period in 2004, NSA analysts were permitted to query [redacted]

~~(TS//SI//OC/NF)~~ According to General Hayden, the Authorization, for the most part, did not change the communications that NSA could collect, but did change the location from which the Agency could collect them by permitting collection [redacted] in the United States. Without that authorization, [redacted]

[redacted]

(U) NSA Discussions about the Lawfulness of the Authorization

~~(TS//SI//NF)~~ NSA leaders believed that they could lawfully carry out the President's authorizations. However, they also recognized that the Program would be controversial and politically sensitive. This section describes how key NSA leaders—the Director, the NSA General Counsel, Deputy General Counsel, and Associate General Counsel for

Operations—concluded that the Program was legally defensible.

(U) Director of NSA

~~(TS//SI//NF)~~ Generals Hayden and Alexander stated that they believed the Authorization was lawful.

(U) General Hayden

~~(TS//SI//NF)~~ When asked how he had decided to execute an Authorization that some would consider legally and politically controversial, General Hayden said that NSA's highest ranking lawyers had advised him, collectively and individually, that the Program was lawful under the President's Article II powers. He said that three factors influenced his decision to implement the Authority. First, NSA would do exactly what the Authorization stated and "not one electron or photon more." Second, the Program was simply an expansion of existing NSA collection activities. Third, the periodic renewal of the Authorization would ensure that the threat continued to justify the Program.

~~(TS//SI//NF)~~ General Hayden said that as time passed, he determined that the Program was still needed. Specifically, he and NSA's Deputy Director reviewed the DCI threat memorandum for each reauthorization and judged that the threats continued to justify the Program.

~~(TS//SI//NF)~~ General Hayden said that no one at NSA expressed concerns to him or the NSA IG that the Authorization was not lawful. Most importantly, General Hayden said that no one outside NSA asserted that he should stop the Program. He occasionally heard concerns from members of Congress, but he sensed general support for the Program from those he briefed outside NSA. He emphasized that he did not just "flip through slides" during briefings. He wanted to ensure that attendees understood the Program; consequently, briefings lasted as long as the attendees wanted.

(U) General Alexander

~~(TS//STLW//SI//OC/NF)~~ When Lieutenant General Keith B. Alexander became NSA/CSS Director in mid-2005, some of the more controversial legal questions surrounding the Authorization had been settled. [redacted] the Office of Legal Counsel had

reviewed its initial opinion and determined that the remaining three types of collection were legally supportable.

(U) NSA Office of General Counsel

~~(TS//SI//NF)~~ After the Authorization was signed on 4 October 2001, NSA's highest ranking attorneys, the NSA General Counsel and Deputy General Counsel, as well as the Associate General Counsel for Operations, orally advised General Hayden that the Authorization was legal

(U) General Counsel

~~(TS//SI//NF)~~ After having received the Authorization on 4 October 2001, General Hayden asked NSA General Counsel Robert Deitz if it was lawful. Mr. Deitz said that General Hayden understood that the Attorney General had already certified its legality by signing the Authorization, but General Hayden wanted Mr. Deitz's view. Mr. Deitz said that on 5 October he told General Hayden that he believed the Authorization to be lawful. He added that he emphasized to General Hayden that if this issue were before the Supreme Court, it would likely rule, although not unanimously, that the Authorization was legal.

(U) Associate General Counsel for Operations

~~(TS//SI//NF)~~ On 5 October 2001, the General Counsel consulted the Associate General Counsel for Operations at his home by secure telephone. The Associate General Counsel for Operations was responsible for all legal matters related to NSA SIGINT activities. According to the General Counsel, he had not yet been authorized to tell the Associate General Counsel about the PSP, so he "talked around" it and did not divulge details. The Associate General Counsel was given enough information to assess the lawfulness of the concept described, but records show that he was not officially cleared for the PSP until 11 October 2001. On Tuesday, 9 October, he told Mr. Deitz that he believed the Authorization was lawful, and he began planning for its implementation.

(U) Deputy General Counsel

~~(TS//SI//NF)~~ The Deputy General Counsel was cleared for the PSP on 11 October 2001. He reviewed the Authorization with Mr. Deitz and the Associate General Counsel for Operations and also concluded that it was lawful.

(U) Discussions on Legality

~~(TS//SI//NF)~~ OGC attorneys said that their discussions about the Program's lawfulness took into account the severity of the 11 September attacks and the fear that foreign persons were in the United States planning attacks. The NSA attorneys concluded that the Authorization was lawful. Given the following factors, the General Counsel said the Authorization was constitutional and did not violate FISA.

[redacted]

- ~~(S//NF)~~ FISA was not a realistic means of addressing the terrorist threat inside the United States because the process lacked speed and agility.
- (U//~~FOUO~~) The Authorization was a temporary 30-day grant of authority.
- (U//~~FOUO~~) The statute allowed such an exception, or, to the extent that it did not, it was unconstitutional.

