

This document is made available through the declassification efforts  
and research of John Greenewald, Jr., creator of:

# The Black Vault

---



The Black Vault is the largest online Freedom of Information Act (FOIA)  
document clearinghouse in the world. The research efforts here are  
responsible for the declassification of hundreds of thousands of pages  
released by the U.S. Government & Military.

**Discover the Truth** at: **<http://www.theblackvault.com>**

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

The application proposed allowing 10 NSA analysts access to the database.<sup>238</sup> The NSA analysts were to be briefed by the NSA Office of General Counsel concerning the circumstances under which the database could be queried, and all queries would have to be approved by one of seven senior NSA officials.<sup>239</sup> ~~(TS//SI//NF)~~

The application explained that the bulk collection would be queried with particular e-mail addresses in order to conduct chaining [REDACTED]. The application proposed that queries of the e-mail meta data archive would be performed when the e-mail address met the following standard:

based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [REDACTED]

[REDACTED]

Under the PR/TT application, the government proposed that it be authorized under FISA [REDACTED] to use the reasonable articulable suspicion standard to query the database with specific addressing information [REDACTED]

~~(TS//STLW//SI//OC/NF)~~

In addition, the NSA proposed applying the minimization procedures in the United States Signals Intelligence Directive 18 (USSID 18) to minimize the information reported concerning U.S. persons. According to the application, compliance with these minimization procedures would be

<sup>238</sup> At the government's request the number of NSA analysts was increased to 15 when the Order was renewed [REDACTED] ~~(TS//SI//NF)~~

<sup>239</sup> When it granted the government's application, the FISA Court noted that in conventional pen register and trap and trace surveillances a court first reviews the application before a particular e-mail account can be targeted. The FISA Court stressed the importance of the NSA Office of General Counsel's obligation to ensure that the legal adequacy for such queries was met. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

monitored by the NSA's Inspector General and General Counsel. The government also proposed that in each renewal application the NSA would report to the FISA Court on queries that were made during the prior period and the application of the reasonable articulable suspicion standard for determining that queried addresses were terrorist-related. ~~(TS//SI//NF)~~

The application and supporting documents explained how the NSA intended to use the collected meta data. The NSA sought to use the meta data [REDACTED] to apply sophisticated algorithms to develop contact chaining [REDACTED].<sup>240</sup> In the application, the NSA estimated that through external intelligence gathering and internal analysis it would meet the proposed querying standard on average less than once a day. The NSA further estimated that these queries would generate approximately 400 tips to the FBI and CIA per year.<sup>241</sup> Of these tips to the FBI and CIA, the NSA projected that 25 percent would include U.S. person information, amounting to leads including information on about "four to five U.S. persons each month." ~~(TS//SI//NF)~~

#### 4. Judge Kollar-Kotelly Raises Questions about PR/TT Application ~~(TS//SI//NF)~~

On [REDACTED] Judge Kollar-Kotelly wrote Baker to inform him that she was considering the application and was in the process of preparing an opinion and order in response to it. She wrote that before the opinion and Order could be completed, however, she required written responses to two questions:

- (1) Apart from the First Amendment proviso in the statute (50 U.S.C. § 1842(a)(1), (c)(2)), what are the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons?
- (2) For how long would the information collected under this authority continue to be of operational value to the counter-terrorism investigation(s) for which it would be collected? ~~(TS//SI//NF)~~

Baker responded in a letter to the FISA Court on [REDACTED]. Concerning the first question, Baker's letter asserted that the proposed

<sup>240</sup> These analytical tools are discussed in Chapter Three. (U)

<sup>241</sup> The NSA arrived at this estimate based on the assumption that each query could be expected to generate [REDACTED] e-mail addresses "one level out," and [REDACTED] addresses "two levels out." The overall number of direct and indirect contacts with the initial seed address would be significantly reduced using "analytical tradecraft." ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

collection activity was consistent with the First Amendment and that he could find no reported decisions holding that the use of pen register and trap and trace devices violated the First Amendment. ~~(TS//SI//NF)~~

In his letter, Baker argued that although the meta data collection would include entirely innocent communications, a good-faith investigation does not violate the First Amendment simply because it is "broa[d] in scope" (quoting *Laird v. Tatum*, 408 U.S. 1, 10 (1972)). He also wrote that the use of the collected meta data would be "narrowly constrained" because the querying standard for the meta data would be subject to a "reasonable articulable suspicion" of a nexus to [REDACTED] ~~(TS//SI//NF)~~

Regarding Judge Kollar-Kotelly's second question concerning how long the collected meta data would continue to be of operational value, Baker wrote that, based on the analytic judgment of the NSA, such information would continue to be relevant to [REDACTED] for at least 18 months. Baker also advised that the NSA believed the e-mail meta data would continue to retain operational value beyond 18 months, but that it should be stored "off-line" and be accessible to queries only by a specially-cleared administrator. Baker proposed that 3 years after the 18-month timeframe, or 4½ years after it is first collected, the meta data could be destroyed.<sup>242</sup> ~~(TS//SI//NF)~~

## 5. FISA Court Order (U)

In response to the application and follow-up questions, on July 14, 2004, Judge Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order based on her findings that the proposed collection of e-mail meta data and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. ~~(TS//HCS//SI//NF)~~

The Order granted the government's application in all key respects. It approved for a period of 90 days the collection within the United States of e-mail meta data [REDACTED] The Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. ~~(TS//HCS//SI//NF)~~

In the Order, the Court found that the information to be collected was "dialing, routing, addressing, or signaling information" that did not include

<sup>242</sup> On [REDACTED] the FISA Court issued an order authorizing the NSA to maintain bulk meta data on-line for 4½ years after which time it must be destroyed. According to the NSA Office of General Counsel, the NSA still follows this retention procedure. ~~(TS//HCS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

the contents of any communication. The Court stressed that it was only authorizing collection of the [REDACTED] categories of information delineated in the application, but acknowledged that additional information "could be gleaned" from that meta data, [REDACTED]

[REDACTED] The Court found that the means by which the [REDACTED] categories of meta data were to be collected met the FISA definition of a "pen register," and that the means for collecting the [REDACTED] category of meta data satisfied the FISA definition of a "trap and trace device." See 18 U.S.C. § 3127(3) & (4), as incorporated in FISA at 50 U.S.C. § 1841(2). ~~(TS//HCS//SI//NF)~~

The Court further found that the government satisfied FISA's requirement that the application certify that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism. The Court concluded that, "under the circumstances of this case, the applicable relevance standard does not require a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [REDACTED] FBI investigations."<sup>243</sup> ~~(TS//HCS//SI//NF)~~

The Court also agreed with the government's position that the privacy interest at stake in the collection of e-mail meta data did not rise to the "stature protected by the Fourth Amendment," and that the nature of the intrusion was mitigated by the restrictions on accessing and disseminating the information, only a small percentage of which would be seen by any person. ~~(TS//HCS//SI//NF)~~

In sum, the Court concluded that the use of pen register and trap and trace devices to collect e-mail meta data would not violate the First Amendment, stating that

the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [REDACTED]

---

<sup>243</sup> The Court cautioned that its ruling with regard to the breadth of the meta data collection should not be construed as precedent for similar collections of the full content of communications under the electronic surveillance provisions of FISA. The Court noted important differences in the two types of collection, including the fact that overbroad electronic surveillance requires a showing of probable cause to believe the target is an agent of a foreign power, while the bulk meta data collection under FISA's pen register and trap and trace device provisions merely requires a showing that the overbroad collection is justified as necessary to discover unknown [REDACTED] persons. The Court also contrasted the high privacy interests at stake with respect to content communications with the absence of a privacy interest in meta data. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

██████████ related operatives and thereby obtaining information likely to be ██████████ to ongoing FBI investigations.  
~~(TS//HCS//SI//NF)~~

However, the Court also was concerned that "the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons." The Court noted that under 50 U.S.C. § 1842(c)(2), pen register and trap and trace information about the communications of a U.S. person cannot be targeted for collection unless it is relevant to an investigation that is not solely based upon the First Amendment. Therefore, the Court ordered that the NSA modify its criterion for querying the archived data by inserting the following underlined language, as shown below:

██████████ will qualify as a seed ██████████ only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with ██████████  
provided, however, that an ██████████ believed to be used by a U.S. person shall not be regarded as associated with ██████████ solely on the basis of activities that are protected by the First Amendment to the Constitution. ~~(TS//HCS//SI//NF)~~

Regarding the storage, accessing, and disseminating of the e-mail meta data obtained by the NSA, the Court ordered that the NSA must store the information in a manner that ensures it is not commingled with other data, and must "generate a log of auditing information for each occasion when the information is accessed, to include the . . . retrieval request." The Court further ordered that the e-mail meta data "shall be accessed only through queries using the contact chaining ██████████" as described by the NSA in the government's application. ~~(TS//HCS//SI//NF)~~

The Court noted the "distinctive legal considerations" involved in implementing the authority the Court was vesting in the NSA. Specifically, the Court observed that conventional pen register and trap and trace surveillance required judicial review before any particular e-mail account could be targeted. However, by granting the government's application, the Court noted that the NSA's decision to target an e-mail address (sometimes referred to as a "seed ██████████") would be made without judicial review. Therefore, the Court ordered that the NSA's Office of General Counsel would be responsible for training analysts to comply with querying standards and

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

other procedures and "to review the legal adequacy for the basis of such queries, including the First Amendment proviso . . . ." ~~(TS//HCS//SI//NF)~~

As suggested by Baker in his [REDACTED] response to Judge Kollar-Kotelly's inquiry regarding the useful life of the collected data, the Court ordered that the e-mail meta data shall be available for 18 months for querying. The Court further ordered that after the 18-month period, the data must be transferred to an "off-line" tape system from which it could still be accessed for querying upon approval of the NSA officials authorized to approve queries, and that such meta data must be destroyed 4½ years after initially collected. ~~(TS//HCS//SI//NF)~~

The Court's Order was set to expire after 90 days. The Court required that any application to renew or reinstate the authority granted in the Order must include: a report discussing queries made since the prior application and the NSA's application of the requisite legal standard to those queries; detailed information regarding [REDACTED] proposed to be added to the authority granted under the Order; any changes to the description of the [REDACTED] described in the Order or the nature of the communications [REDACTED] and any changes to the proposed means of collection, including to the [REDACTED] of the pen register and trap and trace devices [REDACTED] ~~(TS//HCS//SI//NF)~~

Finally, the Court issued separate orders [REDACTED] to assist the NSA with the installation and use of the pen register and trap and trace devices and to maintain the secrecy of the NSA's activities. These orders [REDACTED] called "secondary orders," [REDACTED] The NSA was directed to compensate the carriers for all assistance provided in connection with the PR/TT Order. ~~(TS//HCS//SI//NF)~~

Baker and other witnesses told us that obtaining the Order was seen by the Department as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk e-mail meta data collection. [REDACTED]

[REDACTED] Comey told us that obtaining the Order from the FISA Court also provided an "air of legitimacy" to the program.<sup>244</sup> ~~(TS//STLW//SI//OC/NF)~~

<sup>244</sup> Comey and others informally referred to the PR/TT Order as "the mother of all pen registers." ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~**B. President Orders Limited Use**~~(TS//STLW//SI//OC/NF)~~

E-mail meta data collection under FISA pen register authority began when the PR/TT Order took effect on July 14, 2004. As required by the Order, the data was placed in its own database or "realm."

~~(TS//STLW//SI//OC/NF)~~

We discuss below the President's directive and the OLC memorandum that was drafted to analyze its legality. ~~(TS//STLW//SI//OC/NF)~~

**1. The President's August 9, 2004, Memorandum to the Secretary of Defense** ~~(TS//SI//NF)~~

On August 9, 2004, the same day a routine Presidential Authorization was issued to continue Stellar Wind, the President sent a separate memorandum to the Secretary of Defense regarding the use of the e-mail meta data collected. The memorandum directed the Secretary of Defense that, consistent with the August 9, 2004, Presidential Authorization (and any successor Presidential Authorizations), the NSA was authorized to e-mail meta data when there was a reasonable articulable suspicion that (1) a party to the communication belonged to and (2) the purpose of the search was to produce foreign intelligence information concerning threats.

<sup>245</sup> ~~(TS//STLW//SI//OC/NF)~~

<sup>245</sup> The President's Memorandum provided that the authority to conduct such searches was to terminate on September 23, 2004. In the September 17, 2004, Presidential Authorization, this authority was extended until November 18, 2004. ~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~**2. Office of Legal Counsel Determines** [REDACTED]~~(TS//STLW//SI//OC/NF)~~

Jack Goldsmith resigned as Assistant Attorney General for the Office of Legal Counsel on July 30, 2004. Goldsmith was replaced by Daniel Levin, who served as the Acting Assistant Attorney General for OLC until February 2005. (U)

During late 2004, at the request of Comey and Ashcroft, Levin began work on an OLC memorandum addressing whether it would be lawful for the NSA to analyze the e-mail meta data collected [REDACTED]

[REDACTED]

~~(TS//STLW//SI//OC/NF)~~

<sup>246</sup> The [REDACTED] e-mail meta data has since been placed on tape and is being held by the NSA Office of General Counsel pursuant to a preservation order.

~~(TS//STLW//SI//OC/NF)~~

<sup>247</sup> The final version of the OLC memorandum was signed by Levin on February 4, 2005. Levin told the OIG that a "policy decision" was made to limit application of the memorandum to the specific purpose [REDACTED]. However, Levin stated that, based on his analysis of the issue, he believed that [REDACTED]

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

Thus, the President asserted extrajudicial authority to order the further use of e-mail meta data collected under Stellar Wind for the limited purpose described in his August 9 memorandum. The FISA Court was notified of this action, although the government did not seek its permission. ~~(TS//STLW//SI//OC/NF)~~

### C. Non-Compliance with PR/TT Order ~~(TS//SI//NF)~~

As with other orders issued under FISA, the PR/TT Order was renewed every 90 days. During the early renewals, two major instances of non-compliance were brought to the FISA Court's attention. As described below, these violations of the Order resulted primarily from the NSA senior officials' failure to adequately communicate the technical requirements of the Order to the NSA operators tasked with implementing them, and from miscommunications among the FISA Court, the Justice Department, and the NSA concerning certain legal issues. ~~(TS//SI//NF)~~

#### 1. Filtering Violations ~~(TS//SI//NF)~~

On [REDACTED] OIPR filed a Notice of Compliance Incidents with the FISA Court. In the Notice, Baker stated that the compliance incidents cited in the Notice "raise compliance issues with about [REDACTED] of the collection authorized by the Court."<sup>248</sup> The Notice included as an attachment a letter from NSA General Counsel Robert Deitz to Baker describing incidents that led to "unauthorized collection." Deitz learned of these incidents on [REDACTED].<sup>249</sup> ~~(TS//SI//NF)~~

[REDACTED]

[REDACTED] could be queried for any purpose. Levin told us that, other than Addington, no one else was pushing to broaden the memorandum's application. ~~(TS//STLW//SI//OC/NF)~~

<sup>248</sup> Subsequent filings indicate that [REDACTED] of overall collections under the Order were affected by the violations. ~~(TS//SI//NF)~~

<sup>249</sup> One tipper that was based on this unauthorized collection was disseminated as a lead to the FBI but was subsequently retracted. ~~(TS//SI//NF)~~

[REDACTED]

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

[REDACTED]

Baker told us that Judge Kollar-Kotelly was "not happy" about the violation. On [REDACTED] the FISA Court issued an Order Regarding [REDACTED] (Compliance Order). The Court wrote that the "NSA violated its own proposed limitations, which were attested to by its Director and, at the government's invitation, adopted as provisions of the orders of this Court." The Court found that the violations "resulted from deliberate actions by NSA personnel," as distinguished from technical failures. The Court stated it was also troubled by the duration of the violations, which extended from July 14 through [REDACTED] and that the Court was reluctant to issue a renewal of the PR/TT Order as to [REDACTED] (TS//SI//NF)

That same day, the Court issued an Order to address [REDACTED] (Order Regarding Required Information for Authorities Involving [REDACTED], requiring that any application for renewal or reinstatement of PR/TT surveillance authorities [REDACTED] be accompanied by a sworn declaration by the Secretary of Defense attesting to the state of compliance with the PR/TT Order and a description of the procedures that would be used to ensure compliance. (TS//SI//NF)

On [REDACTED] the government moved for an extension of time (until [REDACTED]) within which to provide the Secretary of Defense's declaration. The motion, which the Court granted, assured the Court that surveillance [REDACTED] had been terminated on [REDACTED] and that on [REDACTED] the NSA had moved to a separate database all meta data obtained [REDACTED] through [REDACTED]. The NSA also represented that it reconstructed its contact chaining database using only properly obtained meta data and purged the unauthorized meta data from the system. (TS//SI//NF)

