NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
SIGINT DIR	1923-06	S3109-080-06

THRU	ACTION	EXREG SUSPENSE
	[X] APPROVAL	
SUBJECT		KCC SUSPENSE
SUBJECT (TS//SI//NF) Recommended Requirements for cryptanalysts at CCs at Texas, Georgia and Hawaii to access NSA and FBI FISA material.	[ ] SIGNATURE	
	[ ] INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION

SUMMARY

PURPOSE: (TS//SI//NF) To obtain SID approval for Cryptanalysis and Exploitation Services (CES) cryptanalysts at the NSA/CSS Cryptologic Centers (CCs) in Texas, Georgia, and Hawaii, who are under direct DIRNSA authority, to access and process NSA SIGINT FISA and CT FBI SIGINT FISA data that is stored in databases in CES at NSAW. This will set a precedent for access to NSA FISA material outside of NSAW.

BACKGROUND: (TS//SI) As part of CES's strategy for the Extended Enterprise buildout, cryptanalysis efforts at the cryptologic centers in Texas, Georgia, and Hawaii will serve as transparent extensions of the cryptanalysis mission performed by CES in the Office of Target Pursuit's exploitation branches (S31142, S31143, S31131, and S31133) at NSAW. Analysts at the cryptologic centers will become part of a virtual team with NSAW analysts. They will access data that is stored within the CES firewall and will use cryptanalytic procedures and tools, also within the CES firewall, by way of a VPN capability that ensures that security is not compromised and that the data and tools accessed cannot get out to the local network. The priorities of cryptanalytic missions will continue to be set in conjunction with mission elements at NSAW and the Cryptologic Centers as appropriate.

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
D21/OGC	[redacted]		SID COS	[redacted]	
SID//S3			SV		
SID//S31					
SID//S2					
SID//S2I					

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
[redacted]			20 June 2006

FORM A6796
REV NOV 95

DRV FM: NSA/CSSM 1-52
Dated: 23 November 2004 DECL ON: 20291123

SECURITY CLASSIFICATION

TOP SECRET//COMINT//NOFORN//20291123

145461

707

[redacted]

(TS//SI) Cryptanalysts at the cryptologic centers will access data that is stored in the following databases at NSAW:

FOURSCORE - fax and DNI data, some of which is NSA or FBI FISA-derived
ZAP - text, some of which is NSA or FBI FISA-derived
CAPRICORN - voice, some of which is NSA or FBI FISA-derived
SOAPOPERA - voice, end product, SRI information, some of which is NSA or FBI FISA-derived

(TS//SI) These databases contain raw data, including enciphered collection, and, when exploitation is possible, decrypted plain text. Some of the data in the databases is NSA FISA-derived or FBI CT FISA-derived. While not every database contains FISA-derived material, it is reasonable to expect that analysts at the CCs will perform mission with agility, moving across targets and databases as mission demands, and that sometimes that will mean accessing data within a database that does contain FISA-derived data. Access to these databases is restricted to analysts who hold the RAGTIME ECI, have a specific 'need to know' about the data stored within the databases, and who are authorized by the data owner. For some years CES has been the recipient of improperly marked/classified data but all analysts have been and are aware that data marked with the SIGAD US984J and case notation XX.SQF* is FBI FISA data, and that all other data marked with SIGAD US-984* is NSA FISA data. CES believes that the appropriate remedy is to correct the classification of the data before it is fed into our systems. This is an ongoing issue which should not impede the approval of this SPF but the matter should be addressed. CES will ensure that all analysts accessing these databases know that data marked with the SIGAD US984J and case notation XX.SQF* is FBI FISA data, and that all other data marked with SIGAD US-984* is NSA FISA data, and that this data should be classified TOP SECRET//COMINT - ECI RAGTIME// NOFORN. Ideally all FISA and non-FISA material should be held separately, and FBI and NSA FISA should be partitioned by individual target. The Office of Oversight and Compliance will work with S3 dataflow and Special Source Operations to correct the markings/classification of data at the front end.

(S//SI) CES at NSAW will work to ensure that all individuals working the cryptanalysis mission at the CCs have the appropriate clearances for access to sensitive data, including RAGTIME, and will dictate specific policy and procedural security measures.

REQUIREMENTS: (TS//SI//NF) Following recent meetings and discussions among SID Oversight and Compliance (SV) and NSAW CES, the following are recommendations and requirements that CES and the Cryptologic Centers should agree to implement prior to accessing, handling, processing, retaining, and disseminating NSA FISA and CT FBI FISA-derived collection.

SV requirements: NSA/CSS TX, NSA/CSS GA, and NSA/CSS HI should commit to:

1) (S//SI) The creation of a permanent FISA coordinator position, to be staffed initially by a person experienced with FISA procedures, to ensure compliance with FISA minimization procedures; build a culture and climate of FISA awareness; and facilitate on-site ability to train, field questions, and handle time-sensitive FISA issues.

(S//SI) NSA/CSS TX has identified a permanent FISA coordinator; however that person has no FISA experience. The CES Mission Manager at TX, who has FISA experience, must perform oversight of CES activities and must participate in the new coordinator's FISA training. SID Oversight & Compliance will brief both individuals on their responsibilities.

(TS//SI//NF) NSA/CSS GA and NSA/CSS HI have permanent FISA coordinators who have been supporting the Counterterrorism analytic mission. CES must work with those persons to ensure oversight of CES activities. The FISA coordinators will ensure consistent FISA oversight across all Cryptologic Center activities.