~~(TS//SI//NF)~~ The NSA attorneys determined that the President could issue the Authorization through his authority under Article II of the Constitution to perform warrantless electronic surveillance for foreign intelligence purposes outside and inside the United States. This conclusion, they said, was supported by the concurring opinion in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), and appellate cases.[8]

~~(TS//SI//NF)~~ The Congressional *Authorization of Use of Military Force* and the canon of constitutional avoidance, which requires a court to attempt to interpret issues so as to avoid constitutional questions, cemented OGC's belief that the President's interpretation of Article II authority had legal merit.

---

[8](U) *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v Buck*, 548 F.2d 871 (9th Cir. 1977); *Zweibon v. Mitchell*, 516 F.2d 594 (DC Cir. 1975); *United States v. Brown* 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied*, 419 U.S. 881 (1974).

~~(TS//SI//NF)~~ The Associate General Counsel for Operations described his position:

> ~~(TS//SI//NF)~~ Does Congress have the authority to limit Presidential Article II authority in foreign intelligence collection? Given the threat, this was a perfect storm of events—3,000 people killed, airplanes and buildings destroyed by foreign terrorists, an attack in the United States by a foreign terrorist organization. No one knew where the terrorists were or if there were more terrorists, and NSA had a collection capability unable to function because with the FISA, you cannot get [redacted] FISA orders needed to cover what you needed covered at that time to look for the terrorists. You go to the President and tell him that there is a statute that prevents you from doing something from a collection standpoint that may protect the United States from a future attack and that while the country is in danger, I have to adhere with a statute and can't get the amount of warrants I need. Any president is going to say there has got to be a way to do this – a federal law can't let me stand here and watch the country go down the tubes. Does the President have to abide by a statute depriving him of his authority and watch the country go down the tubes? Given the case law of five different circuits with the Supreme Court denying certiorari in two cases, there was good basis for deciding this.

~~(TS//SI//NF)~~ NSA OGC attorneys said that they did not prepare a formal written legal opinion because it was not necessary. The Attorney General had already certified the legality of the Program, and General Hayden had not asked for a written legal opinion. The attorneys also said that they did not have time to prepare a written legal opinion given the pace of operations.

~~(TS//SI//NF)~~ After having concluded that the Authorization was lawful, NSA attorneys believed it was important to ensure that NSA's implementation of the Program complied with the Authorization, that processes were well documented, and that strict controls and due diligence were embedded into the execution of the Program. Recognizing that the legal basis of the Program might become controversial, they said that they wanted to ensure that NSA's execution of the Authority would withstand scrutiny.

This page intentionally left blank.

[redacted]

~~(TS//STLW//SI//OC/NF)~~ *NSA PSP operations began on 6 October 2001 and ended on 17 January 2007 and involved the collection, analysis, and reporting of two types of information: metadata and content. NSA assumed that the PSP was temporary and did not immediately formalize processes and procedures for operations, which were quickly set up to provide SIGINT on terrorist targets. As the Authorization continued to be renewed, NSA implemented special procedures to ensure that selectors used for metadata analysis and domestic selectors tasked for content collection were linked to al-Qa'ida, its associates, or international terrorism and that related decisions were documented. NSA did not target communications with both ends in the United States under PSP authority, although some of these communications were incidentally collected, and the OIG found no intentional violations of the Authorization. Over the life of the Program, NSA issued more than [redacted] products based on PSP data. According to senior NSA leaders, the value of the PSP was that SIGINT coverage provided confidence that someone was looking at the seam between the foreign and domestic intelligence domains to detect and prevent attacks in the United States.*

(U) NSA Begins PSP Operations

~~(S//NF)~~ On 4 October 2001, General Hayden received the initial Authorization and informed the SIGINT Director and other key personnel.

[redacted]

[redacted]

[9] ~~(S//NF)~~ A permanent cover term, STELLARWIND, was assigned to Program information on 31 October 2001.

[10] ~~(S//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ **Authorization Renewed**

~~(S//NF)~~ NSA leaders assumed the PSP would be temporary, so they did not establish processes and procedures for a long-term program, and they had plans to cease operations if the Authorization was not renewed. However, the President continued to renew the Authorization, and General Hayden stated that the DCI threat memoranda accompanying each renewal continued to justify the Program.

(U) FISA Authority Still not an Option in 2002

~~(TS//SI//NF)~~ In January 2002, senior NSA leaders still thought that neither the FISA court order process nor the infrastructure associated with FISA collection was suited to large numbers of targets [redacted]

[redacted]

~~(TS//SI//NF)~~ NSA's First Attempt to Obtain FISA Authority on [redacted] Failed.