A declaration by NSA Director Hayden accompanying the government's motion stated a total of [REDACTED] e-mail addresses were tipped as leads to the FBI and CIA during the violation period and that [REDACTED] of these leads may have come from the unauthorized collection. Hayden wrote that

[REDACTED]

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

this lead was purged from the FBI's and CIA's databases on [REDACTED]

[REDACTED] (TS//SI//NF)

The NSA Office of the Inspector General subsequently issued a report on its investigation of the unauthorized collections. The NSA OIG report stated that the filtering violations "probably led to actual unauthorized collection, but we have not been able to determine the extent of such collection, and we are not certain that we will be able to do so." The report further stated that the collection program under PR/TT Order authority was

[REDACTED]

(TS//STLW//HCS//SI//OC/NF)

The report concluded that "there were systemic management failures within both [REDACTED] within the Signals Intelligence Directorate (SID)], and a complete lack of program management with regard to collection." The report stated that while the training provided by the NSA Office of General Counsel was "vigorous, conscientious, and compliant with the July 14 Order, it was inadequate in scope." (TS//STLW//HCS//SI//OC/NF)

According to the report, the NSA removed as much of the tainted collection from the PR/TT database as possible. The NSA was unable to segregate unauthorized collection from [REDACTED] so it rebuilt that portion of the PR/TT database from [REDACTED] (the day after the violation was discovered), forward. Moreover, according to the NSA OIG report, analytical personnel were restricted from accessing the unauthorized meta data. (TS//STLW//HCS//SI//OC/NF)

## 2. FISA Court Renews PR/TT Order (TS//SI//NF)

The FISA Court's PR/TT Order expired on [REDACTED] On that date the government filed its first renewal application. The Renewal Application sought authorization to collect e-mail meta data on [REDACTED] and stated that the NSA had fully complied with the PR/TT Order with respect to [REDACTED] The government did not seek reauthorization for collection [REDACTED] due to a variety of operational reasons which the application did not specify. (TS//SI//NF)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Judge Kollar-Kotelly signed the Renewal Order on [REDACTED] authorizing through [REDACTED] the use of pen register and trap and trace devices at [REDACTED] to collect e-mail meta data. The Renewal Order and the original Order were similar in most respects. However, in the Renewal Order the Court required the NSA to submit reports every 30 days concerning queries made since the prior report and describing any changes made to [REDACTED] and the [REDACTED] [REDACTED] <sup>251</sup> (TS//SI//NF)

3. [REDACTED]

Baker told us that during one of his "oversight" visits to the NSA following the FISA Court's PR/TT Order, he was given a demonstration of how the NSA analysts processed the e-mail meta data, including an explanation of how e-mail meta data is collected and queried. Baker said he was informed that among the pieces of data that might be used to meet the reasonable articulable standard for querying the e-mail meta data [REDACTED]

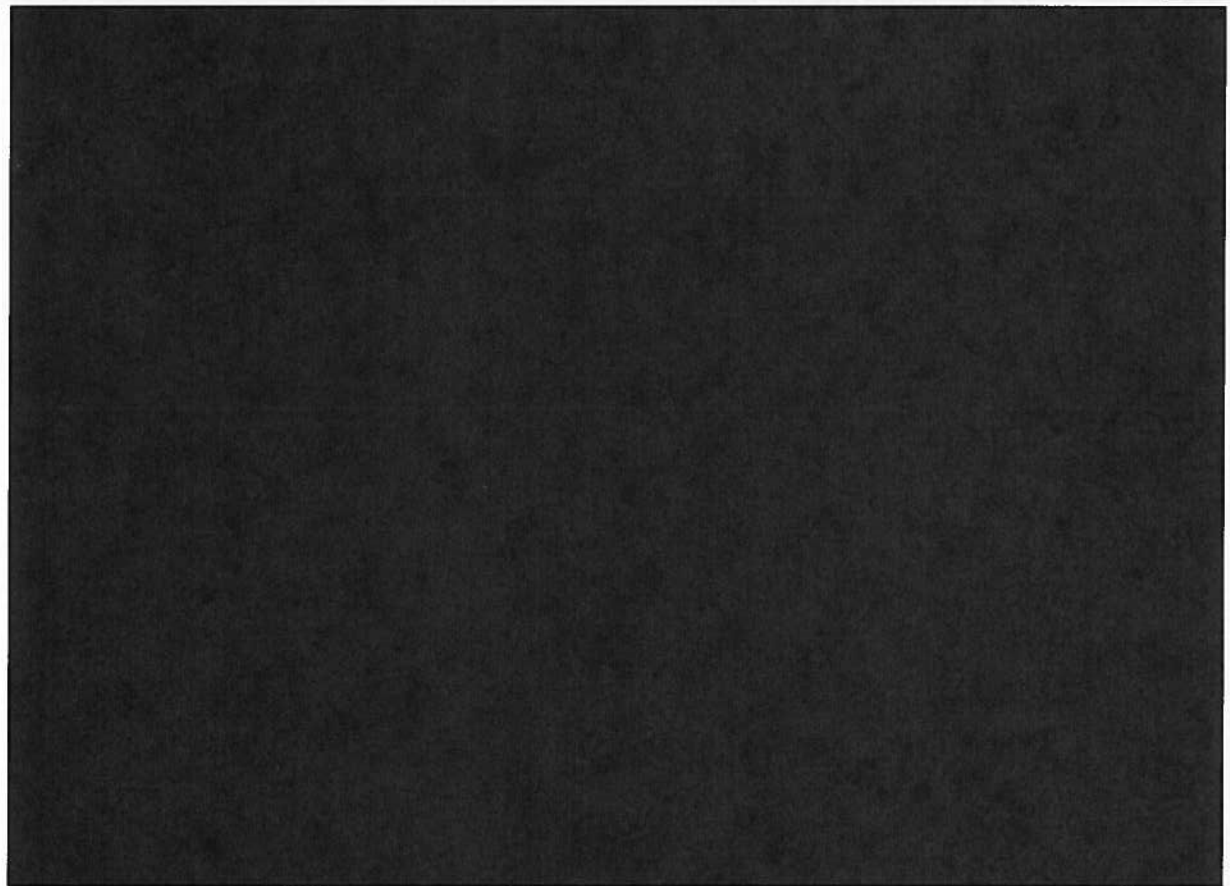
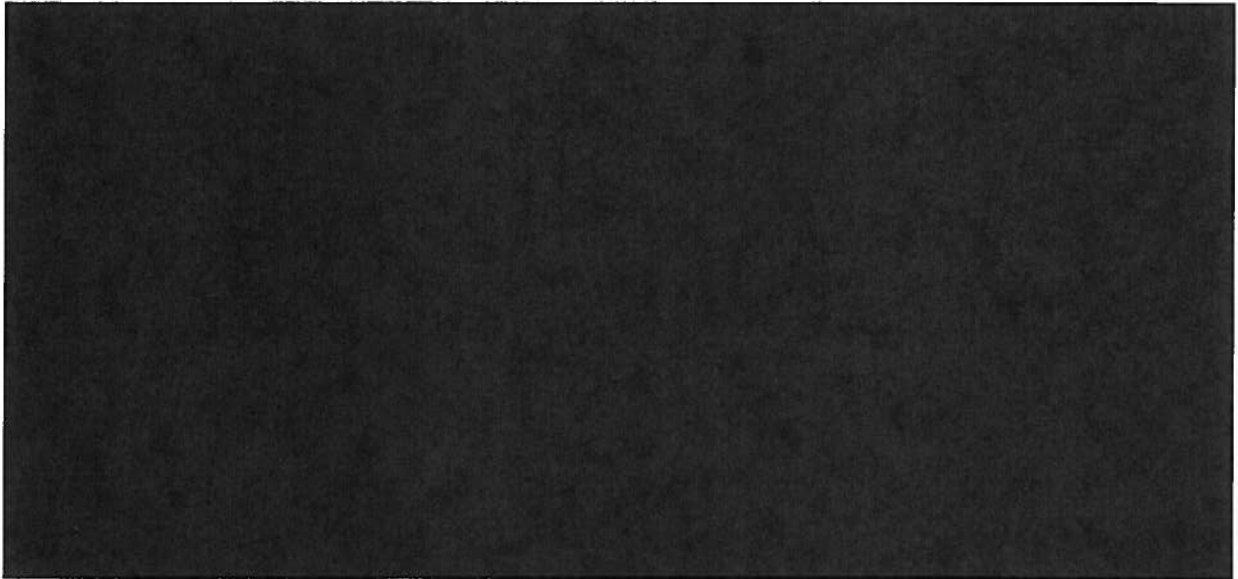
[REDACTED] (TS//STLW//SI//OC/NF)

<sup>251</sup> In the initial PR/TT Order, the Court required such a report only upon the government's submission of a renewal application every 90 days. (TS//SI//NF)

<sup>252</sup> As noted above, seed [REDACTED] are e-mail addresses or telephone numbers for which a reasonable articulable suspicion exists to believe the [REDACTED] is related to a terrorist entity. Seed [REDACTED] are used to query the meta data database to reveal links with other addresses or numbers. (TS//SI//NF)

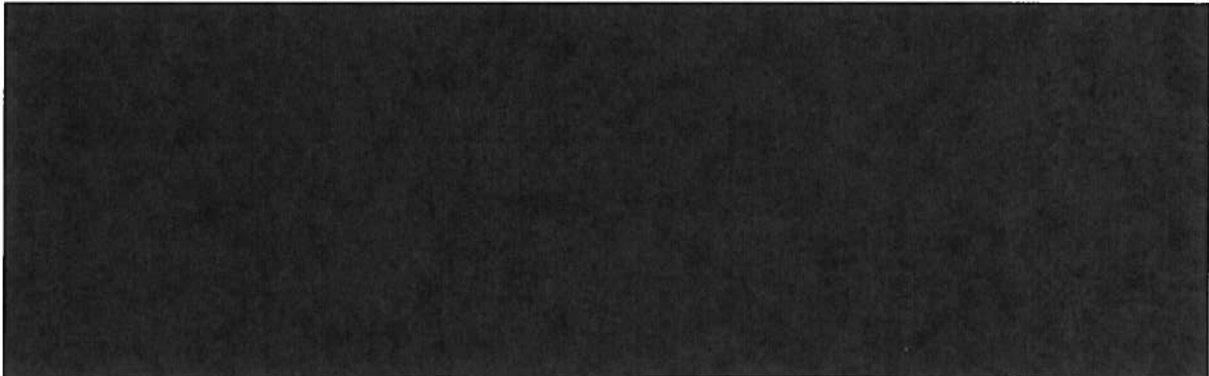
~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~




~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~**D. Subsequent PR/TT Applications and Orders** ~~(TS//SI//NF)~~

As described above, the PR/TT Order was first renewed on [REDACTED] and was renewed by subsequent orders of the FISA Court at approximately 90-day intervals.<sup>254</sup> ~~(TS//SI//NF)~~

On [REDACTED] the FISA Court issued a Supplemental Order requiring the government to enhance its reporting to the Court of the foreign intelligence benefits realized under the PR/TT Orders. Writing for the FISA Court, Judge Kollar-Kotelly stated that the authority granted under these orders allowed the NSA "to collect vast amounts of information about e-mail [REDACTED] communications[.]" but that "the Court is unable on the current record to ascertain the extent to which information so collected has actually resulted in the foreign intelligence benefits originally anticipated." Supplemental Order at 1-2. The government responded with a motion requesting that, in light of prior briefings it had given the FISA Court, it not be required to fully comply with the Supplemental Order. It is not clear what if any specific action the FISA Court took in response to this motion, although based on the OIG's review of the PR/TT docket the government continued to submit regular reports to the FISA Court.


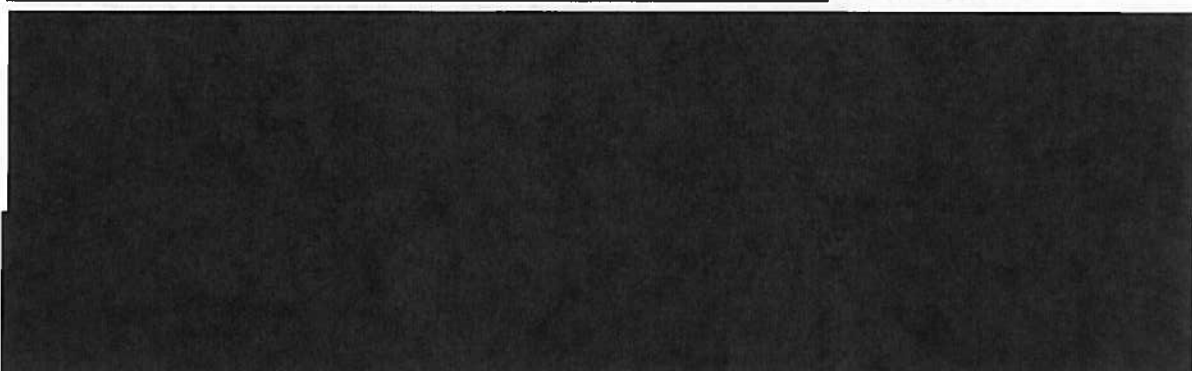
~~(TS//STLW//SI//OC/NF)~~

Under the PR/TT renewal applications the scope of authorized queries against the PR/TT database remained limited to queries that concerned [REDACTED]

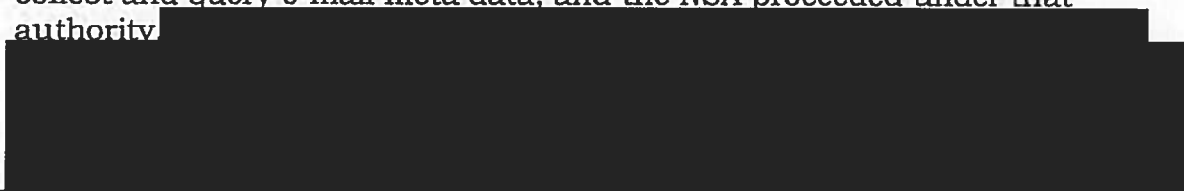


<sup>254</sup> In these renewals, [REDACTED] were added and dropped from [REDACTED] that were approved in the July 14, 2004, PR/TT Order. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~  
(TS//SI//NF)-

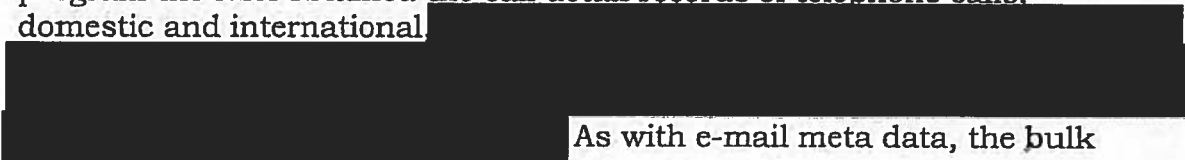
Although the FISA Court continued to renew the NSA's authority to collect and query e-mail meta data, and the NSA proceeded under that authority



(TS//STLW//SI//OC/NF)-

## II. Telephony Meta Data Collection Under FISA (TS//SI//NF)-

The second part of the Stellar Wind program brought under FISA authority was the NSA's bulk collection of telephony meta data (basket 2). As described in Chapter Three, under this aspect of the Stellar Wind program the NSA obtained the call detail records of telephone calls, domestic and international



As with e-mail meta data, the bulk



<sup>257</sup> As discussed in Chapter Three,

Call detail records consist of routing information, including the originating and terminating telephone number of each call, and the date, time, and duration of each call. The call detail records do not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. (TS//SI//NF)-

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

nature of the telephony collection provided the NSA the ability to conduct  
 [REDACTED] - contact chaining [REDACTED]

~~(TS//STLW//SI//OC/NF)~~

The transition of bulk telephony meta data collection from Presidential Authorization under the Stellar Wind program to FISA authority relied on a provision in the FISA statute that authorized the FBI to seek an order from the FISA Court compelling the production of "any tangible things" from any business, organization, or entity, provided the items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. See 50 U.S.C. § 1861. Orders under this provision commonly are referred to as "Section 215" orders in reference to Section 215 of the USA PATRIOT ACT, which amended the "business records" provision in title V of FISA.<sup>258</sup> The "tangible things" the government sought in the Section 215 application described in this section were the call detail records [REDACTED]. ~~(TS//STLW//SI//OC/NF)~~

We describe below the circumstances that led to the government's decision to transition the bulk collection of telephony meta data from presidential authority to FISA Authority. We then summarize the government's initial application and the related Court Order.

