SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
SIGINT DIR	2012-704	S353-113-11

THRU	ACTION	EXREG SUSPENSE
	[X] APPROVAL	
SUBJECT	[ ] SIGNATURE	KCC SUSPENSE
(S//REL) SSO's Support to the FBI for Implementation of their Cyber FISA Orders	[ ] INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION
V2, V3, V07

SUMMARY

RECOMMENDATION: (U//FOUO) Approve the provision of the assistance to FBI, with the proviso that the FBI remains responsible for any additional expenses incurred.

PURPOSE: (S//REL) To obtain the SIGINT Director's approval for the Office of Special Source Operations (SSO) to provide ongoing technical assistance to the Federal Bureau of Investigation (FBI) for the implementation of the various orders they have obtained, and will obtain, from the Foreign Intelligence Surveillance Court (FISC) in certain Cyber cases involving agents of foreign powers (e.g. - [redacted] soon, [redacted]). The preparation of this Staff Processing Form was a collaborative effort between SSO and the NSA Office of General Counsel (OGC).

BACKGROUND: (S//REL) On December 20, 2011, NSA received a request for technical assistance from the FBI seeking access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers. The FISC has issued a number of orders at the request of the FBI authorizing electronic surveillance directed at communications related to computer intrusions being conducted by foreign powers. The orders include some that are limited to pen register/trap and trace (PRTT) information as well as others that authorize collection of content. The first of these for which NSA assistance has been requested is directed at communications related to intrusions conducted by the [redacted] (Docket Number 11-91), regarding what FBI refers to as STYGIAN FLOW.

(S//REL) In mid-2011, prior to receipt of the request for technical assistance, SSO became aware of FBI's plans to seek these orders and has been in discussions with FBI throughout the latter half of the year, in the belief that use of NSA's collection/processing infrastructure would allow the FBI to

Continued...

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
OGC	[redacted] /email/ 30 Jan.				
F1B	[redacted] /email/ 9 Feb.		S3	[redacted] /s/ 3-20-12	
SI	[redacted] /s/		S35	[redacted]	
NTOC	[redacted] /s/		SV	[redacted] /s/ 31 Jan.	
T	[redacted] /s/ 6 Feb		POC	[redacted]	[redacted]

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
[redacted] Digitally signed by [redacted] DN: c=US, [redacted] ou=DOD, ou=NSA, ou=D002, [redacted] Date: 2011.12.21 07:42:01 -05'00'	S353	[redacted]	20111221

FORM A6796DE REV NOV 2008(Supersedes A6796 FEB 05 which is obsolete)
NSN: 7540-FM-001-5465
Derived From: NSA/CSS Manual 1-52
Dated: 8 January 2007
Declassify On: 20320108

SECURITY CLASSIFICATION

SECRET//REL TO USA, FVEY

maximize the value of the collection without incurring the expenses associated with duplication of that infrastructure. Although FBI conducts numerous electronic surveillances without NSA's assistance, the vast majority of them are directed against targets located inside the United States, and U.S. providers served with FISC orders are ordinarily able to identify and deliver to the FBI most, if not all, of the targets' communications that they carry. That is because such electronic surveillance is typically effected at a point or points in the provider's infrastructure in physical proximity to the target's location. In the case of computer intrusions being conducted by foreign powers, the providers may be carrying a target's communications, but it is much more difficult to identify and locate them, because the communications in question will enter and leave the United States via any convenient path, and their path may be obscured to avoid detection. In other words, in these cases, because the target's location is outside the United Statues and not well-characterized, effecting the surveillance via FBI's traditional means is not effective.

(S//REL) However, in support of FAA and in anticipation of the need to conduct similar collection activities for computer network defense purposes, over the last decade, NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States. Collection at such chokepoints is much better suited to electronic surveillance directed at targets located outside the United States than FBI's traditional means of collection. In theory, FBI could rely on the orders it has obtained to direct U.S. providers to conduct surveillance at these chokepoints without relying on NSA capabilities, but it would take a considerable amount of time to do so, and FBI would have to reimburse the providers to recreate (i.e., duplicate) what NSA has already put in place. The cost alone would be prohibitive, and the time lost in doing so would necessarily result in a loss of foreign intelligence.

(S//REL) The assistance being sought by the FBI is limited in nature. The U.S. providers served with Secondary Orders in this matter will assume full responsibility for the provisioning of PR/TT and content collection to the FBI. Since all of the authorized "facilities" (typically known as "targeted selectors" in NSA parlance) to date are Internet Protocol (IP) addresses used by the targets, there is no question as to the providers' abilities to employ devices under their control (e.g., routers) to provision fully-compliant, authorized intercept.

(S//REL) Neither the providers nor the FBI will require NSA's Government off the Shelf (GOTS) Digital Network Intelligence (DNI) collection and processing solutions (e.g., TURMOIL, XKEYSCORE). Instead, metadata and full content derived from the authorized intercept will be produced using Commercial off the Shelf (COTS) processing solutions. If these COTS processing solutions involve components developed at NSA's expense and used, primarily, for NSA's Cyber survey purposes, the SSO will make careful and informed decisions prior to authorizing use of these components.

(S//REL) Prior to authorizing use of the extensive secure Wide Area Networks established at the two primary providers (cover terms, LITHIUM and ARTIFICE, respectively) as the end-to-end data delivery infrastructure to connect intercept and processing locations with the FBI's designated Cyber data repository at the Engineering Research Facility, Quantico, VA, SSO will make careful and informed decisions to ensure this capability is undertaken on a 100% non-interference basis with NSA's current and future data backhaul needs on these same networks.

(S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

(S//REL) Should the FBI require a sustained and high-level of dedicated analytical resources (i.e., cleared, technical manpower) at the providers in order to optimize the collection effectiveness of their PR/TT and content orders, they will contract for those services directly with the providers. If, on the other hand, the FBI's requirement for provider analytical support is more ad hoc and aperiodic in nature during the period of time these orders remain in effect, SSO will make careful and informed decisions prior to authorizing labor charges against the relevant SSO contracts with the providers for these services on behalf of the FBI. Any charges that cannot be justified as necessary for NSA purposes will not be made unless/until FBI agrees to reimburse NSA.

DISCUSSION: (S//REL) If SID decides to approve the requested assistance, SSO will assist the FBI in effecting any cyber orders submitted to it after the NSA/OGC has verified that each of them contains language permitting NSA's involvement. As stated in Attachment 1, NSA will have the opportunity to review and respond to any proposed use of FISA-derived information from these collections prior to the Attorney General authorizing the use of such information in any criminal proceedings.

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA

Continued...

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA Amendments Act (FAA) of 2008. To the contrary, the relatively recent discovery of these FBI Cyber FISA orders and the countless pages of SIGINT-derived evidence that was cited in the respective Applications to the FISC have already formed the basis for a dialog between NSA's OGC and the Department of Justice's National Security Division.

(C) DIRECTOR, SIGNALS INTELLIGENCE DECISION:

CONCUR: Teresa H. Shea DATE: 3-827-12

NON-CONCUR:_____ DATE:_____