~~(TS//SI//NF)~~ In September 2002, NSA attempted to obtain FISA authority to collect Internet and electronic wire communications of [redacted] using the standard process for seeking authority on foreign powers and foreign agents. Before preparing an application, NSA submitted a "Memorandum of Justification" to the [redacted][11]

[redacted]

~~(TS//SI//NF)~~ The request was prompted by a CT Product Line staff member, who explained that technical problems delayed NSA's receipt of e-mail collected through FISC orders that the FBI had obtained. [redacted] In one case, an FBI order listed only [redacted] terrorist agents of interest to NSA.

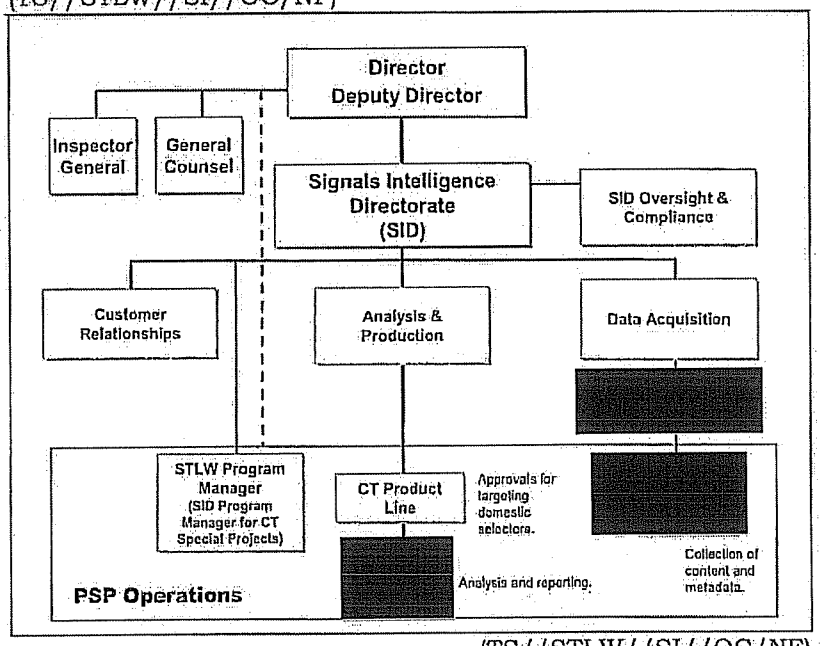
[redacted]

(U) NSA Structure for PSP Operations

[redacted]

(U//~~FOUO~~) NSA Organizational Structure for PSP Activity
November 2004

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



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

(U) Chain of Command

~~(S//NF)~~ NSA's Director and Deputy Director exercised senior operational control and authority over the Program. According to NSA's Deputy Director, General Hayden handled "downtown" and the Deputy Director managed everything within NSA. The SIGINT Director at the start of the Program stated that once she was confident that the Program had appropriate checks and balances, she left direct management to the Director, Deputy Director, and the OGC. She noted that General Hayden took personal responsibility for the Program and managed it carefully. By 2004, specific roles related to collection, analysis, and reporting had been delegated to the SIGINT Director, who delegated management responsibilities to the Program Manager and mission execution responsibilities to the Chief of the CT Product Line and subordinate leaders.

[redacted]

[redacted]

(U) Coordination with FBI

~~(TS//STLW//SI//OC/NF)~~ On 24 January 2003, NSA, SID, and the FBI agreed to detail FBI personnel working under NSA SIGINT authorities to SID's [redacted] Under the agreement, detailees assisted with terrorism-related SIGINT metadata analysis, identified and disseminated terrorism-related SIGINT information meeting FBI foreign intelligence information needs, and facilitated NSA analyst access to FBI terrorism-related information.

[redacted]

(b)(1), (b)(3)

[redacted]

~~(TS//SI//NF)~~ Minimization Procedures and Additional Controls on PSP Operations[12]

~~(TS//STLW//SI//OC/NF)~~ Management emphasized that the minimization rules required under non-PSP authorities also applied to PSP. The Authorization specifically directed NSA to "minimize the information collected concerning American citizens, to the extent consistent with the effective

[12](U) Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations.

accomplishment of the mission of detection and prevention of acts of terrorism within the United States." NSA complied by applying USSID SP0018 minimization procedures. For example, and as described in the following sections:

- The collection of U.S. person information was minimized by [redacted] (b)(1), (b)(3)

- When analysts encountered U.S. person information, they handled it in accordance with minimization guidance, which included reporting violations or incidents.

- Dissemination of U.S. person information was minimized by requiring pre-release verification that the information was related to counterterrorism and necessary to understand the foreign intelligence or assess its importance.