~~(TS//STLW//SI//OC/NF)~~

**A. Decision to Seek Order Compelling Production of Call detail records ~~(TS//SI//NF)~~**

The timing of the Department's decision in May 2006 to seek a FISA Court order for the bulk collection of telephony meta data was driven primarily by external events. On December 16, 2005, The New York Times published an article entitled, "Bush Lets U.S. Spy on Callers Without Courts." The article, which we discuss in more detail in Chapter Eight, described in broad terms the content collection aspect of the Stellar Wind program, stating that the NSA had "monitored the international telephone calls of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to al Qaeda." [REDACTED]

~~(TS//STLW//SI//OC/NF)~~

<sup>258</sup> The term "USA PATRIOT Act" is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act." (U)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

On December 17, 2005, in response to the article, President Bush publicly confirmed that he had authorized the NSA to intercept the international communications of people with "known links" to al Qaeda and related terrorist organizations (basket 1). On January 19, 2006, the Justice Department issued a document entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President" and informally referred to as a "White Paper," that addressed in an unclassified form the legal basis for the collection activities that were described in the New York Times article and confirmed by the President.

~~(TS//STLW//SI//OC/NF)~~

According to Steven Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper [REDACTED]

[REDACTED] Although the New York Times article did not describe this aspect of Stellar Wind, reporters at USA Today were asking about this aspect of the program in early 2006. Bradbury [REDACTED] anticipated that a USA Today story would attract significant public attention when it was published.<sup>259</sup> ~~(TS//STLW//SI//OC/NF)~~

[REDACTED]

---

<sup>259</sup> On May 11, 2006, USA Today published the results of its investigation. The article, entitled "NSA Has Massive Database of American Phone Calls," reported that the NSA "had been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth." The article stated that the program, launched shortly after the September 11 attacks, collected the records of billions of domestic calls in order to analyze calling patterns to detect terrorist activity. The article reported that the records provided to the NSA did not include customer names, street addresses, and other personal information, but noted that such information was readily available by cross-checking the telephone numbers against other databases.

~~(TS//STLW//SI//OC/NF)~~

[REDACTED]

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

**B. Summary of Department's Application and Related FISA Court Order (S/NF)—**

As noted previously, applications to the FISA Court that seek an order compelling the production of "tangible things" are commonly referred to as "Section 215" applications, in reference to Section 215 of the USA PATRIOT ACT. Section 215 authorizes the FBI to request a FISA Court order

requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. (U)

50 U.S.C. § 1861(a)(1).<sup>261</sup> Section 215 does not require that the items sought pertain to the subject of an investigation; the government need only demonstrate that the items are relevant to an authorized investigation.<sup>262</sup> (U)

On May 23, 2006, the FBI filed with the FISA Court a Section 215 application seeking authority to collect telephony meta data to assist the NSA in finding and identifying known and unknown members or agents of [REDACTED] in support of the [REDACTED] related FBI investigations then pending and other Intelligence Community operations. The application requested an order compelling [REDACTED] to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. The application described call detail records as routing information that included the

---

<sup>261</sup> "United States person" is defined in FISA as a citizen, legal permanent resident, or unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, and corporations incorporated in the United States as long as such associations or corporations are not themselves "foreign powers." 50 U.S.C. § 1801(i)(2005). (U)

<sup>262</sup> Prior to the enactment of Section 215, the FISA statute's "business records" provisions were limited to obtaining information about a specific person or entity under investigation. Also, information could be obtained only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. (U)

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

originating and terminating telephone number of each call, and the date, time, and duration of each call. The application stated that telephony meta data did not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. According to the application, the majority of the telephony meta data provided to the NSA was expected to involve communications that were (1) between the United States and abroad, or (2) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED] <sup>263</sup> ~~(TS//SI//NF)~~

The application acknowledged that the [REDACTED] collection would include records of communications of U.S. persons located within the United States who were not the subject of any FBI investigation. However, relying on the precedent established by the PR/TT Order, the application asserted that the collection was needed for the NSA to perform analysis to find known [REDACTED] and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons. The application stated that it was not possible to determine in advance which particular piece of meta data will identify a terrorist. The application stated that obtaining such bulk data increases the NSA's ability, through contact-chaining [REDACTED] to detect and identify members of [REDACTED]. <sup>264</sup> In other words, according to the application, meta data analysis is possible only if the NSA "has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related." <sup>265</sup> ~~(TS//SI//NF)~~

<sup>263</sup> The NSA told us that the actual average amount of telephony meta data collected per day is approximately [REDACTED] call detail records and that the figure has not reached [REDACTED] ~~(TS//SI//NF)~~

<sup>264</sup> [REDACTED]

<sup>265</sup> The FISA Court had stated in its July 2004 PR/TT Order that the FISA statute's "relevance" requirement is a relatively low standard and that in evaluating whether bulk meta data is "relevant" to an investigation into [REDACTED] "deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information." The government cited this precedent in the Section 215 application, stating, "[j]ust as the bulk collection of e-mail meta data was relevant to FBI investigations into [REDACTED] so is the bulk collection of telephony metadata described herein." ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

The application also explained how the meta data would be used. [REDACTED]

[REDACTED] <sup>266</sup> The database could be queried only if the NSA determined that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [REDACTED]

[REDACTED] the Section 215 application, like the PR/TT application and Order, added the following proviso to the query standard: "provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution." ~~(TS//SI//NF)~~

According to the application, the NSA estimated that only a tiny fraction (1 in 4 million, or 0.000025 percent) of the call detail records included in the database were expected to be analyzed. The results of any such analysis would be provided, or "tipped," to the FBI or other federal agencies (as was being done under Stellar Wind). [REDACTED]

[REDACTED] ~~(TS//SI//NF)~~

The application also proposed restrictions on access to, and the processing and dissemination of, the data collected that were essentially identical to those included in the PR/TT Order. These included the requirement that queries be approved by one of seven NSA officials or managers and that the NSA's Office of the General Counsel would review and approve proposed queries of telephone numbers reasonably believed to be used by U.S. persons.<sup>267</sup> ~~(TS//SI//NF)~~

266 [REDACTED]

<sup>267</sup> The application included several other measures to provide oversight of the use of meta data, such as controls on the dissemination of any U.S. person information, the creation of a capability to audit NSA analysts with access to the meta data, the destruction of collected meta data after a period of 5 years (the destruction period for e-mail meta data was 4½ years), and a review by the NSA's Inspector General and General Counsel conducted within 45 days of implementing the FISA Court order that assessed the

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

On May 24, 2006, the FISA Court approved the Section 215 application. The Court's Order stated that there were reasonable grounds to believe that the telephony meta data records sought were relevant to authorized investigations being conducted by the FBI to protect against international terrorism. The Order incorporated each of the procedures proposed in the government's application relating to access to and use of the meta data. These procedures included a requirement that any application to renew or reinstate the authority for the bulk collection contain a report describing (1) the queries made since the Order was granted; (2) the manner in which the procedures relating to access and use of the meta data were applied; and (3) any proposed changes in the way in which the call detail records would be received from the communications carriers. The Order also requires the Justice Department to review, at least every 90 days, a sample of the NSA's justifications for querying the call detail records. ~~(TS//SI//NF)~~

Through March 2009, the FISA Court renewed the authorities granted in the May 24 Order at approximately 90-day intervals, with some modifications sought by the government. For example, the Court granted a motion filed on August 8, 2006, requesting [REDACTED]

268

[REDACTED] Except for these and other minor modifications, the terms of the FISA Court's grant of Section 215 authority for the bulk collection of telephony meta data remained essentially unchanged since first approved on May 24, 2006, through March 2009.

[REDACTED] Further, the FISA Court's Section 215 Orders did not require the NSA to modify its use of the telephony meta data from an analytical perspective. However, as discussed below, the FISA Court drastically changed the authority contained in its March 2009 Section 215 Order following the government's disclosure of incidents involving the NSA's failure to comply with the terms of the Court's prior orders.

~~(TS//STLW//SI//OC/NF)~~

---

adequacy of the management controls for the processing and dissemination of U.S. person information. ~~(TS//SI//NF)~~

<sup>268</sup> As noted above, the Court granted an identical motion at the same time in connection with the bulk collection of e-mail meta data. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~**C. Non-Compliance with Section 215 Orders ~~(TS//SI//NF)~~**

On January 9, 2009, representatives from the Department's National Security Division attended a briefing at the NSA concerning the telephony meta data collection. During the course of this briefing, and as confirmed by the NSA in the days that followed, the Department came to understand that the NSA was querying the telephony meta data in a manner that was not authorized by the FISA Court's Section 215 Orders. Specifically, the NSA was on a daily basis automatically querying the meta data with thousands of telephone identifiers from an "alert list" that had not been determined to satisfy the reasonable articulable suspicion (RAS) standard the Court required be met before the NSA was authorized to "access the archived data" for search or analysis purposes.<sup>269</sup> ~~(TS//SI//NF)~~

The alert list contained telephone identifiers that were of interest to NSA counterterrorism analysts responsible for tracking the targets of the Section 215 Orders [REDACTED]

[REDACTED] The list was used to compare the incoming telephony meta data obtained under FISA authority, [REDACTED]

[REDACTED] Under the procedures the NSA had developed to implement the Section 215 authority, alerts (or matches) generated from RAS-approved identifiers could be used to automatically conduct contact chaining [REDACTED] of the telephony meta data. However, automated analysis for alerts generated by non-RAS approved identifiers were not permitted; instead, the alerts were sent to analysts to determine whether chaining [REDACTED] was warranted in accordance with the RAS standard. ~~(TS//SI//NF)~~

On January 15, 2009, the Justice Department notified the FISA Court that the NSA had been accessing the telephony meta data with non-RAS approved identifiers. [REDACTED]

<sup>270</sup> On January 28, 2009, the [REDACTED]

<sup>269</sup> The term "telephone identifier" used by the government means a telephone number as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing or routing communications. ~~(TS//SI//NF)~~

<sup>270</sup> Following the Department's notice to the Court, the NSA attempted to complete a software fix to the alert process so that "hits" against the telephony meta data generated by non-RAS-approved telephone identifiers were deleted and that only "hits" generated by RAS-approved identifiers were sent to NSA analysts for further analysis. The NSA also attempted to construct a new alert list consisting of only RAS-approved telephone identifiers. However, the implementation of these modifications was unsuccessful and on January 24, 2009, the NSA shut down the alert process completely. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

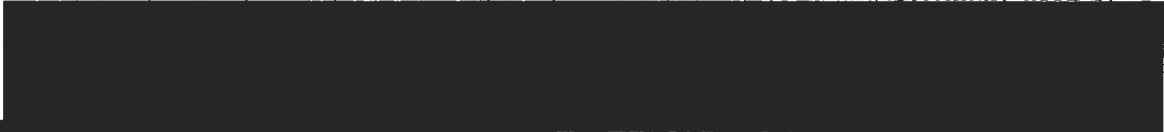
~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Court issued an order stating that it was "exceptionally concerned about what appears to be a flagrant violation of its Order in this matter[.]" The Court required the government to file a brief to "help the Court assess whether the Orders in this docket should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violation of its Orders, either through its contempt powers or by referral to appropriate investigative offices." The Court also required the government to address several additional specific issues, including who knew that the alert list being used to query the meta data included identifiers that had not been determined to meet the reasonable and articulable suspicion standard, how long the "unauthorized querying" had been conducted, and why none of the entities the Court directed to conduct reviews of the meta data collection program identified the problem earlier.<sup>271</sup>  
~~(TS//SI//NF)~~

On February 17, 2009, the government responded to the Court's Order and acknowledged that the NSA's previous descriptions to the Court of the alert list process were inaccurate and that the Section 215 Order did not authorize the government to use the alert list in the manner that it did. The government described for the Court in detail how the NSA developed procedures in May 2006 to implement the Section 215 authority that resulted in the NSA querying the telephony meta data with non-RAS approved telephone identifiers for over 2 years in violation of the Court's Orders, and how those procedures came to be described incorrectly to the Court. According to the government, the situation resulted from the NSA's interpretation of the term "archived data" used in the Court's Orders and the NSA's mistaken belief that the alert process under the Section 215 authority operated the same as the alert process under the Pen Register/Trap and Trace authority.<sup>272</sup> The government told the Court that "there was never a complete understanding among key personnel" who reviewed the initial report to the Court describing the alert process about

<sup>271</sup> The entities directed to conduct such reviews under the Section 215 Orders were the NSA's Inspector General, General Counsel, and Signals Intelligence Directorate Oversight and Compliance Office. (U//~~FOUO~~)

<sup>272</sup> The NSA understood the term "archived data" in the Court's Order to refer to the NSA's analytical repository for the telephony meta data. As the term is normally used by

 The NSA believed that the requirement to satisfy the RAS standard was only triggered when the NSA sought access to the stored, or "archived," repository of telephony meta data. For this reason, in the NSA's view, it was not required to limit the alert list to RAS-approved identifiers. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

what certain terminology was intended to mean, and that "there was no single person who had complete technical understanding of the BR FISA system architecture." ~~(TS//SI//NF)~~

The government argued that the Section 215 Orders should not be rescinded or modified "in light of the significant steps that the Government has already taken to remedy the alert list compliance incident and its effects, the significant oversight modifications the Government is in the process of implementing, and the value of the telephony metadata collection to the Government's national security mission[.]"<sup>273</sup> Among the several measures the government highlighted to the Court was the NSA Director's decision to order "end-to-end system engineering and process reviews (technical and operational) of NSA's handling of [telephony] metadata." Less than two weeks after the government filed the response summarized above, the government informed the Court that the NSA had identified additional compliance incidents during these reviews.<sup>274</sup> ~~(TS//SI//NF)~~

In Orders dated March 2 and 5, 2009, the FISA Court addressed the compliance incidents reported by the government and imposed drastic changes to the Section 215 authorities previously granted. The Court first addressed the NSA's interpretation of the term "archived data." The Court said the interpretation "strains credulity" and observed that an interpretation that turns on whether the meta data being accessed has been "archived" in a particular database at the time of the access would "render compliance with the RAS requirement merely optional." ~~(TS//SI//NF)~~

273

The NSA also determined that in all instances that a U.S. telephone identifier was used to query the meta data for a report, the identifier was either already the subject of a FISA Court order or had been reviewed by the NSA's Office of General Counsel to ensure the RAS determination was not based solely on a U.S. person's First Amendment-protected activities. ~~(TS//SI//NF)~~

<sup>274</sup> The additional compliance incidents involved the NSA's handling of the telephony meta data in an unauthorized manner. The first incident involved the NSA's use of an analytical tool to query (usually automatically) the meta data with non-RAS approved telephone identifiers. The tool determined if a record of a telephone identifier was present in NSA databases and, if so, provided analysts with information about the calling activity associated with that identifier. The second incident involved three analysts who conducted chaining analyses in the telephony meta data using 14 non-RAS approved identifiers. According to the government's notice to the Court, the analysts conducted queries of non-FISA authorized telephony meta data and were unaware their queries also ran against the FISA-authorized meta data. The government stated that none of the queries used an identifier associated with a U.S. person or telephone identifier and none of the queries resulted in intelligence reporting. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

The Court next addressed the misrepresentations the government made to the Court from August 2006 to December 2008 in reports that inaccurately described the alert list process. The Court recounted the specific misrepresentations and summarized the government's explanation for their occurrence. The Court then concluded,

Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect [REDACTED] call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigations and whose call detail information could not otherwise have been legally captured in bulk. ~~(TS//SI//NF)~~

The Court also addressed the additional non-compliance incidents that were identified during the initial review ordered by the NSA Director, observing that the incidents occurred despite the NSA implementing measures specifically intended to prevent their occurrence. In view of the record of compliance incidents the government had reported to date, the Court stated,

[I]t has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively. ~~(TS//SI//NF)~~

Despite the Court's concerns with the telephony meta data program, and its lack of confidence "that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders," it authorized the government to continue collecting telephony meta data under the Section 215 Orders. The Court explained that in light of the

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

government's repeated representations that the collection of the telephony meta data is vital to national security, taken together with the Court's prior determination that the collection properly administered conforms with the FISA statute, "it would not be prudent" to order the government to cease the bulk collection. ~~(TS//SI//NF)~~

However, believing that "more is needed to protect the privacy of U.S. person information acquired and retained" pursuant to the Section 215 Orders, the Court prohibited the government from accessing the meta data collected "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."<sup>275</sup> The government may, on a case-by-case basis, request authority from the Court to query the meta data to obtain foreign intelligence.<sup>276</sup> Such a request must specify the telephone identifier to be used and the factual basis for the NSA's RAS determination. ~~(TS//SI//NF)~~

The Court ordered that upon completion of the NSA's end-to-end system engineering and process reviews, the government file a report that describes the results of reviews, discusses the steps taken to remedy non-compliance incidents, and proposes minimization and oversight procedures to employ should the Court authorize resumption of regular access to the telephony meta data. The government's report also must include an affidavit from the FBI Director and any other government national security official deemed appropriate describing the value of the telephony meta data to U.S. national security. ~~(TS//SI//NF)~~

Additionally, the Court ordered the government to implement oversight mechanisms proposed in the government's response to the compliance incidents. These mechanisms generally require the Justice Department's National Security Division to assume a more prominent role in the NSA's administration of the bulk collection program. For example, the NSA's Office of General Counsel must now consult with the National

---

<sup>275</sup> The Court also stated, "Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons[.]" ~~(TS//SI//NF)~~

<sup>276</sup> The Court authorized the government to query the meta data without Court approval to protect against an imminent threat to human life, with notice to the Court within the next business day of the query being conducted. The Court also authorized the government to access the meta data to ensure "data integrity" and to develop and test technological measures designed to enable to the NSA to comply with previously approved procedures for accessing the meta data. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Security Division on all significant legal opinions that relate to the interpretation, scope, or implementation of past, current, and future Section 215 Orders related to the telephony bulk meta data collection.

