(U//FOUO) What's the Policy on Sharing NOFORN With Second Party Integrees?

FROM: [redacted] and [redacted]
SIGINT Policy (S02L1)
Run Date: 05/09/2006

(U//FOUO) In light of SID's commitment to robust information sharing, and the increasing importance of Second Party Integrees to SID's mission, have you ever needed clarification on the Agency's policy for sharing NOFORN information with Second Party Integrees? If so, the guidance below will help!

(U//FOUO) The primary policy on Second Party Integrees' access to NOFORN SIGINT and other sensitive information is available in NSA/CSS Policy 1-13 , " *Second Party Integrees* ." See especially paragraph 2 of its main body and paragraphs 3.c** and 3.f of its annex. (Policy 1-13 supercedes earlier policy on this subject that had been promulgated by a former Deputy Director for Operations.)

(U//FOUO) We encourage you to review Policy 1-13 in its entirety, but for your convenience offer the following extracts from it regarding access to sensitive data:

(S) **SIGINT that Can Always Be Freely Shared with Integrees:**

- (S) SIGINT ***without*** any restrictive control markings (NOFORN or REL TO) may be shared freely with our Second Party Integrees. Second Party Integrees, here and in the field, have access to non-caveated SIGINT products through the finished SIGINT product database.
- (S) SIGINT information with REL TO markings may be freely shared (as you would expect) with a Second Party Integree whose country is designated in the control marking. (For example, a British integree can view material marked REL USA/GBR.)

(S) **When/How Can SIGINT that is NOFORN or REL TO Be Shared with Integrees?**

- (S) Release of **NOFORN** -marked SIGINT information to any Second Party Integree must be approved by the originating element, based on source sensitivities and consideration of other partners' equities. Furthermore, only the SIGINT Director; SIGINT Deputy Director; Chief, Information Sharing Services, and Chief, Policy Services may approve the release of Special Series hardcopy reports marked NOFORN. The Second Party Integree's supervisor will keep an internal record of the approval and release, and NSA's Foreign Affairs Directorate (FAD) will be informed.
- (S) Release of SIGINT information with **REL TO** markings that do not include the integree's home country (e.g., REL USA/GBR information for a Canadian Integree) must be approved by the originating element of the SIGINT information, based on source sensitivities and consideration of other partners' equities. The Second Party Integree's supervisor will keep an internal record of the originator's verbal or written approval and the release, and NSA's Foreign Affairs Directorate (FAD) will be informed.

(S) **What About Non-SIGINT Information?**

- (S) **Non-caveated** classified information produced by other Intelligence Community members can only be released to Second Party Integrees when sanitized and approved by a Designated Intelligence Disclosure Official in accordance with the rules in DCID 6/6. (See in INTELINK at the Category 6 DCIDs webpage .)
- (S) Only the originator of **NOFORN** -caveated and classified Community information may grant approval for a sanitized version of the intelligence to be released to any foreign integree. The integree's supervisor will keep an internal record of the approval and

release, and NSA's Foreign Affairs Directorate (FAD) will be informed.

- (S) Similarly, only the originator of a **REL TO** -caveated and classified Community product may grant approval for a sanitized version of the intelligence to be released to a foreign integree whose country is not already designated in the REL TO marking. The integree's supervisor will keep an internal record of the approval and release, and NSA's Foreign Affairs Directorate (FAD) will be informed.

(U) **Emergency Sharing Policies**

(U) For emergency sharing guidelines, refer to DCID 6/6, Section 10. (Available on INTELINK via the Category 6 DCIDs webpage .)

(U) **Jobs That Integrees May *Not* Hold:**

- (U//FOUO) Second Party Integrees shall not be assigned positions for which access to NOFORN information is routinely required, without prior approval from all originators of that information.
- (U//FOUO) Second Party Integrees may not perform Information Technology (IT) systems administration functions or hold privileged user access on NSA/CSS IT systems.

** NOTE: (S) Paragraph 3.c of the annex regards piece-by-piece access to NOFORN SIGINT in accordance with paragraph 2 of the main policy. The lists of what has been accessed by a Second Party integree should be complete enough that, should there be a cryptologic insecurity in the future, a determination could be made regarding what the integree had access to so that a cryptologic damage assessment could be performed. The hardships incurred by having to keep these lists are intentional so that release is not done lightly. It should also help to remind all SIGINTers to appropriately mark information with the maximum sharing level initially.

(S) Second Party Integrees' access to NOFORN SIGINT databases requires approval at the level in SID appropriate to cover all owners of the data. Examples of such approvals are available on the SIGINT Policy homepage at the following links:

database access example #1

database access example #2

Another example of a special NOFORN approval for Second Party Integrees is available here: NOFORN-sharing example .

(U//FOUO) This article was prompted by a letter to the SID Mailbag .
