NSA/CSS Manual 123-2
Dated: 24 February 1998
Declassify On: X1, X3, X5, X6, X7, X8

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

Overview (U)

Introduction (U)

(S//SI) This is an informal guide to USSID 18 for areas concerning U.S. identities. It briefly addresses the regulations and directives which guide NSA's authorities, collection and reporting issues for threat and non-threat situations, and lists procedures for U.S. identity release. This informal guide directs the reader to the specific USSID 18 sections and is not a substitute for USSID 18, but should be used in conjunction with it. Use of this guide does not relieve the reader of his or her obligation to review E.O. 12333, DoD Reg 5240.1-R, NSA/CSS Directive 10-30 and USSID 18 at least annually.

(S//SI) U.S. identities may be released to customers under specific conditions. Procedures for release of U.S. identities appearing in SIGINT are outlined in the memorandum on pages 7 and 8.

(S//SI) Comments and questions may be addressed to the following POCs:

- P013 - Collection and Retention Guidance
  963-2194
- P0112 - Reporting Guidance
  963-1911
- P0113 - Customer Requests for Disclosure of U.S. Identities
  963-3453

Guidance Regulations (U)

~~(S//SI)~~ Executive Order 12333 sets forth NSA's basic authorities—to collect, process, and disseminate SIGINT information for NATIONAL FOREIGN INTELLIGENCE PURPOSES and to support military operations.

~~(S//SI)~~ NSA/CSS implements EO 12333 and DoD Reg 5240.1-R through NSA/CSS Directive 10-30 and USSID 18, which addresses the way in which we conduct our SIGINT mission while protecting U.S. persons.

~~(S//SI)~~ USSID 18 provides specifics on whom we may target, how we collect, select, and store such information, and how we disseminate information on U.S. persons.

USSID 18 Issues for Threat Situations (~~FOUO~~)

Consensual Collection Procedures (~~FOUO~~)

(~~FOUO~~) Individuals may fill out a consent agreement allowing the Agency to collect either their communications or information about them (USSID 18, Section 4.1.c.(1)).

(~~FOUO~~) After the consent agreement is completed, it is forwarded to P0212.

(~~FOUO~~) P0212 prepares an SPF for Deputy Director approval and obtains proper coordination through the system.

(~~FOUO~~) After Deputy Director approval, P0212 prepares memorandum for the workforce to implement collection and processing.

Implied Consent Procedures (~~FOUO~~)

(~~S-CCO~~) Used in cases where a U.S. person is held captive by a foreign power or a group engaged in international terrorism and consent for NSA collection could be implied (USSID 18, Section 4.1.c.(1)).

(~~S-CCO~~) P0212 prepares an SPF for DERNSA's approval and obtains proper coordination through the system.

- The SOO can authorize collection if DERNSA is not available, but DERNSA approval must be obtained by the next morning [redacted] dated 25 January 1997, subject: Standing Procedures for the Approval of Collection, Processing, and Dissemination Under "Implied Consent").

63/86-36

(~~FOUO~~) After approval, P0212 notifies all appropriate elements and orders termination when the situation warrants.

Reporting Threat Information (~~FOUO~~)

(~~S-CCO~~) When specific, actionable threat information involving U.S. persons is obtained:

- Reporting elements issue a report with as much information as possible, including U.S. names, in the interest of protecting U.S. per-

sons.

- As soon after the report is issued as practicable, the reporting element sends a memorandum explaining the situation to P023, with courtesy copies to P0212 and P0215.
- Reporting elements also account for dissemination in Quarterly Report to the IG (USSID 18, Section 7.2.c.(5) and *U.S. Identities in SIGINT*, pages 4 and 11).
- Appropriate customers may be tipped by phone as soon as the report is released.

Collateral information (U)

~~(S//SI)~~ Collateral information may be included in SIGINT reporting when it contributes to the report by amplifying, clarifying, explaining, or supplementing the SIGINT information.

~~(S//SI)~~ In those circumstances, when collateral is found after the SIGINT report has been released, the originator of the collateral may be contacted with a request that the originator reconfirm the collateral as appropriate.

~~(S//SI)~~ If time does not permit contacting the originator of the collateral, the Office of the IG is informed that SIGINT personnel "in include field sites and small operations at DIA/DO may disseminate collateral. In these cases, the originator should be contacted as soon as possible.

~~(S//SI)~~ [redacted]

b1
b3/all ~~(S//SI)~~ [redacted]

USSID 18 and Non-Threat Situations (~~FOUO~~)

(~~S-CCO~~) Communications from, to, or about a U.S. person [redacted] may not be intentionally collected without further legal authorities. (USSID 18, Section 4 applies.)

b1 b3/all

(~~S-CCO~~) Incidental collection of a U.S. person's communications in a foreign communication may be processed and reported if there is valid foreign intelligence, the report is focused on the foreign side of the communication, and USSID 18 guidelines are followed for reporting.

(~~S-CCO~~) Communications solely between U.S. persons inadvertently intercepted during foreign communications collection are to be destroyed upon recognition; there are exceptions whereby the Director may waive destruction and allow reporting. Example of this are such communications that contain SIGNIFICANT foreign intelligence or possible evidence of a crime. (USSID 18, Section 5.4 applies.

(~~S-CCO~~) 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) should be destroyed. (USSID 18 5.4.c)

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

b1 b3 all

[redacted] (Exceptions - see USSID 18, Section 6.1.)

[redacted]

~~SECRET~~

[redacted]

(Exceptions - see USSID 18, Section 6.1.)

[redacted] b1 03/all

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

Normal Handling of U.S. Identities in Reports

(S-CCO) Any U.S. identity, even if allowed, is only used when necessary to understand or assess the foreign intelligence.

- ✓ (S-CCO) Only senior executive branch officials may be identified by title (all others are generic).
- ✓ (S-CCO) The United States Government Manual determines which officials are senior.
- ✓ (S-CCO) Members of the judicial and legislative branches must be rendered generically.
- ✓ (S-CCO) Properly protect state/local officials/organizations by using generic terms.
- ✓ (S-CCO) Only senior U.S. officials in international organizations may be identified by title (use generic terms for all others). (Senior officials are those who can make decisions on behalf of the organization).
- ✓ (S-CCO) Identities of U.S. private entities must be rendered generically.
- ✓ (S-CCO) Avoid contextual identification of U.S. entities.

(S-CCO) Focus on foreign intelligence/counterintelligence and on the foreign perspective.

(S-CCO) Minimize incidental U.S. communications.

THREE (3) PAGES WITHHELD

~~SECRET~~

NOTES