~~(TS//SI//NF)~~

On May 29, 2009, the Court authorized the government to continue collecting telephony meta data under the Section 215 Orders for 43 days subject to the same limitations set out in its orders of March 2 and 5, 2009.

~~(TS//SI//NF)~~

### **III. Content Collection under FISA ~~(TS//SI//NF)~~**

The third and last part of the Stellar Wind program brought under FISA authority was content collection (basket 1). The effort to accomplish this transition was legally and operationally complex, and our discussion in this section does not address each statutory element or the full chronology of the government's applications and related FISA Court orders. Rather, we describe the circumstances surrounding the government's decision to transition content collection from presidential to FISA authority.

[REDACTED] We also summarize the FISA Court's response to the government's content collection proposals and the orders it issued. In this section, we describe one FISA Court judge's rejection of the government's legal approach to content collection, a decision that hastened the enactment of legislation that significantly amended the FISA statute and provided the government surveillance authorities broader than those authorized under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

#### **A. Decision to Seek Content Order ~~(TS//SI//NF)~~**

The Department first began work on bringing Stellar Wind's content collection activity (basket 1) under FISA in March 2005, shortly after Alberto Gonzales became Attorney General. Gonzales told us that he initiated discussions about making this change with OLC Principal Deputy Assistant Attorney General Bradbury. Gonzales said that he had questions about how the NSA was conducting the collection in terms of audits and checks being performed, and he wanted to ensure that the agency was running the program properly. Gonzales told us that placing content collection under FISA authority would also eliminate the constitutional debate about the activity and would reassure people that the President was acting according to the Constitution and the law. Gonzales said that, in his view, it is better to conduct activities such as content collection without a direct order from the President when possible. Gonzales added that in 2001 nobody thought it was possible to bring Stellar Wind under FISA authority.

~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

When Gonzales became Attorney General in early 2005, however, he also knew there had been a leak to The New York Times about the NSA's content collection activity under Stellar Wind and that the paper was actively investigating the story. In November 2004, Gonzales (then the White House Counsel), together with Deputy Attorney General Comey and his Chief of Staff, had met with New York Times reporters to discuss the potential article.<sup>277</sup> ~~(TS//STLW//SI//OC/NF)~~

In response to Gonzales's request, Bradbury, working with attorneys in OLC and the Office of Intelligence and Policy Review (OIPR) as well as with NSA personnel, devised a legal theory, summarized below, for bringing under FISA the Stellar Wind program's content collection activities while preserving the "speed and agility" many Intelligence Community officials cited as the chief advantage of the NSA program. In June 2005, Bradbury, together with Associate Deputy Attorney General Patrick Philbin, presented the legal theory to White House officials David Addington, Harriet Miers, and Daniel Levin and received their approval to continue work on a draft FISA application.<sup>278</sup> ~~(TS//STLW//SI//OC/NF)~~

Bradbury told the OIG that he also spoke to the Director of National Intelligence and to NSA officials about bringing Stellar Wind's content collection under FISA. According to Bradbury, the Director of National Intelligence responded positively to the proposal, but the NSA was skeptical as to whether a FISA approach would be feasible, in view of the substantial administrative requirements under the FISA Court's PR/TT Order. The NSA also believed that the FISA Court would be reluctant to grant the NSA the operational flexibility it would insist on in any content application, resulting in less surveillance coverage of telephone numbers and e-mail addresses used by persons outside the United States. ~~(TS//STLW//SI//OC/NF)~~

As discussed in detail in Chapter Eight of this report, in December 2005 The New York Times published its series of articles on the content collection portion of the Stellar Wind program, resulting in considerable controversy and public criticism of the NSA program. Through the spring of 2006, the Department continued work on the content application. In May 2006, at the first of the FISA Court's semiannual meetings that year, the Department provided the Court a draft of the application for content collection to obtain feedback on the government's unconventional approach to the FISA statute. None of FISA Court judges indicated whether the

---

<sup>277</sup> The New York Times held the article until December 2005, when it published a series of articles on the content collection portion of Stellar Wind. ~~(TS//SI//NF)~~

<sup>278</sup> After serving as Acting Assistant Attorney General for OLC from June 2004 to February 2005, Levin joined the National Security Council, where he remained until approximately November 2005. (U)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

application would be granted if filed, but some identified concerns with certain aspects of the proposal. (TS//STLW//SI//OC/NF)—

At this time, Congress and the Administration were also discussing how to modernize the FISA statute to authorize the type of electronic surveillance that the content application sought. Work on the application was temporarily suspended as the Department focused its attention on working with Congress to craft this legislation. However, this suspension of work on the content application was brief. Bradbury said he concluded by the fall of 2006, as Congress was heading for recess, that there would be no legislative reform of the FISA statute in the foreseeable future that would address content collection as it was being conducted under Stellar Wind. As a result, the Department pressed forward with the draft content application to the FISA Court. (TS//STLW//SI//OC/NF)—

**B. Summary of Department's December 13, 2006, Content Application (TS//SI//NF)—**

In November 2006, at the second of the Court's semiannual meetings, the Department presented an updated draft of the application that incorporated feedback received from members of the Court during the previous semiannual meeting. On December 13, 2006, the Department formally filed the content application with the Court. (TS//SI//NF)—

The government's December 13 application sought authority to intercept the content of telephonic and electronic communications of [REDACTED]

[REDACTED] 279 The application stated:

Speed and flexibility are essential in tracking individuals who

[REDACTED] To follow the trails effectively, and to respond to new leads, it is vital for the U.S. Intelligence Community to be able quickly and efficiently to acquire communications to or from individuals reasonably believed to

<sup>279</sup> The content application included the following caveat:

By filing this application, the United States does not in any way suggest that the President lacks constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization.

(TS//SI//NF)—

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

be members or agents of these [REDACTED] foreign powers.

~~(TS//SI//NF)~~

According to the application, the goal was to establish "an early warning system" under FISA to alert the government to the presence of members and agents of foreign powers [REDACTED]

[REDACTED] and to assist tracking such individuals within the United States. The "early warning system" sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular phone number or e-mail address, referred to by the NSA as a "selector," was being used or about to be used by members or agents of a foreign power.

~~(TS//SI//NF)~~

In the place of this individualized process, the application proposed that the FISA Court establish broad parameters for the interception of communications – specifically, [REDACTED] that can be targeted and the locations where the surveillance can be conducted – and that NSA officials, rather than FISA Court judges, determine within these parameters the particular selectors whose communications the NSA would intercept. [REDACTED]

[REDACTED] albeit with FISA Court review and supervision.<sup>280</sup> ~~(TS//SI//NF)~~

The legal arguments underlying the government's approach are complex and involve substantial communications terminology. They also require lengthy discussion of the FISA statute and previous FISA Court decisions. Rather than describe at length these issues, in this section we detail the two main components of the government's approach to content collection in the FISA application that are critical for understanding one judge's approval of the application and another judge's later rejection of essentially the same application. ~~(TS//SI//NF)~~

First, the government proposed an interpretation of the term "facility" in the FISA statute that was broader than how the term was ordinarily, but

---

<sup>280</sup> The Department's application provided an example to illustrate the risks associated with the existing requirement that FISA Court approval or Attorney General emergency authorization be obtained each time the government seeks to target a particular telephone number or e-mail address: [REDACTED]

[REDACTED] According to the application, valuable intelligence could be lost in the time it would take to receive FISA Court authorization or Attorney General emergency authorization to target the new address. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

not always, applied.<sup>281</sup> Section 1805(a)(3)(B) of FISA provides that the Court may order electronic surveillance only upon finding that there is probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by" a group involved in international terrorism. The term "facilities" generally was interpreted to refer to individual telephone numbers or e-mail addresses at which surveillance is "directed." ~~(TS//SI//NF)~~

The government proposed in its content application that the term "facilities" be interpreted broadly to include [REDACTED]

<sup>282</sup> Under this approach, instead of examining the target's use of particular telephone numbers or e-mail addresses, the Court would determine only whether there was probable cause to believe that the target was using [REDACTED] to communicate telephonically or by e-mail.<sup>283</sup> ~~(TS//STLW//SI//OC/NF)~~

Second, the government's application requested that senior NSA officials be authorized to make individualized findings of probable cause about whether a particular telephone number or e-mail address was being used by a member or agent of one of the application's targets. Ordinarily, a FISA Court judge makes this probable cause determination. ~~(TS//SI//NF)~~

To implement this transfer of authority, the government proposed that NSA officials make the probable cause determinations as part of requirements called "minimization procedures," which are detailed rules

---

<sup>281</sup> The government's Memorandum of Law filed in support of the content application described several instances where the FISA Court authorized surveillance of facilities that was not limited to particular telephone numbers and e-mail addresses. According to the application, [REDACTED]

The government's proposed interpretation of the term in the content application was far broader than previously authorized by the Court. ~~(TS//SI//NF)~~

<sup>282</sup> [REDACTED]

<sup>283</sup> As noted, the targets of the content application were [REDACTED]. The government's content application included a declaration from the NSA Director that addressed [REDACTED] use of the international telephone system and [REDACTED] communications. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

that govern how the government must handle communications that it intercepts pertaining to U.S. persons. The FISA statute provides that each FISA application must include, and the FISA Court must approve, minimization procedures that the agency will follow with respect to communications intercepted pursuant to a FISA Court order. ~~(TS//SI//NF)~~

Minimization procedures, in the FISA context, ordinarily govern the handling of intercepted communications involving U.S. persons after the acquisition has been approved by the FISA Court. In other words, a FISA Court authorizes the agency to intercept the communications of particular selectors, and the agency follows the minimization procedures with respect to how it retains, uses, and disseminates any U.S. person information it collects under the Court's order. ~~(TS//SI//NF)~~

However, the government proposed as part of the content application that the minimization procedures also encompass how the NSA acquires the communications.<sup>284</sup> Specifically, the application proposed that the NSA could intercept the communications of specific selectors if agency officials determined there was probable cause to believe that (1) the selector is being used by a member or agent of a [REDACTED] and (2) the communication is to or from a foreign country. The application referred to this as the "minimization probable cause standard."<sup>285</sup> ~~(TS//SI//NF)~~

Thus, the content application had a two-prong "minimization probable cause standard": (1) probable cause to believe a selector is being used by a member or agent of a targeted group, and (2) probable cause to believe the communication intercepted is to or from a foreign country. [REDACTED]

<sup>284</sup> Bradbury told the OIG that this argument was based on the text of the FISA statute, which states that minimization procedures apply to the "acquisition" of communications in addition to their retention and dissemination. See 50 U.S.C. § 1801(h)(1). Indeed, the government's Memorandum of Law filed in support of the content application described several cases in which the FISA Court authorized the government to conduct electronic surveillance that included minimization at the time of acquisition. According to the application, the cases involved surveillance broadly targeted [REDACTED] than those the government specifically sought to acquire. [REDACTED]

~~(TS//SI//NF)~~

<sup>285</sup> The proposed "minimization probable cause standard" was in addition to the standard minimization procedures that accompany every FISA application submitted by the government and that have been long-approved by the FISA Court. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~~~(TS//STLW//SI//OC/NF)~~

For the first prong – probable cause to believe a selector is being used by a member or agent of a targeted group – NSA analysts would assess sources of “reliable intelligence,” defined in the application as information from a variety of domestic and foreign intelligence and law enforcement activities. Under the terms of the application, positive findings of probable cause would be recorded in a database and the assessment process would be subject to periodic internal review by NSA officials, including the NSA General Counsel and Inspector General. ~~(TS//SI//NF)~~

For the second prong – probable cause to believe the communication intercepted is to or from a foreign country

For example, the application stated that there would be probable cause to believe

<sup>286</sup> With respect to e-mails, the application stated that

<sup>287</sup> ~~(TS//STLW//SI//OC/NF)~~

<sup>286</sup> The application acknowledged that communications intercepted at the “facilities” could include some calls where in the United States, or where in the United States (even where there is probable cause to believe that the United States).

If the NSA had probable cause to believe one of the communicants was a member of the call could be intercepted. The application stated that such communications would be handled in accordance with NSA’s standard minimization procedures that apply to all of the agency’s electronic surveillance activities. ~~(TS//SI//NF)~~

<sup>287</sup> As it did with telephone communications, the application acknowledged that the manner in which e-mail communications are routed would cause the NSA to collect some e-mail communications that in fact are between communicants wholly within the United

(Cont’d.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Thus, viewing the government's approach to both "facilities" and "minimization procedures" together, the December 13, 2006, content application asked the FISA Court to find probable cause to believe that [REDACTED]

[REDACTED] engaged in international terrorism, and that these groups use the international telephone system and the [REDACTED] communications system [REDACTED]

[REDACTED] Then, within these broad parameters authorized by the Court, NSA officials would make probable cause findings about whether individual telephone numbers or e-mail addresses are used by members or agents of [REDACTED]

[REDACTED] and whether the communications of those numbers and addresses are to or from a foreign country. If they were, the NSA could direct the telecommunications carriers to intercept the communications of those telephone numbers and e-mail addresses and provide them to the NSA. [REDACTED]

[REDACTED] (TS//STLW//SI//OC/NF)

Under the terms of the application, communications acquired by the NSA could be retained for 5 years, unless the Court approved retention for a longer period. The application also stated that the NSA expected to initially target [REDACTED] telephone numbers and e-mail addresses used by members or agents or [REDACTED]

[REDACTED] (TS//SI//NF)

An additional aspect of the content application is important to understand. The "early warning system" the government proposed applied both to "domestic selectors" and "foreign selectors." Domestic selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals in the United States; foreign selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals outside the United States. Under Stellar Wind, the NSA intercepted the communications of both categories of selectors, although the NSA tasked far more foreign selectors than domestic selectors. (TS//STLW//SI//OC/NF)

---

States, even though the NSA had probable cause to believe the communication was to or from a foreign country. The application stated that the NSA would handle any such communications in accordance with its standard minimization procedures. (TS//SI//NF)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

The government proposed in its content application that the domestic selectors would be subject to more rigorous targeting approval and more frequent reporting to the FISA Court than foreign selectors, but the application sought to preserve NSA officials' authority to make the probable cause determinations as to each.<sup>288</sup> As we describe below, the first FISA Court judge to consider the content application, Judge Malcolm Howard, was unwilling to extend this authority to domestic selectors. (TS//SI//NF)

**C. Judge Howard Grants Application in Part (TS//SI//NF)**

The Department's December 13, 2006, content application was assigned to Judge Howard, because he was the "duty" judge that week responsible for considering new applications.<sup>289</sup> Judge Howard advised the Department orally that he would not authorize, on the terms proposed in the application, the electronic surveillance of selectors to be used by persons in the United States (domestic selectors). He did not issue a written opinion or order concerning this decision. The Department, in response to Judge Howard's oral advisement, filed a separate application requesting authority to conduct electronic surveillance on domestic selectors. This application, summarized below, was filed on January 9, 2007, and is considered the first "domestic selectors application"; the December 13 application is considered the first "foreign selectors application."  
(TS//SI//NF)

Judge Howard also requested additional briefing from the Justice Department on the subject of whether [REDACTED] constituted "facilities" under FISA, and whether the surveillance authority sought in the government's content application would in fact be "directed" not at these "facilities" but rather at the particular telephone numbers and e-mail addresses the government would task for collection. (TS//SI//NF)

In response, the Department filed a supplemental memorandum of law on January 2, 2007, arguing that the government's construction of the

---

<sup>288</sup> Under the terms of the original content application, domestic selectors tasked by the government would subsequently be reported to the Court for approval. The Court either had to approve each domestic selector within 48 hours of receiving the government's report or, if the Court did not agree there was probable cause to believe the selector was being used by a member or agent of a target of the application, provide the government 24 hours to submit additional information establishing probable cause. Foreign selectors tasked by the government did not require subsequent approval by the Court, although the Court could direct that the surveillance of any selector cease. (TS//SI//NF)

<sup>289</sup> The Department offered to submit the application to the FISA Presiding Judge, Judge Kollar-Kotelly, but she said that it should be filed in the normal fashion, which meant it would be assigned to the FISA duty judge that week. (TS//SI//NF)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