2) (S//SI) The creation of a core FISA workforce which, at all times, contains a stable body of personnel who ideally have at least one year's experience working FISA. A stable, non-transient workforce ensures a well-founded culture for FISA, as has been established at NSAW over many years. Such a culture minimizes the number of FISA-related violations by reinforcing the requirements, restrictions, and sensitivities of accessing and processing FISA.

(S//SI) The CES Mission Managers at Texas, Georgia, and Hawaii have FISA experience and will have supervisory responsibilities over all CES employees at those sites. CES will ensure that all cryptanalysts at Texas, Georgia, and Hawaii will be trained on how to perform the CES mission and on how to handle sensitive materials; all will be knowledgeable about USSID SP0018 and Annex A that describes FISA handling.

3) (S//SI) Provide assurances and documentation that the on-site physical layout of terminals and the means to secure the FISA material is such that access is restricted to only cleared personnel with a need for access to the FISA data.

(S//SI) Seating for individuals performing the cryptanalysis mission will be clustered together to ensure that they have visual and acoustical privacy for technical conversations and to ensure that their conversations and the data displayed on their computer screens is neither accessible nor viewable by those who do not have the appropriate clearances and a "need-to-know". In addition, these individuals will have one or more dedicated printers and combination safes for storage of any authorized FISA material.

4) (S//SI) Provide assurances that FISA material will not be revealed or disseminated as part of site briefings or demonstrations, or in any other format, unless it conforms to and is handled in accordance with FISA Court requirements and minimization procedures approved by the Attorney General, and NSA dissemination policies and procedures. Due to the sensitivity of the sources and methods used to obtain this collection, it cannot be shared with site visitors or other uncleared personnel without proper minimization and attribution to protect those sources and methods.

OGC requirements:

(S//SI) Except in exigent circumstances, all personnel that will have access to FISA material should receive initial OGC USSID SP0018 and FBI FISA minimization briefings in person. The briefings given by OGC are interactive in nature and the personal setting gives OGC a better opportunity to interact with all participants. When in person briefings are not possible, briefings will be done via VTC.

RECOMMENDATION: (U) SIGINT DIR concur on access with oversight as described.

SIGINT DIR'S DECISION:

Concur: [redacted] Date: 9/6/06

Nonconcur: _____ Date: _____

Other: _____ Date: _____

CHIEF,
SID OVERSIGHT & COMPLIANCE

4 August 2006

TO: (U) SIGINT Director

SUBJ: (S) Recommended Requirements for Cryptanalysts at CCs at Texas, Georgia and Hawaii to access NSA and FBI FISA material.

(TS//SI) This request will set a precedent as no prior request for access to NSA FISA material outside NSAW has been approved. NSA FISA is SIGINT derived from NSA's own submissions to the US FISA Court. An individual in SID Oversight and Compliance (SV), in a personally sworn declaration to the US FISA Court, assures the Court that all individuals, wherever located and in any job (linguist, crytpanalyst, reporter, collector, etc.), who access or use NSA FISA material are trained and will comply with all NSA obligations attached to this sensitive access.

(TS//SI) While SV supports the S3/CES build out to the Cryptologic Centers in principle, SV has learned that there are existing deficiencies in classification and handling of NSA FISA and FBI FISA material in CES's databases that must be addressed and fixed before additional access at the CCs is approved.

(TS//SI) It is vital that both NSA FISA and FBI FISA material be properly and separately identified so that 1) users of that material know that they are accessing NSA FISA or FBI FISA, and 2) NSA can remain in compliance with Department of Justice and all other obligations for FISA handling and minimization. It is possible that there are already FISA violations resulting from the way data has been stored in these databases and it is critical that these problems be fixed before the problems are spread to new locations.

TOP SECRET//COMINT//20291123

(TS//SI) For example, the databases FOURSCORE and ZAP contain both NSA FISA and FBI FISA that does not carry the appropriate classification (all NSA and FBI FISA material must carry the "TS//SI-ECI RGT//NOFORN//2029123" classification. FBI FISA should also be marked with the OGC-approved FBI FISA banner). Further, NSA FISA and FBI FISA materials are mixed together within the databases, despite the differences in allowed retention between the two versions of FISA, and both are mixed with non-FISA material. CES should also provide SV with an SOP clarifying how access (by both CES and S2 target analysts) to these target folders is maintained, including what checks are in place to verify user clearances to view NSA FISA and/or FBI FISA material.

(TS//SI) If you support access in principle, I would recommend that no action be taken to establish accounts at the CCs for these CES databases until SV can ensure that the issues of classification, partitioning and access are resolved and any existing FISA access or retention violations are identified and cleared up.

(TS//SI) Further, SV recommends that this access not be approved until S3/CES and the Cryptologic Centers involved coordinate with the offices that sponsored the NSA FISA court orders and agree to the responsibilities that each will have relative to satisfying the FISA minimization procedures (USSID SP0018, Annex A). This is necessary to ensure that all individuals who touch NSA FISA material personally abide by NSA's FISA handling and minimization requirements, ensure that no one makes erroneous assumptions about what another office is doing vis-a-vis meeting those requirements, and ensure that the NSA declarant can swear under oath that NSA abides by its obligations.

[redacted]

TOP SECRET//COMINT//20291123