On January 10, 2007, Judge Howard approved the Department's content application as to foreign selectors, endorsing the legal framework on which the content application for foreign selectors was based, including the broad construction of the term "facility" and the use of minimization procedures to empower NSA officials to make targeting decisions about particular selectors. Judge Howard's Order authorized the government to conduct electronic surveillance for a period of 90 days at the "facilities" identified in the application, and was set to expire on April 6, 2007. The Order [REDACTED]

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

the Court found that the first prong of the standard has not been satisfied. In addition, the Order required the NSA Inspector General, General Counsel, and Signals Intelligence Directorate to periodically review the authorized collection activities. These NSA offices were required to submit a report to the Court 60 days after the collection was initiated under the Order that would address the adequacy of management controls and whether U.S. person information was being handled properly. ~~(TS//SI//NF)~~

According to several Department and NSA officials, the effort to implement Judge Howard's January 10, 2007, Order was a massive undertaking. [REDACTED]

[REDACTED] ~~(TS//STLW//SI//OC/NF)~~

As a result of the Order, the Department and NSA submitted to the FISA Court for its review the factual basis for each selector supporting the government's determination that the "minimization probable cause standard" had been satisfied. The Department accomplished this pursuant to a schedule approved by Judge Howard under which the Department filed [REDACTED] foreign selectors every [REDACTED] days for the duration of the 90-day Order. ~~(TS//SI//NF)~~

The probable cause explanation for each foreign selector filed with the Court typically was described in several sentences. According to Bradbury, he impressed upon the NSA that Judge Howard would review each submission and inquire about how recently the NSA had acquired communications relating to a particular selector. According to Matthew Olsen, the Deputy Assistant Attorney General in the Department's National Security Division who was responsible for overseeing intelligence matters, Judge Howard did in some cases inquire about the government's factual basis for believing the minimization probable cause standard has been met.<sup>293</sup> Bradbury also said he stressed that the Court would scrutinize the NSA's probable cause determinations more rigorously than the agency had been doing itself and that the Court was more likely to approve a selector where the surveillance was current than it would a selector that has "remained dormant for months."<sup>294</sup> ~~(TS//SI//NF)~~

<sup>293</sup> Olsen was involved in the drafting and presentation to the FISA Court of the content application and the government's implementation of the related FISA Court Orders. ~~(TS//SI//NF)~~

<sup>294</sup> However, Bradbury noted that the FISA Court's "tendency to look for recent information" in assessing whether the probable cause standard has been met is "problematic" because [REDACTED]

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Olsen told us that [REDACTED] foreign selectors ultimately were filed with the FISA Court under the terms of Judge Howard's Order. Olsen said that the NSA strived to submit selectors that were deemed high priority, that had a well-documented nexus to [REDACTED] foreign powers, and that had recent communications activity. Attorneys from OIPR, who under the terms of the Order were required to review the NSA's justification for each foreign selector that it tasked, worked with the NSA on this large-scale review process. According to Olsen, OIPR attorneys "double-checked" the NSA's probable cause determination for each selector, but did not conduct independent probable cause inquiries. This review identified [REDACTED] selectors that in OIPR's judgment required additional documentation before they could be submitted to the Court.<sup>295</sup> Olsen described the back-and-forth between OIPR and the NSA as "constant," and said the NSA was receptive to OIPR's involvement. Olsen stated that the NSA committed significant resources to the transition of foreign selectors. ~~(TS//SI//NF)~~

Both Bradbury and Olsen observed that the transition of content collection of foreign selectors to FISA required some adjustment by the NSA in its approach to establishing probable cause. For example, while an NSA analyst might base a probable cause determination to some extent on intuition, similar to a "cop on the beat," it was a different proposition when that probable cause determination had to be reviewed by several OIPR attorneys trying to anticipate how the FISA Court might view the judgment. Olsen stated that it was also "new" for the NSA to document the probable cause to the level OIPR believed the FISA Court would require. According to Bradbury, the effort sought an equilibrium between "the necessary speed and agility" and the "multiple layers of probable cause determination." Bradbury and Olsen both told the OIG that the NSA had concerns about whether the FISA approach to content collection would work and the extent to which a measure of effectiveness would be lost under FISA Court supervision. ~~(TS//SI//NF)~~

#### **D. Domestic Selectors Application and Order** ~~(TS//SI//NF)~~

In contrast to foreign selectors, Judge Howard advised the Justice Department that requests for surveillance of the international calls of domestic selectors – telephone numbers or e-mail addresses reasonably believed to be used by individuals in the United States – should be filed with

[REDACTED]  
~~(TS//SI//NF)~~

<sup>295</sup> Olsen told the OIG that he believes the NSA de-tasked some of these foreign selectors. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

the Court in a separate application. Judge Howard also advised OIPR officials that any such application should take a more traditional approach to FISA, meaning the "facilities" targeted by the application should be particular telephone numbers and e-mail addresses and that the probable cause determination for tasking a selector would reside with the FISA Court, not with NSA officials pursuant to minimization procedures. (TS//SI//NF)

On January 9, 2007, the Department filed the first domestic selectors application. The application sought two things. First, the application requested authority to intercept the international communications of [REDACTED] specific domestic selectors.<sup>296</sup> Second, the application sought, for purposes of future applications, approval to use a "streamlined version" of the emergency authorization procedures available under FISA. These emergency procedures authorize the use of electronic surveillance for a period of up to 72 hours without a Court order when the Attorney General reasonably determined that an emergency situation exists. See 50 U.S.C. § 1805(f). The procedures required the Attorney General to inform the FISA Court that the surveillance has been initiated and required the Department to file with the Court an emergency application to continue the surveillance not more than 72 hours after the surveillance was authorized. (TS//SI//NF)

The goal of the Department's proposed streamlined emergency application procedures, referred to in the January 9, 2007, application as a "Verified Application," was to ensure that the emergency surveillance process be completed as swiftly as possible for qualifying domestic selectors. The proposal allowed the Verified Application to incorporate by reference the reasons or facts contained in the original domestic selectors application necessary to satisfy some of the statutory requirements under FISA, instead of reestablishing in each application for a new domestic selector that each of the requirements of FISA were met. The only new substantive information contained in a Verified Application would be the identity of the target, if known, the telephone number the target was using or was about to use, and the factual basis supporting probable cause to believe the target is [REDACTED] and is using or is about to use the identified telephone number. (TS//SI//NF)

Judge Howard granted the domestic selectors application on January 10, 2007, for a period of 90 days. His Order also approved the

<sup>296</sup> Unlike the December 13, 2006, application, the January 9, 2007, application did not seek authority to target agents of [REDACTED] nor did the application seek authority to conduct content surveillance of e-mail communications. The declaration summarized for each of the domestic selectors, generally in two to three paragraphs, the facts that supported the government's belief that the telephone number was used or about to be used by a known or unknown agent of [REDACTED] located in the United States. (TS//SI//NF)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

streamlined emergency authorization procedures proposed in the application for any additional domestic selectors whose communications the government sought to intercept during the 90-day period for which surveillance was authorized.<sup>297</sup> ~~(TS//SI//NF)~~

NSD Deputy Assistant Attorney General Olsen told the OIG that in comparison with foreign selectors, the Department conducted a more rigorous review of the initial domestic selectors submitted to the FISA Court to ensure that probable cause was met. Olsen said a few domestic selector packages "on [their] face" lacked sufficient documentation and that these deficiencies were apparent to OIPR attorneys reviewing the information because the attorneys were looking at the information for the first time. He said that the NSA analysts responsible for the selectors, in contrast, were very familiar with the numbers and knowledgeable of details about the users that might not have been evident to persons reviewing documentation *de novo*. According to Olsen, for selector packages that were considered deficient, the NSA either provided the Justice Department attorneys with additional information or de-tasked the selector.<sup>298</sup> ~~(TS//SI//NF)~~

**E. Last Stellar Wind Presidential Authorization Expires**  
~~(TS//SI//NF)~~

On December 8, 2006, the President signed what would become the final Presidential Authorization for the Stellar Wind program. The December 8 Authorization was scheduled to expire on February 1, 2007. However, Judge Howard's January 10, 2007, Orders relating to foreign and domestic selectors completed the transition of Stellar Wind's

---

<sup>297</sup> On January 22, 2007, the Department filed, and Judge Howard approved, the first Verified Application with the FISA Court using the streamlined procedures approved in the Order. ~~(TS//SI//NF)~~

<sup>298</sup> Olsen and OIPR Deputy Counsel Margaret Skelly-Nolen told the OIG that during the application for and implementation of the domestic selectors Order, it became apparent that there were coordination problems between the FBI and the NSA. They noted that in many instances a domestic selector the NSA sought to task was already targeted by an FBI FISA order. According to Skelly-Nolen, in those cases problems can arise in providing accurate, current, and consistent information to the FISA Court about such selectors. She said the NSA's practice has been to consult with the FBI analysts assigned to the NSA and to request from them the most current information the FBI has about a particular telephone number or user of that number. The FBI analysts at the NSA have access to FBI databases to search for such information, although the most current information frequently can only be obtained from the operational personnel at FBI Headquarters. As a consequence, according to Skelly-Nolen, the FISA Court has on some limited occasions been provided inconsistent information concerning domestic telephone numbers or the users of those numbers. Olsen told the OIG that the domestic selectors Order has required a higher level of coordination between the FBI and NSA and that the National Security Division has worked to address this issue. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

communications and meta data collection activities from Presidential Authorization to FISA authority. Bradbury told the OIG that because it was believed that Judge Howard's Orders, particularly the foreign selectors Order, provided the NSA sufficient flexibility to conduct content collection, it was not necessary to renew the December 8, 2006, Presidential Authorization. ~~(TS//STLW//SI//OC/NF)~~

Therefore, on February 1, 2007, the Presidential Authorization for the Stellar Wind program officially expired.<sup>299</sup> ~~(TS//SI//NF)~~

**F. First Domestic and Foreign Selectors FISA Renewal Applications** ~~(TS//SI//NF)~~

Judge Howard's January 10, 2007, Orders were set to expire after 90 days. During the week of March 20, 2007, the government filed renewal applications to extend the authorities both as to domestic and foreign selectors. These applications were filed with Judge Roger Vinson, the FISA Court duty judge that week. ~~(TS//SI//NF)~~

The domestic selectors application, filed March 22, 2007, was in all material respects identical to the government's original application. Judge Vinson granted the application on April 5, 2007.<sup>300</sup> ~~(TS//SI//NF)~~

The foreign selectors application was filed on March 20, 2007. The content and construction of the March 20 application was substantially identical to the government's original application, and advanced the same broad construction of the term "facilities" and the use of minimization procedures to authorize NSA officials, instead of judges, to make probable cause determinations (subsequently reviewed by the FISA Court) about particular selectors. ~~(TS//SI//NF)~~

On March 29, 2007, Judge Vinson orally advised the Department that he could not grant the foreign selectors application. His decision validated some concerns within the Justice Department that Judge Howard's original

<sup>299</sup> On January 17, 2007, Attorney General Gonzales sent a letter to Senators Leahy and Specter, the Chairman and Ranking Member of the Senate Judiciary Committee, informing them of Judge Howard's Orders. Gonzales's letter stated that as a result of the January 10, 2007, FISA Court Orders, any electronic surveillance that was occurring under the Terrorist Surveillance Program would now be conducted under FISA, and that "the President determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires." ~~(TS//SI//NF)~~

<sup>300</sup> As noted previously, the domestic selectors Order presented special coordination issues between the FBI and the NSA, and [REDACTED]. The Order was renewed for the final time in [REDACTED] and has since expired. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Order might not be a sustainable long-term strategy for intercepting the communications of foreign selectors. Judge Vinson's decision also accelerated the Department's efforts to obtain legislation amending the FISA statute to authorize the type of surveillance conducted under Stellar Wind and that was approved by Judge Howard. ~~(TS//SI//NF)~~

On April 3, 2007, Judge Vinson issued an Order and Memorandum Opinion explaining the reasoning for his conclusion that he could not grant the foreign selectors application. However, Judge Vinson did not deny the government's application. Instead, he encouraged the Department to file a motion with Judge Howard requesting a 60-day extension of the existing January 10, 2007, foreign selectors Order. In explaining why he was encouraging the Department to file the motion with Judge Howard, Judge Vinson wrote,

I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA's surveillance program, which had been conducted under the President's assertion of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in [the January 10, 2007, foreign selectors Order], on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of [REDACTED] phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion. ~~(TS//SI//NF)~~

Judge Vinson wrote that the Department's foreign selectors renewal application concerns an "extremely important issue" regarding who may make probable cause findings that determine the individuals and the communications that can be subjected to electronic surveillance under FISA. In Judge Vinson's view, the question was whether probable cause determinations are required to be made by the FISA Court through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Judge Vinson concluded, based on past practice under FISA and the congressional intent underlying the statute, that probable cause determinations must be made by the FISA Court. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

In explaining his reasoning, Judge Vinson first rejected the Department's broad construction of the term "facilities," concluding that the "electronic surveillance" under the government's application – the acquisition of the content of communications – was directed at particular telephone numbers and e-mail addresses, and not at broad swaths of communications [REDACTED]

[REDACTED], as the government contended. Judge Vinson distinguished prior cases that the government cited for its broad interpretation of "facilities," observing, "[t]ellingly, none of the cited cases stand for the proposition on which this application rests – that electronic surveillance is not 'directed' at particular phone numbers and e-mail addresses, [REDACTED]

[REDACTED].” (TS//SI//NF) —

Judge Vinson wrote that his conclusion was also supported by the government's and the Court's past practice, as well as the legislative history of FISA, which, according to Judge Vinson, made clear that "Congress intended the pre-surveillance 'judicial warrant procedure,' and particularly the judge's probable cause findings, to provide an 'external check' on executive branch decisions to conduct surveillance." He wrote that the government's proposal that "the Court assess [REDACTED] and make a highly abstract and generalized probable cause finding [REDACTED]" removed from the Court's pre-surveillance purview the question of whether the communications to be acquired will relate to the targeted foreign powers.<sup>301</sup>

(TS//SI//NF) —

Judge Vinson rejected the government's "minimization probable cause standard," stating that "[m]inimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA." Judge Vinson concluded that government's proposed minimization procedures, by authorizing the NSA to make probable cause decisions, conflicted with specific provisions of FISA that govern electronic surveillance, such the requirement that only the Attorney General can grant emergency approvals to conduct surveillance (followed within 72 hours by an application to the

<sup>301</sup> Stated another way, "[the application] represented that NSA will make the required probable cause finding for each such facility before commencing surveillance." Judge Vinson wrote, "[t]he application seeks, in effect, to delegate to the NSA the Court's responsibility to make such findings 'based on the totality of circumstances.' Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order (emphasis in original)."

(TS//SI//NF) —

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

FISA Court), and that renewals for surveillance coverage must be based on "new findings" of probable cause by a judge. Judge Vinson summarized his position:

The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute. ~~(TS//SI//NF)~~

Judge Vinson wrote that he was mindful of the government's argument that the proposed minimization procedures were necessary to provide or enhance the "speed and flexibility" with which the NSA responds to threats, and that foreign intelligence information may be lost in the time it takes to obtain Attorney General emergency authorizations. However, in Judge Vinson's view, FISA's requirements reflected a balance struck by Congress between privacy interests and the need to obtain foreign intelligence information, and until Congress took legislative action on FISA to respond to the government's concerns, the Court must apply the statute's procedures.<sup>302</sup> He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and e-mail addresses. Vinson rejected this position, stating, "provided that the surveillance is within FISA at all, the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States."<sup>303</sup> ~~(TS//SI//NF)~~

---

<sup>302</sup> Judge Vinson stated that he recognized that the government maintained the President may have constitutional or statutory authority to conduct the surveillance requested in the renewal application. Judge Vinson stated, "[n]othing in this order and opinion is intended to address the existence or scope of such authority, or this Court's jurisdiction over such matters." ~~(TS//SI//NF)~~

<sup>303</sup> Judge Vinson wrote in a footnote that the status of the proposed surveillance as being within the scope of FISA was "assumed, but not decided, for purposes of this order and opinion." He continued, "I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States." Judge Vinson suggested that "Congress should also consider clarifying or modifying the scope of FISA and of this Court's jurisdiction with regard to such facilities . . . ." Bradbury told the OIG that Judge Vinson's suggestion was an important spur to Congress's willingness to consider FISA modernization legislation in

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

Attorney General Gonzales told us that his reaction to Judge Vinson's decision was one of "disappointment" and that the decision "confirmed our concern about going to the [FISA Court]." Gonzales also said he believed the decision was "troubling for purposes of the national security of our country."

~~(TS//STLW//SI//OC/NF)~~

Bradbury told us the government considered several options after Judge Vinson's ruling, including appealing the decision to the FISA Court of Review. However, he said the decision was made to attempt to work with Judge Vinson to craft a revised application and also separately to renew the Administration's efforts to obtain legislation to modernize FISA.

~~(TS//SI//NF)~~

**G. Revised Renewal Application for Foreign Selectors and Order** ~~(TS//SI//NF)~~

As suggested by Judge Vinson, in April 2007 the Justice Department obtained from Judge Howard an extension of the existing foreign selectors Order until May 31, 2007, to prepare a revised foreign selectors application. In the interim, the Department filed two reports with Judge Vinson describing a new approach to foreign selectors that addressed the concerns expressed in his Opinion, and that sought input from the Court about how best to facilitate the submission of an application that would seek authority to direct surveillance at [REDACTED] selectors. ~~(TS//SI//NF)~~

On May 24, 2007, the Department filed a revised renewal application seeking to renew, with modifications, the authorities granted in Judge Howard's January 10, 2007, Order. However, the application did not include the broad construction of "facilities" and instead sought authority to conduct electronic surveillance of conventional facilities – telephone numbers and "e-mail [REDACTED]"<sup>304</sup> The application also did not include the "probable cause minimization standard" approved

the summer of 2007. In Section IV below, we summarize this legislation, the Protect America Act, and its successor, the FISA Amendments Act of 2008. ~~(TS//SI//NF)~~

<sup>304</sup> According to the May 24, 2007, application, such uses include Internet communications that are sent to and from a targeted e-mail "address," [REDACTED]

[REDACTED] The May 24 application was the [REDACTED] to use the term "e-mail [REDACTED]" to describe the facility at which e-mail surveillance would be directed;

However, according to the application, the government "routinely requests, and the Court authorizes, electronic surveillance using [the e-mail [REDACTED]] descriptor to identify this type of facility." ~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

by Judge Howard that had the effect of shifting from the FISA Court to the NSA the probable cause determinations about particular selectors.

~~(TS//SI//NF)~~

However, the targets of the government's revised application remained selectors (telephone number and e-mail facilities) reasonably believed to be used outside the United States and for which there is probable cause to believe were being used, or are about to be used, by [REDACTED]

<sup>305</sup> The application also sought [REDACTED]

[REDACTED] and in the same manner as was approved in Judge Howard's Order.<sup>306</sup> ~~(TS//SI//NF)~~

Specifically, the application requested authority to direct surveillance at [REDACTED] categories of foreign selectors:

- Foreign telephone number and e-mail selectors presently known to the government. This category accounted for a portion of the [REDACTED] foreign selectors already under surveillance pursuant to Judge Howard's Order.<sup>307</sup>

<sup>305</sup> The May 24, 2007, application explicitly stated that the government was not seeking surveillance authority for any new facilities reasonably believed by the NSA to be used by U.S. persons. The application stated that surveillance of those facilities would be initiated only through FISA's emergency authorization provisions and the streamlined FISA applications approved for domestic selectors. ~~(TS//SI//NF)~~

<sup>306</sup> [REDACTED]

<sup>307</sup> The government submitted an appendix with the revised renewal application that identified [REDACTED] facilities and contained the factual basis for the NSA's belief that each of the facilities was being used by a person outside the United States and for which there was probable cause to believe were being used or about to be used by a member or agent of one of the targeted foreign powers. The government had provided Judge Vinson these facilities on a rolling basis during May 2007 for his consideration. The NSA discontinued the surveillance of facilities that were targeted under Judge Howard's Order, but that were not included among the facilities submitted to Judge Vinson for approval. The NSA told the OIG that the decision to discontinue surveillance on these [REDACTED] facilities largely was a resource decision and that [REDACTED] facilities figure was the amount the NSA could timely process for filing with the Court. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

- Foreign e-mail selectors (not telephone number selectors) presently unknown to the government but that "refer to" or are "about" known foreign e-mail selectors. This category of surveillance, which the NSA had been conducting under Judge Howard's Order, includes situations where an already targeted e-mail facility is mentioned in the body of a message between two third-party, non-targeted facilities.<sup>308</sup> ~~(TS//SI//NF)~~

According to the application, the [REDACTED] of surveillance would enable the NSA to initiate surveillance of newly discovered facilities "with the speed and agility necessary to obtain vital intelligence and to detect and prevent terrorist attacks." The application stated,

[REDACTED]

The collection authorities requested in the renewal application that pertained to currently unknown facilities would, according to the application, address this limitation.<sup>309</sup> ~~(TS//SI//NF)~~

Judge Vinson granted the government's revised renewal application on May 31, 2007. His Order authorized, for a period of 90 days, each of the [REDACTED] categories of electronic surveillance described above, although the

---

<sup>308</sup> The category presented an issue under FISA in that communications are being acquired because they contain the targeted e-mail selector, and not because there was probable cause to believe the e-mail accounts sending or receiving the communications are used or about to be used by an international terrorist group. In such cases, the surveillance is not "directed at" the targeted e-mail selector. The government argued that such acquisition was still consistent with FISA because, "at the time of acquisition, the NSA has probable cause to believe that the facilities at which the NSA is directing surveillance are being used by the foreign power target." ~~(TS//SI//NF)~~

<sup>309</sup> The government argued that the FISA Court's authority to authorize subsequent collection against new selectors unknown to the government at the time an application was approved is rooted in section 1805(c)(3) of FISA. That provision imposes specific reporting requirements on the government where the FISA Court approves an electronic surveillance in circumstances where the nature and location of each of the facilities at which surveillance will be directed is unknown at the time of the application. ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

Order defined the precise circumstances under which the NSA could acquire communications falling within the [REDACTED] category of surveillance.<sup>310</sup> The Order also included reporting schedules with respect to the [REDACTED] categories of surveillance, for which the government was required to submit newly discovered selectors to the Court. ~~(TS//SI//NF)~~

Judge Vinson initially approved [REDACTED] foreign selectors under the terms of his May 31, 2007, Order (these selectors were submitted with the government's May 24, 2007, application). Shortly after the Order was issued, the FISA Court decided that the weekly reports filed by the government notifying the Court of newly discovered selectors, as well as the government's motions seeking approval to conduct surveillance on additional selectors, could be filed for review with any member of the Court. As the government received feedback from judges on the first reports and motions that were filed, it observed that judges were applying a more rigorous standard of review to the factual basis supporting the surveillance for each selector than Judge Vinson applied to the [REDACTED] selectors he approved. The government consequently adjusted the amount of factual information it provided the FISA Court in subsequent reports and motions and ultimately added [REDACTED] foreign selectors to Judge Vinson's Order. ~~(TS//SI//NF)~~

According to Bradbury, the more rigorous scrutiny applied by FISA Court judges after Judge Vinson's initial approval [REDACTED] foreign selectors caused the NSA place only a fraction of the foreign selectors under coverage than it wanted to. This concern, combined with the comparatively laborious process for targeting foreign selectors under Judge Vinson's Order, accelerated the government's efforts to obtain legislation that would amend FISA to address the government's surveillance capabilities within the United States directed at persons located outside the United States. The Protect America Act, signed into law on August 5, 2007, accomplished this objective

310

[REDACTED] However, his Order authorized the surveillance of any previously non-targeted e-mail facilities that transmitted e-mail messages containing a targeted e-mail account only when the NSA determined, based on the acquired communication and other intelligence or publicly available information, that there was probable cause to believe the e-mail facility was being used, or was about to be used, by one of the targeted foreign powers. Judge Vinson agreed with the government's position that there was probable cause to believe that Internet communications relating to a previously targeted e-mail facility were themselves being sent or received by one of the targeted foreign powers and could be acquired. Judge Vinson called this holding "novel," but concluded that the decision was "consistent with the overall statutory requirements; it requires the government to promptly report and provide appropriate justification to the Court; and it supplies the Government with a necessary degree of agility and flexibility in tracking the targeted foreign powers." ~~(TS//SI//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

and effectively superseded Judge Vinson's foreign selectors Order. The government therefore did not seek to renew the Order when it expired on August 24, 2007. ~~(TS//SI//NF)~~

In the next section, we summarize the effect of the Protect America Act and successor legislation, the FISA Amendments Act of 2008. (U)

#### **IV. The Protect America Act and the FISA Amendments Act of 2008 (U)**

In August 2007, the Protect America Act was enacted, amending FISA to address the government's ability to conduct electronic surveillance in the United States of persons reasonably believed to be located outside the United States. This legislation expired on February 1, 2008, but was extended by Congress to February 16, 2008. In July 2008, the FISA Amendments Act of 2008 was enacted, which, among other things, created a comprehensive process under FISA for content collection directed at foreign targets. These two laws modernized the FISA statute as it applied to the acquisition in the United States of communications of persons reasonably believed to be outside the United States. (U)

As discussed in Chapter Three, FISA was enacted in 1978 when most international calls were carried by satellite. The interception of such calls constituted "electronic surveillance" for purposes of FISA only if the acquisition intentionally targeted a U.S. person in the United States, or if all participants to the communication were located in the United States. Thus, government surveillance of satellite communications that targeted foreign persons outside the United States generally was not considered electronic surveillance, and the government was not required to obtain a FISA Court order authorizing the surveillance even if one of the parties to the communication was in the United States. However, in the mid-1980s, fiber optic technology began to replace satellites as the primary means for transmitting international (and domestic) telephone communications. This change brought within FISA's definition of "electronic surveillance" the acquisition of telephone calls to or from a person in the United States if the acquisition occurred in the United States, thereby triggering the requirement that the government obtain FISA Court orders to conduct surveillance that it previously conducted outside of FISA. ~~(TS//SI//NF)~~

Under the Stellar Wind program, the NSA collected international communications [REDACTED] by targeting facilities (telephone numbers and e-mail addresses) located outside the United States (foreign

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

selectors).<sup>311</sup> As noted in Chapters Three and Four, the Administration contended that FISA, as supplemented by a subsequent legislative enactment (the AUMF), did not preclude the surveillance activities under Stellar Wind, or in the alternative represented an unconstitutional infringement on the President's Article II authority as Commander in Chief to the extent it conflicted with these collection activities.

~~(TS//STLW//SI//OC/NF)~~

The Justice Department's effort to transfer content collection from presidential authority under Stellar Wind to FISA raised the issue of FISA's application to the acquisition in the United States of communications to or from targeted foreign selectors. The Protect America Act and the FISA Amendments Act, in slightly different ways, addressed this issue by treating the communications of persons reasonably believed to be located outside the United States differently from communications of persons located in the United States.<sup>312</sup> ~~(TS//STLW//SI//OC/NF)~~

#### **A. The Protect America Act (U)**

The Protect America Act of 2007, Pub. L. No. 110-55, was a temporary measure signed into law on August 5, 2007.<sup>313</sup> The Protect America Act's chief objective was to exclude from the requirements of FISA the interception in the United States of communications of persons located outside the United States, the category of communications referred to above as "foreign selectors." (U)

The Protect America Act amended FISA so that the interception of foreign selector communications fell outside the statute's definition of "electronic surveillance." Under the original definition of "electronic surveillance," FISA generally applied to any communication to or from a known United States person inside the United States if the communication is acquired by targeting the known United States person.<sup>314</sup> FISA also

---

<sup>311</sup> The NSA also targeted under Stellar Wind a much smaller number of facilities located inside the United States (domestic selectors). ~~(TS//STLW//SI//OC/NF)~~

<sup>312</sup> The two laws did not substantially affect the provisions of FISA relating to pen register and trap and trace surveillance or to the production of "tangible things." The government continues to collect bulk e-mail and telephone meta data under the PR/TT and Section 215 Orders described in Sections I and II of this chapter. ~~(TS//SI//NF)~~

<sup>313</sup> The Protect America Act was set to expire 180 days after its enactment, or on February 1, 2008. However, Congress passed and on January 31, 2008, the President signed a bill to extend the Protect America Act for 15 days while further discussions on new legislation occurred. However, no agreement was reached on new legislation and the Act expired on February 16, 2008. (U)

<sup>314</sup> The original FISA definition of "electronic surveillance" included:

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

applied to the acquisition of other communications (such as communications acquired by targeting persons outside the United States) if the communication was a "wire communication" and the acquisition occurred inside the United States. (U)

The Protect America Act amended FISA by stating: "Nothing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States." The effect of this amendment was to exclude from the requirements of FISA any communication acquired by targeting a foreign selector, regardless of where the communication was intercepted or whether the communication traveled by wire. As a result, the Act eliminated the need for Judge Vinson's May 2007 foreign selectors Order, because the collection of communications targeted under that Order no longer constituted "electronic surveillance" under FISA and therefore no longer required FISA Court orders.<sup>315</sup> ~~(TS//SI//NF)~~

---

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(20)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f). (U)

315

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

In the place of individualized FISA Court orders, the Protect America Act also inserted several provisions into the FISA statute to govern the acquisition of communications from persons "reasonably believed to be outside the United States." These provisions authorized the Attorney General and the Director of National Intelligence to acquire foreign intelligence information concerning such persons for up to one year, provided these officials certified that there are reasonable procedures in place for the government to determine that a target is reasonably believed to be outside the United States and that the acquisition of the foreign intelligence therefore is not "electronic surveillance" under the amended definition of the term.<sup>316</sup> The targeting procedures accompanying the certification had to be submitted to the FISA Court for approval, based on the clearly erroneous standard, within 120 days of the Protect America Act's enactment. However, the certification was not required to identify specific facilities or places at which the acquisition of foreign intelligence information would be directed.<sup>317</sup> (U)

In addition, the Protect America Act authorized the Attorney General and the Director of National Intelligence to direct a person (telecommunications carriers) to provide the government with "all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition. . . ." Protect America Act, Sec. 2(e). The Protect America Act also authorized the Attorney General and the Director of National

---

[REDACTED] The Protect America Act addressed this issue by excluding all surveillance directed at persons reasonably believed to be outside the United States.

~~(TS//SI//NF)~~

<sup>316</sup> The Attorney General and the Director of National Intelligence also had to certify that the acquisition involves the assistance of a communications service provider; that a "significant purpose" of the acquisition to obtain foreign intelligence information is for foreign intelligence purposes; and the minimization procedures to be used with the acquisition activity comport with 50 U.S.C. § 1801(h). Protect America Act, Sec. 2, codified in FISA at 50 U.S.C. § 1805B(a)(1)-(5). (U)

<sup>317</sup> The Protect America Act left unchanged the procedures for acquiring foreign intelligence information by targeting foreign powers or agents of foreign power inside the United States, as well as the procedures under Executive Order 12333 Sec. 2.5 to obtain Attorney General approval before acquiring foreign intelligence information against a U.S. person outside the United States. Thus, FISA orders issued prior to the enactment of the Protect America Act, and FISA orders, including applications for renewals, sought after enactment of the Protect America Act but not pursuant to the Act's amendments (acquisition of foreign intelligence information from targets outside the United States) were still subject to FISA as it existed prior to the Protect America Act. The Protect America Act also provided, by means of an "opt-out" clause, that the government did not have to use the new procedures for new applications and could instead file applications under the provisions of FISA as it existed before the Protect America Act. See Protect America Act, Sec. 6(b). (U)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

Intelligence to seek the assistance of the FISA Court to compel compliance with such directives, and implemented procedures for the telecommunications carriers to challenge the legality of any such directives.<sup>318</sup> (U)

The Protect America Act authorized the Attorney General and the Director of National Intelligence to issue orders without individualized FISA Court approval for up to one year targeting persons reasonably believed to be outside the United States. These orders remained in effect beyond the expiration of the Protect America Act on February 16, 2008. (U)

On August 10, 2007, the Attorney General and the Director of National Intelligence filed a certification with the FISA Court, as required under the Protect America Act, relating to surveillance of persons reasonably believed to be outside the United States likely to communicate information concerning [REDACTED]

[REDACTED] The certification included directives for assistance to specific telecommunications carriers. ~~(TS//SI//NF)~~

[REDACTED] foreign selectors under Judge Vinson's Order were "rolled over" to the new Protect America Act authority. A Deputy Assistant Attorney General in the National Security Division familiar with the transition of Stellar Wind to FISA Court authority told us that the government also began to "build new selectors" under the Protect America Act and worked toward restoring the universe of foreign selectors that were first authorized for tasking under Judge Howard's January 2007 Order when content collection under Stellar Wind initially had migrated to FISA Court authority. ~~(TS//SI//NF)~~

Although the Department viewed the Protect America Act as an adequate temporary fix to those provisions of FISA seen as outdated because of changes in telecommunications technology, Department officials continued to press Congress for more permanent modernization legislation. (U)

---

<sup>318</sup> The Protect America Act also stated that any person providing assistance to the government pursuant to a governmental directive would not be subject to any cause of action for providing such assistance. However, the Protect America Act did not grant retroactive legal immunity to any "person," a term defined in FISA to include "any group, entity, association, corporation, or foreign power." 50 U.S.C. § 1801(m). On August 22, 2008, the FISA Court of Review upheld as constitutional the Protect America Act provision authorizing the Director of National Intelligence and the Attorney General to direct a person to assist the government in implementing the Act. See *In Re: Directives* [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01. (U)

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~**B. The FISA Amendments Act of 2008 (U)**

On July 11, 2008, the President signed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act). This legislation, composed of four titles, replaced the Protect America Act with similar but more comprehensive surveillance authority. The provisions of the FISA Amendments Act expire, with limited exceptions, on December 31, 2012. (U)

A chief objective of the FISA Amendments Act was to change the rules for intercepting the electronic communications of persons reasonably believed to be outside the United States when the acquisition occurs in the United States. As discussed above, the Protect America Act accomplished this by amending FISA's definition of "electronic surveillance" to exclude this activity from FISA requirements. The FISA Amendments Act took a different approach. Instead of excluding the activity from the statute's definition of "electronic surveillance," the FISA Amendments Act created a new title in FISA to govern how the government may conduct this electronic surveillance. Under this approach, the FISA Amendments Act, unlike the Protect America Act, distinguishes between the targeting of non-U.S. and U.S. persons reasonably believed to be outside the United States.<sup>319</sup> (U)

For non-U.S. persons, the new title created by the FISA Amendments Act provides for surveillance authority similar to the Protect America Act. Instead of requiring the government to obtain individualized orders from the FISA Court to intercept communications of non-U.S. persons reasonably believed to be outside the United States, the FISA Amendments Act authorized the government to conduct any such interceptions for a period of up to one year provided that it adopts, and the FISA Court approves, general targeting procedures designed to ensure that the new authority is not used

---

<sup>319</sup> The Senate Select Committee on Intelligence (SSCI) prepared a section-by-section analysis of the FISA Amendments Act of 2008 explaining the significance of the FISA Amendment Act's approach. According to the SSCI report, the goal of the Protect America Act in redefining the term "electronic surveillance" was to exclude the surveillance of persons outside the United States from the individualized order requirements of FISA. However, a consequence of the term's redefinition was to broadly exempt foreign surveillance activities both of non-U.S. and U.S. persons outside the United States. The FISA Amendments Act of 2008, instead of adopting the Protect America Act's modified definition of "electronic surveillance," explicitly stated that the targeting of non-U.S. persons outside the United States shall be conducted under the new FISA procedures, which does not require an application for a FISA order. In this way, the FISA Amendments Act accomplished the same goal as the Protect America Act without exempting the targeting of U.S. persons outside the United States from FISA's individualized order requirements. (U)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

to direct surveillance at persons within the United States or at U.S. persons outside the United States.<sup>320</sup> (U)

In contrast, to conduct U.S.-based surveillance of U.S. persons reasonably believed to be located outside the United States, the FISA Amendments Act requires the government to obtain individualized FISA Court orders for 90-day periods based on a showing of probable cause to believe that the U.S. person is outside the United States and is a foreign power or an agent, officer, or employee of a foreign power. Such surveillance previously was governed by Executive Order 12333, and required only a certification from the Attorney General, not the FISA Court. (U)

Compared to Stellar Wind, the FISA Amendments Act provides the government broader authority to acquire in the United States, with Court supervision, the communications of non-U.S. persons reasonably believed to be located outside the United States. Under Stellar Wind, the NSA was authorized to collect communications where there was probable cause to believe the communications originated or terminated outside the United States and a party to the communications was al Qaeda or a group affiliated with al Qaeda. Under the FISA Amendments Act, the NSA is authorized to collect in the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence.

~~(TS//STLW//SI//OC/NF)~~

<sup>320</sup> Like the Protect America Act, in addition to these targeting procedures the certification the government is required to file with the FISA Court must also contain minimization procedures and state that a significant purpose of the acquisition that will be conducted is to obtain foreign intelligence information. However, unlike the Protect America Act the FISA Amendments Act does not limit the FISA Court's review of the targeting procedures to a "clearly erroneous" standard. On August 5, 2008, the government submitted to the FISA Court a certification pursuant to the FISA Amendments Act. On September 5, 2008, the Court approved the certification and the use of the targeting and minimization procedures the government submitted. ~~(S//NF)~~

<sup>321</sup> On the other hand, the FISA Amendments Act does not similarly broaden the government's authority to conduct surveillance of U.S. persons reasonably believed to be located outside the United States. The Presidential Authorizations did not distinguish between U.S. and non-U.S. persons, and the NSA was authorized under Stellar Wind to intercept the communications of U.S. persons (domestic selectors) provided the communications originated or terminated outside the United States.

~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

In Chapter Three, we noted that under certain circumstances technological limitations associated with the e-mail content aspect of the Stellar Wind program caused [REDACTED]

[REDACTED]

(TS//SI//NF)-

The NSA undertook measures to identify and correct incidents [REDACTED] under Stellar Wind, and the government described the issue to the FISA Court in the December 2006 application that sought to bring Stellar Wind's content collection under FISA authority [REDACTED]

[REDACTED]

(TS//SI//NF)-

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

## V. **OIG Analysis (U)**

As discussed in this chapter, the government's effort to transition Stellar Wind from presidential authority to FISA, which began in March 2004, eventually resulted in all three baskets of collection being authorized by FISA. While the legal theories supporting this transition were aggressive, we believe that the Department could have and should have pursued transition to FISA as a viable legal alternative earlier than it did, rather than operate aspects of the Stellar Wind program solely under presidential authority for several years. ~~(TS//STLW//SI//OC/NF)~~

In Chapters Three and Four we discussed John Yoo's 2001 and 2002 memoranda concerning the legality of Stellar Wind and his contention that FISA represented an unconstitutional infringement on the President's Commander-in-Chief authority under Article II of the Constitution to conduct electronic surveillance during wartime. We recognize that Yoo's analysis was to some extent a response to the extraordinary circumstances that confronted the federal government immediately after the September 11 terrorist attacks and its effort to take emergency steps to thwart what many officials believed was an imminent second wave of attacks. Yet, even if one agrees with Yoo's Article II analysis and supports the decision to enhance outside the judicial or legislative process the NSA's signals intelligence collection capabilities, we believe there are strong countervailing considerations that favored attempting to transition the program to FISA, especially as Stellar Wind became less a temporary response to the September 11 attacks and more a permanent surveillance tool. ~~(TS//STLW//SI//OC/NF)~~

Chief among these considerations was the Stellar Wind program's substantial effect on privacy interests of U.S. persons. Under Stellar Wind, the government engaged in an unprecedented collection of information concerning U.S. persons. The President authorized the NSA to intercept, without judicial approval or oversight, the content of international communications involving many U.S. persons and the NSA collected large amounts of non-content data about U.S. persons' domestic and international telephone calls and to a lesser extent e-mail communications for possible analysis consistent with the extant Presidential Authorization. We believe the FISA Court, as an Article III court and the judicial authority charged by statute to oversee U.S.-based electronic surveillance and other collection activities affecting U.S. persons for foreign intelligence purposes, was the appropriate entity to monitor and approve such broad acquisitions

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

of U.S.-person information conducted under Stellar Wind.<sup>322</sup>

~~(TS//STLW//SI//OC/NF)~~

Second, as several Justice Department and NSA officials commented, the FISA statute offered a "firmer footing" for the NSA's collection activities under Stellar Wind. As discussed in Chapter Three and Four, the aggressive assertion of Article II authority on which Stellar Wind was based largely reflected the legal reasoning of a single Justice Department attorney working alone, without adequate review or scrutiny of his analysis. As we also concluded, this led to a flawed legal analysis on which the program rested for several years. This approach also led to a contentious dispute between Department and White House officials in 2004 involving renewal of aspects of the program. By contrast, the FISA statute provided an alternative basis for Stellar Wind-like collection activities that we believe should have been considered, and pursued, much earlier by the Administration. ~~(TS//STLW//SI//OC/NF)~~

In this regard, the White House's strict control over the Justice Department's access to the program lessened the opportunity for lawyers with relevant expertise to advise the Administration on the viability of working within the FISA statute to achieve the same operational objectives as the Stellar Wind program. Moreover, as the limited number of Department read-ins persisted, meaningful consideration of FISA as an alternative to presidential authority for the program was limited.<sup>323</sup>

~~(TS//STLW//SI//OC/NF)~~

---

<sup>322</sup> For instance, under Stellar Wind the meta data querying standards did not include restrictions on acquiring data that may have been based solely on the exercise of First Amendment rights. When these activities were placed under the FISA Court's supervision, the Court required that this intelligence-gathering activity adhere to the FISA standard that an e-mail address or telephone number cannot be targeted for acquisition based solely on activities protected by the First Amendment. ~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

We also found there were operational benefits to transitioning Stellar Wind to FISA. The PR/TT and Section 215 Orders to collect e-mail and telephone meta data that were eventually obtained from the FISA Court allowed the government to compel [REDACTED] the [REDACTED] telecommunications carriers. [REDACTED]

(TS//STLW//SI//OC/NF)

The transition of Stellar Wind to FISA authority, together with the passage of the Protect America Act, allowed the NSA to begin the process to close, or "de-compartment," the Stellar Wind program. This change, which was not completed until mid-2008, has allowed agents in FBI field offices greater access to information about the telephone numbers and e-mail addresses being provided as leads. As described in Chapter Three, the principal complaint of agents who were assigned [REDACTED] and [REDACTED] leads was the lack of detail provided about the nature of the international contacts and the foreign entity allegedly involved with terrorism that was one of the communicants. These details often were not provided because of the highly classified and compartmented nature of the Stellar Wind program. Now that such information is gathered under FISA authority and not compartmented as it was under Stellar Wind, it is classified at a level that allows agents in FBI field offices to gain access to additional details upon request.<sup>324</sup> (TS//STLW//SI//OC/NF)

We recognize that Stellar Wind's transition to FISA resulted in the imposition of new responsibilities and conditions on the exercise of these unprecedented collection authorities. In the PR/TT and Section 215 Orders, the FISA Court imposed significant oversight measures that were not required under Stellar Wind. To be sure, the government, particularly the NSA, must devote substantial resources to ensure compliance with these oversight measures. Yet, we believe that such requirements are appropriate, given the massive amounts of data collected and the potential impact on the privacy interests of U.S. persons. (TS//STLW//SI//OC/NF)

We also recognize that the transition of content collection from presidential authority to statutory authority under FISA resulted in significant diminution in authorized surveillance activity of the content of communications. We described in this chapter how first under Judge Howard's Order, and then more significantly under Judge Vinson's revised

---

<sup>324</sup> Chapter Six of this report discusses FBI agents' improved access to program-derived information under FISA after the Stellar Wind program was closed. (TS//SI//NF)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

Order, the NSA placed increasingly fewer foreign selectors under FISA coverage as compared to Stellar Wind. The NSA was tasking [REDACTED] foreign selectors under Stellar Wind at the time of the first content application in December 2006, but placed [REDACTED] foreign selectors under surveillance coverage under Judge Vinson's May 2007 Order. National Security Division officials told us that they successfully added approximately [REDACTED] foreign selectors under the terms of the Court's Order. ~~(TS//STLW//SI//OC/NF)~~

However, we believe that such broad surveillance and collection activities conducted in the United States, particularly for a significant period of time, should be conducted pursuant to statute and judicial oversight, even though this resulted in a diminution of foreign selectors due to resource issues. We also believe that placing the activities under Court supervision provides an important measure of accountability for the government's conduct that is less assured when the activities are both authorized and supervised by the Executive Branch alone.<sup>325</sup>  
~~(TS//STLW//SI//OC/NF)~~

In sum, we concluded there were compelling reasons to pursue beginning the process of transitioning the collection activities of Stellar Wind to FISA authority earlier than [REDACTED] 2004. These included the program's large collection of information about U.S. persons, which warranted judicial oversight; the instability of the legal reasoning on which the program rested for several years; and the substantial restrictions placed on FBI agents' access to and use of program-derived information due to Stellar Wind's highly classified status. We acknowledge that transitioning Stellar Wind's collection activities to FISA would have been an enormously complex and time-consuming effort that rested upon novel interpretations and uses of FISA that not all FISA Court judges would authorize. Nevertheless, the events described in this chapter demonstrate that a full transition to FISA authority was achievable and, in our judgment, should have been pursued earlier. ~~(TS//STLW//SI//OC/NF)~~

---

<sup>325</sup> Even Judge Vinson's decision regarding the foreign selectors content application, [REDACTED] was not without benefit. Judge Vinson's decision reflected what some intelligence officials considered limitations in the FISA statute as it applied to the acquisition of communications in the United States of persons located outside the United States, especially non-U.S. persons. In this way, transitioning Stellar Wind's content collection to FISA helped the government make its case to Congress in concrete, non-hypothetical terms for modernization legislation amending the statute. ~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~**CHAPTER SIX****(S//NF)**

The preceding chapters examined the evolution of the Stellar Wind program and its transition from Presidential Authorization to FISA authority. In this chapter, we examine more closely the FBI's involvement in Stellar Wind and the impact the program had on FBI counterterrorism efforts. ~~(TS//STLW//SI//OC/NF)~~

[REDACTED] is the codename for the project, classified at the Secret level, that the FBI initiated in September 2002 to disseminate Stellar Wind information to FBI field offices in a manner that did not disclose the source of the information or the means by which it was acquired. The FBI originally opened [REDACTED] as an administrative file to serve as the repository for all communications FBI Headquarters disseminated to FBI field offices relating to Stellar Wind information, as well as all communications FBI Headquarters received from field offices reporting the results of any investigation conducted in response to the "tipped" information originating from Stellar Wind. In November 2006, the FBI opened an investigative file under the name [REDACTED]<sup>326</sup>  
~~(TS//STLW//SI//OC/NF)~~

Section I of this chapter summarizes how the FBI used [REDACTED] to disseminate Stellar Wind information to FBI field offices. Section II describes the FBI's decision in mid-2003 to make its headquarters-based Communications Analysis Unit (CAU), instead of FBI field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information for telephone numbers (basket 2 of Stellar Wind) disseminated under [REDACTED]<sup>327</sup> Section III discusses the role the FBI played, beginning in approximately March 2004, in the process to "scrub" international terrorism FISA applications for Stellar Wind information.  
~~(TS//STLW//SI//OC/NF)~~

Section IV of this chapter examines the impact of the information obtained from Stellar Wind on FBI counterterrorism efforts. It first provides statistics concerning the number of tipplers the NSA derived from Stellar Wind information – telephony, e-mail, and content – disseminated to FBI

<sup>326</sup> As discussed in Chapter Three, [REDACTED] was preceded by the [REDACTED] which the FBI created in October 2001 to receive and disseminate Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

<sup>327</sup> The CAU is the successor to the Telephone Analysis Unit (TAU), which the FBI created after the September 11 terrorist attacks to analyze telephone communications. The CAU assumed TAU's responsibilities in late 2002. ~~(S//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

field offices through the [REDACTED] process. Next, it describes how FBI field offices generally investigated [REDACTED] tippers and the typical results of the investigations. The section then summarizes two statistical surveys of meta data tippers the FBI conducted in 2006 to assess the value of Stellar Wind to FBI operations, and describes observations about the program's contribution and value provided by FBI officials and employees in OIG interviews and contained in documents the OIG obtained during the course of this review. In addition, the section examines five FBI international terrorism investigations commonly cited as examples of Stellar Wind's contribution to counterterrorism efforts in the United States.<sup>328</sup>

~~(TS//STLW//SI//OC/NF)~~

Lastly, Section V of this chapter contains the OIG's analysis of [REDACTED] impact on FBI operations. ~~(S//NF)~~—

#### **I. [REDACTED] Process ~~(S//NF)~~**

The [REDACTED] process was managed by a group of FBI employees from CAU, designated as "Team 10," who in February 2003 were assigned full-time to the NSA to work on the Stellar Wind program.<sup>329</sup> Team 10 was described to us as a "conduit" and a "curtain" between Stellar Wind and the FBI, in that Team 10's chief responsibility was to disseminate Stellar Wind-derived information to FBI field offices for investigation without disclosing that the NSA was the source of the information or how the NSA acquired the information. ~~(TS//STLW//SI//OC/NF)~~

Team 10 initially was staffed with two FBI special agents (one of whom served as supervisor) and two analysts. The CAU subsequently replaced one agent position with a third analyst and later added a fourth analyst. At the NSA, Team 10 was co-located in a large open space with dozens of NSA and other Intelligence Community personnel assigned to the Stellar Wind program. Each team member was provided a computer with direct access to NSA information associated with Stellar Wind. The NSA told the OIG that Team 10 members worked at the NSA under the authority of the NSA Director and as such were required to adhere to NSA minimization rules and attend the same training as NSA employees. Team 10 members also were provided access to Stellar Wind-related systems and

<sup>328</sup> As noted above, our report examines the FBI's role in the Stellar Wind program and does not review the use of the program by other agencies, such as the CIA. ~~(S//NF)~~

<sup>329</sup> The CAU is organized into ten teams, nine of which are responsible for providing communications analysis support to specific field offices and FBI Legal Attaches (Legat). According to an FBI organizational chart, Team 10 supports "Off-site Intelligence Community Special Projects." Team 10 was exclusively responsible for managing [REDACTED]

~~(S//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

databases, and had access from their computers to FBI systems such as the Automated Case Support (ACS) system and [REDACTED]  
(TS//STLW//SI//OC/NF)

The process under [REDACTED] to disseminate Stellar Wind information was similar to the process the FBI established under the [REDACTED] described in Chapter Three. In short, the NSA provided Top Secret, compartmented Stellar Wind reports to Team 10, which in turn converted the information into Secret, non-compartmented [REDACTED] electronic communications (EC) and disseminated the communications, referred to as [REDACTED] "tippers," to FBI field offices for appropriate action.<sup>330</sup> The [REDACTED] process was applied, with some differences, to each of Stellar Wind's three "baskets" of information. The vast majority of Stellar Wind reports involved the NSA's analysis of telephony meta data – that is, basic information such as date, time, and duration, about contacts between foreign and domestic telephone numbers for which the NSA determined there was a reasonable articulable suspicion to believe were related to al Qaeda or an affiliated group.<sup>331</sup> (TS//STLW//SI//OC/NF)

Each [REDACTED] EC included a paragraph that summarized the [REDACTED] project and explained that the CAU could not disclose the source of the information contained in the EC, but that the information came from a "sensitive and highly reliable" source. Each EC also included a paragraph advising the field offices that the information provided by the [REDACTED] source could be used for "lead purposes only" and could not be "incorporated into any affidavit, court proceeding, FISA application or

330

331

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

unclassified investigative file." In addition, each [REDACTED] EC assigned a "lead" that instructed the field office what investigative action, if any, should be taken regarding the information provided. We further describe [REDACTED] leads and FBI field offices' handling of them in Section IV of this chapter. (TS//STLW//SI//OC/NF)

Before Team 10 disseminated Stellar Wind-derived information to field offices, an analyst queried FBI databases for relevant information about the telephone number, e-mail address, or individual (in the case of a content report) identified in the Stellar Wind report. These queries often identified, for example, subscriber information the FBI previously obtained for Stellar Wind telephone numbers as part of a prior FBI investigation, or active counterterrorism investigations in which the subscriber to a Stellar Wind-targeted number was the subject or in which the number, and sometimes the subscriber, were referenced. Team 10 analysts also checked public and commercial databases, most commonly in connection with e-mail addresses. These checks sometimes identified the specific [REDACTED] and any domain names the user of an e-mail address had registered. [REDACTED]

Any such information Team 10 located about a Stellar Wind-derived telephone number or e-mail address was included in the [REDACTED] EC as a "CAU Comment" or an "Analyst Comment" to differentiate the FBI information from the information provided by the Stellar Wind source.<sup>332</sup> (TS//STLW//SI//OC/NF)

Over time, Team 10 began to do more than receive and disseminate program-derived information. For example, Team 10 occasionally submitted telephone numbers to the NSA for possible querying against the database containing the bulk telephony meta data collected under Stellar Wind.<sup>333</sup>

<sup>332</sup> In this respect, Team 10 handled Stellar Wind content reports differently from meta data reports. Team 10 analysts typically did not perform additional analytical work on the information provided in Stellar Wind content reports other than to identify any FBI cases to which the information was relevant. For example, a content report might summarize intercepted communications indicating that an acquaintance of the subject of an FBI investigation is traveling to or from the United States. The connection between this Stellar Wind information and the relevant FBI investigation would be reported in the [REDACTED] EC. (TS//STLW//SI//OC/NF)

<sup>333</sup> As described in previous chapters, the purpose of the bulk collection of meta data under Stellar Wind was to allow the NSA to use analytical tools such as contact chaining [REDACTED] to identify known and unknown individuals associated with al Qaeda or an al Qaeda affiliate. The technique involves querying the telephony or e-mail database with a number or address for which an analyst had a "reasonable articulable suspicion" to believe was used by persons involved in al Qaeda or an al Qaeda affiliate, and then examining any contacts with that number or address. (TS//STLW//SI//OC/NF)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

The telephone numbers Team 10 provided typically were obtained from the FBI's domestic and international counterterrorism operations, such as a number identified during a phone conversation monitored under FISA or a number found in the address book of a subject arrested abroad. The NSA conducted independent analysis to determine whether telephone numbers (or e-mail addresses) provided by Team 10 met the querying standard established by the Presidential Authorizations that governed Stellar Wind (that is, a reasonable articulable suspicion to believe that communications from the telephone number relate to al Qaeda or an affiliated group).<sup>334</sup>  
~~(TS//STLW//SI//OC/NF)~~

Team 10 also contributed to the NSA's drafting process for Stellar Wind reports. Telephone numbers and e-mail addresses identified through queries of the databases that contained the bulk telephony and e-mail meta data were reviewed by NSA analysts to determine whether the contacts should be reported to the FBI in a Stellar Wind report. Team 10 participated in this process by reviewing draft reports and providing any information from FBI databases that might be relevant to this determination.<sup>335</sup>  
~~(TS//STLW//SI//OC/NF)~~

We were told that one of the benefits of Team 10's presence at the NSA and its involvement in the Stellar Wind report drafting process was an improvement in the quality of the information disseminated to FBI field offices. For example, the FBI Supervisory Special Agent (SSA) who supervised Team 10 from April 2005 to July 2006 told the OIG that he tried to reduce the NSA's reporting of telephone numbers that were several hops removed from the telephone number linked to al Qaeda or an affiliated terrorist group. He said that he wanted Team 10 to disseminate "solid numbers with value," not numbers with questionable value such as "high volume numbers" (public telephones, for example) and [REDACTED]

The FBI SSA said that the NSA expressed the concern

<sup>334</sup> Team 10 analysts submitted such telephone numbers to the NSA electronically through "Requests for Information," or RFIs, which is the formal process by which the FBI and other agencies provide leads and request information from the Stellar Wind database. FBI records indicate that from April 2002 to January 2006 the FBI directed [REDACTED] to NSA analysts for possible analysis under Stellar Wind. The records do not indicate the disposition of each RFI.  
~~(TS//STLW//SI//OC/NF)~~

<sup>335</sup> The NSA developed formal "checklists" to guide the Stellar Wind report drafting process for telephony and e-mail tipplers. The checklists include over 30 steps that NSA analysts were required to complete, and a supervisor had to approve, before a report could be distributed to the FBI or any other Stellar Wind customers (the CIA and National Counterterrorism Center). A significant feature of the checklist from the FBI's perspective was the requirement that NSA analysts check any telephone numbers and e-mail addresses in a draft report with the FBI and "make best effort to include FBI . . . data in [the] tipper."  
~~(TS//STLW//SI//OC/NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

that it could not foresee whether any particular contact, although remote, might prevent the next terrorist attack, and did not want to find itself in the position of defending its decision not to pass that number to the FBI. However, he said the NSA took several steps to improve the quality of information such as [REDACTED] for the domestic contacts that were reported and including analytical judgments about the contacts.<sup>336</sup>  
~~(TS//STLW//SI//OC/NF)~~

As discussed in Chapter Five, the government transitioned Stellar Wind's bulk e-mail meta data collection (basket 3) to FISA authority in July 2004 with the Pen Register/Trap and Trace Order, bulk telephony meta data collection (basket 2) in May 2006 with the Section 215 Business Records Order, and content collection (basket 1) in January 2007 when the FISA Court granted the government's domestic and foreign selectors applications. ~~(TS//STLW//SI//OC/NF)~~

However, after the transition was completed the NSA continued to produce reports within the Stellar Wind compartment to the FBI and other program customers, even though the information contained in the reports was derived from the FISA-authorized collection activities. Consequently, the FBI continued to disseminate the information under the [REDACTED] process. The current Team 10 supervisor told us that this decision, reached after consultation with the FBI's Office of the General Counsel (OGC), was made to adhere to the FISA Court's continuing requirement that international terrorism FISA applications be scrubbed for Stellar Wind information (the procedure for which is described in Section III of this chapter). ~~(TS//STLW//SI//OC/NF)~~

The NSA received permission to begin the process to close, or "de-compartment," the Stellar Wind program after the Protect America Act was passed in August 2007. In mid-2008, the NSA officially closed the program and discontinued issuing "Stellar Wind" reports. In November 2008, the FBI initiated a new investigative file, [REDACTED] to disseminate the NSA's FISA-derived information.<sup>337</sup> The Team 10 supervisor

<sup>336</sup> The NSA told us that one of the difficulties it faced with the Stellar Wind program was that the NSA was serving two customers – the FBI and the CIA – but had just one set of reporting guidelines. This was so because the NSA traditionally does not provide single-agency reporting except in narrowly defined circumstances. [REDACTED]

[REDACTED] ~~(S//NF)~~

<sup>337</sup> According to the FBI memorandum explaining the predication for opening the file, the focus of [REDACTED] investigation is on known and unknown operatives of [REDACTED]

[REDACTED] The memorandum stated that as of August 2008 the FBI had [REDACTED] open national security investigations related to [REDACTED] of individuals believed to be associated with [REDACTED]

(Cont'd.)

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

told us that the dissemination process and the FBI's coordination with the NSA under [REDACTED] is similar to what occurred under [REDACTED]. However, one notable difference is that the NSA's FISA-derived reports, while classified at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, are not subject to the highly restrictive Stellar Wind compartment designation, which is significant from an operational standpoint. [REDACTED] ECs, like [REDACTED] ECs, can only include information classified Secret or lower because the FBI's primary computer network for disseminating communications cannot be used for Top Secret information. Unlike under [REDACTED] agents in field offices can now request access to additional information about [REDACTED] leads because agents have the appropriate clearances. As discussed in Chapter Three and addressed below, the chief criticism of [REDACTED] leads was the lack of detailed information that could be provided to field agents about tippers because of the highly compartmented nature of Stellar Wind.

~~(TS//STLW//SI//OC/NF)~~

## II. **FBI's Decision to Issue National Security Letters under [REDACTED] [REDACTED] to Obtain Telephone Subscriber Information** ~~(S//NF)~~

From August 2003 to November 2006, as part of the [REDACTED] process the Communications Analysis Unit (CAU) assumed responsibility from the field offices for requesting National Security Letters (NSL) to obtain subscriber information for [REDACTED] telephone number tippers.<sup>338</sup> The NSLs were authorized by the FBI's OGC and issued pursuant to the [REDACTED] project. As discussed below, however, this practice was contrary to applicable FBI investigative guidelines because [REDACTED] was opened as a non-investigative file and therefore under FBI policy should not have been used as the basis for issuing NSLs. ~~(S//NF)~~

The FBI uses NSLs to obtain information from third parties such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies. NSLs, authorized by five specific provisions contained in four federal statutes, direct third parties to provide customer account information and transactional records such as telephone toll billing

[REDACTED] of individuals believed to be associated with [REDACTED] and [REDACTED]  
[REDACTED] of [REDACTED] ~~(S//NF)~~

<sup>338</sup> Field offices remained responsible for issuing NSLs in connection with e-mail address tippers, which was likely attributable to the comparatively low volume of e-mail tippers and the ability of field offices to handle them expeditiously. ~~(S//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~



~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

records.<sup>339</sup> The OIG issued two reviews in 2007 and 2008 examining the FBI's use of NSLs.<sup>340</sup> (U)

Justice Department investigative guidelines issued by the Attorney General govern the circumstances under which the FBI may use NSLs. The Attorney General guidelines in effect during the Stellar Wind program authorized the FBI to issue NSLs relevant to and in the course of an authorized national security investigation.<sup>341</sup> Further, FBI internal policy distinguishes between "investigative files" and non-investigative "administrative files" (commonly referred to as "control files"). This distinction is not a mere technicality. Investigative files, in the national security context, are opened based on evidence that a person, group, or organization is involved in international terrorism. From October 2003 to September 2008, the Attorney General Guidelines required the FBI to provide summary reports to the Justice Department at the end of each year

<sup>339</sup> The four federal statutes are the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422; the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709; the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; and the National Security Act, 50 U.S.C. § 436(a)(1) (2000). NSLs issued under [REDACTED] relied on the ECPA statute, which provides that the FBI may obtain subscriber information from a communications service provider if the FBI certifies that the information sought is

relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

18 U.S.C. § 2709(b)(2) (2000 & Supp. IV 2005). The statute also permits access to "toll billing records" or "electronic communication transactional records," 18 U.S.C. § 2709(a), but requires a warrant for access to the content of telephone communications. See 18 U.S.C. § 2511 (Wiretap Act) and 3121 (Pen Register Act); see also 18 U.S.C. § 2702(b)(8). (U)

<sup>340</sup> The OIG's first report on NSLs, issued in March 2007, was entitled, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*. The OIG's second report, issued in March 2008, was entitled, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*. (U)

<sup>341</sup> From March 8, 1999, through October 31, 2003, national security investigations were governed by the Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCI Guidelines). The FCI Guidelines were replaced, effective October 31, 2003, with the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines). (U)

The evidentiary standard for initiating an investigation is the same under both sets of guidelines. To open a full investigation, the FBI is required to demonstrate [REDACTED]

[REDACTED] A preliminary investigation (or "inquiry," under the FCI guidelines) requires only a showing of [REDACTED] of such involvement. See NSI Guidelines, Section II.C. (October 31, 2003); FCI Guidelines, Section III.B. (March 8, 1999). ~~(S//NF)~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

a full national security investigation continues. These requirements helped ensure that there was sufficient, documented predication for investigative activities FBI agents sought to conduct, such as requesting NSLs. ~~(S//NF)~~

Control files, in contrast, are "separate files established for the purpose of administering specific phases of an investigative matter or program." The files do not require any predication and remain open indefinitely without any reporting requirements for national security investigations. For example, the September 2002 EC requesting that a control file [REDACTED] be opened for Stellar Wind information stated that "a dedicated control file for this project will better serve the specific needs of the special project and will add an additional layer of security for the source." The file has remained open since September 2002 without any official documentation of need or justification. (As discussed below, in November 2006 the FBI opened an [REDACTED] investigative file; however, the [REDACTED] control file was not closed at that time.)  
~~(TS//STLW//SI//OC/NF)~~

The FBI's National Foreign Intelligence Program (NFIP) Manual states that [REDACTED]

[REDACTED]<sup>342</sup> Thus, in accordance with the NFIP Manual, it was improper for the FBI to issue NSLs from control files during the Stellar Wind program. ~~(S//NF)~~

The OIG's March 2007 NSL report identified the [REDACTED] project as one of two circumstances where the FBI was using control files rather than investigative files to issue NSLs. The OIG report concluded that this use was contrary to FBI policy. However, our report also found that the CAU officials involved in the decision to issue NSLs from the [REDACTED] control file concluded in good faith that the FBI had sufficient predication either to connect the [REDACTED] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. ~~(S//NF)~~

[REDACTED]

~~TOP SECRET//STLW//HCS//SI//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~

As part of our review of the FBI's participation in Stellar Wind, we sought additional explanation for the use of NSLs under [REDACTED]. We were told the purpose of having the CAU instead of the field offices obtain approval for the issuance of such NSLs was to make the telephony tippers more "actionable" by ensuring that field offices at a minimum knew the subscribers for the numbers. As described in Chapter Three, the members of the [REDACTED] (the predecessor to [REDACTED]) had received complaints from agents in FBI field offices that [REDACTED] leads lacked direction about how to make investigative use of the telephone numbers and did not provide sufficient information to open national security investigations. This was problematic because leads disseminated under the [REDACTED] and for a time under [REDACTED] instructed field offices to obtain subscriber information for tipped telephone numbers. Thus, if agents could not locate the information in FBI or commercial databases, they faced a dilemma about how to proceed in the absence of what they viewed as sufficient predication. ~~(TS//STLW//SI//OC/NF)~~

The CAU's first Unit Chief (who served in an Acting capacity) discussed the problem in an EC distributed in January 2003 that addressed the [REDACTED] project. The EC stated,

Depending on the nature of the information provided [in an [REDACTED] lead], field offices may determine this intelligence could be used to predicate either a criminal investigation or an intelligence investigation of someone in their territory. Some of the [REDACTED] leads may contain a request for a field office to confirm a subscriber in their territory, if possible, in addition to providing intelligence. The identification of some subscribers might actually require a National Security Letter (NSL) or a Grand Jury subpoena; however, the [REDACTED] control file would not be the appropriate legal authority for these requests. ~~(S//NF)~~

The Acting Unit Chief's supervision of the CAU ended in February 2003. In March 2003, another FBI Supervisory Special Agent (SSA) was appointed as the CAU's first permanent Unit Chief. He told us that when he joined the CAU he was aware that field offices sometimes did not obtain subscriber information on tippers because some agents did not believe [REDACTED] ECs provided sufficient information to open a national security investigation. The Unit Chief disagreed, based in part on his insider knowledge about how Stellar Wind operated. He said that he believed the

~~TOP SECRET//STLW//HCS//SI//ORCON//NOFORN~~