~~(C//NF)~~ In addition, as PSP operations stabilized and the Authorization continued to be renewed, NSA management designed processes and procedures to implement the Program effectively while ensuring compliance with the Authorization and protecting U.S. person information. By April 2004, formal procedures were in place, many of which were more stringent than those used for non-PSP SIGINT operations. One analyst commented that the PSP "had more documentation than anything else [she] had ever been involved with." Examples of controls, some of which will be explained in more detail in the following sections of this report, include:

- ~~(TS//STLW//SI//OC/NF)~~ Approvals—Shift Coordinators approved foreign and domestic target selectors for metadata analysis. The Chief or Deputy of CT Product Line Chief or the Program Manager approved domestic selectors for content collection under the PSP.

- ~~(TS//STLW//SI//OC/NF)~~ Documentation—RFIs, leads, tasked domestic selectors, and tippers were tracked in the [redacted] Justifications for contact chaining were recorded, and justification packages and approvals for tasking domestic selectors for content collection were formally documented.

- ~~(TS//SI//NF)~~ Monitoring—Statistics on content tasking and reports were maintained and reviewed by SID, Oversight and Compliance by 2003. A CT Product Line employee stated: "... [N]owhere else did NSA have to report on selectors and how many selectors were rolled off [detasked] and why."

- (U//~~FOUO~~) OGC involvement—Personnel working under PSP authority noted that they had a continuous dialogue with the OGC on what was permissible under the Authorization. The Associate General Counsel for Operations confirmed that the OGC "was involved with the operations people day in and day out."

- (U//~~FOUO~~) Due Diligence Meetings—The PSP Program Manager chaired due-diligence meetings attended by operational, OIG, and OGC personnel. They discussed OIG and OGC reviews and Program challenges, processes, procedures, and documentation.

~~(TS//SI//NF)~~ PSP Operations: Metadata

~~(TS//STLW//SI//OC/NF)~~ The Authorization defines "metadata" as "header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication." For example, e-mail message metadata includes the sender and recipient e-mail addresses. It does not include the subject line or the text of the e-mail, which are considered content. Telephony metadata includes such information as the calling and called telephone numbers, but not spoken words.

b(3)

[redacted]

[redacted]

~~(TS//SI//NF)~~ Process to Conduct Metadata Analysis

(b)(3)

[redacted]

~~(TS//SI//NF)~~ Standards for Conducting Metadata Analysis

~~(TS//SI//NF)~~ During an OIG review in 2006, the Associate General Counsel for Operations described OGC's standards for complying with the terms of the Authorization when conducting metadata analysis and contact chaining.

~~(TS//SI//NF)~~ To conduct contact chaining under the PSP, the Authorization required that NSA meet one of the following conditions: 1) at least one party to the communication had to be outside the United States, 2) no party to the communication could be known to be a U.S. citizen, or 3) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there were specific and articulable facts giving reason to believe that the communication relates to international terrorism or activities in preparation therefor. The Associate General Counsel for Operations said that OGC's guidance was more stringent than the Authorization in that the OGC always required that the third condition be met before contact chaining began. Analysts were required to establish a link with designated groups related to international terrorism, al-Qa'ida, or al-Qa'ida affiliates.[14]

~~(S//NF)~~ The Associate General Counsel for Operations said that establishing a link to international terrorist groups or al-Qa'ida and its affiliates met the Authorization's requirement that all activities conducted under the PSP be for the purpose of detecting and preventing terrorist acts within the United States. He explained that because the President had determined that specified international terrorist groups and al-Qa'ida presented a threat within the United States, regardless of where members were located, linking a target selector to such groups established that the collection was for

---

[13](U) Smith v. Maryland, 442 U.S. 735, 742 (1979).

[14]~~(TS//SI//NF)~~ In March and April 2004, authorization language for bulk and Internet metadata and content narrowed from "international terrorism, or activities in preparation therefor," to Al-Qa'ida, a group affiliated with Al-Qa'ida, or another group that the President determined was in armed conflict with the United States and posed a threat of hostile action within the United States.

the purpose of detection and prevention of terrorist acts within the United States.

~~(TS//SI//NF)~~ In a 2005 Program memorandum, NSA OGC defined the NSA standard for establishing a link to al-Qa'ida under the PSP. NSA could target selectors when "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe a party to such communication is an agent of al-Qa'ida, or a group affiliated with al-Qa'ida."

> ~~(TS//STLW//SI//OC/NF)~~ Facts giving rise to "reasonable grounds for belief" means reliable facts in NSA's possession, either derived from its signals intelligence activity, or facts provided to NSA by another government department or agency, or facts reliably in the public record (e.g., a newspaper article). Whatever the source of information, the key is that NSA is basing its determination on articulable facts, not on bare assertions made by someone else. We need evidence, rather than conclusions. Thus a mere statement that person X is a member of al Qaeda, without more information, will not suffice as a justification for chaining or for content tasking. Instead we need to know what facts have led NSA, or another agency, or the press, etc., to that conclusion. Focus on the facts and determine whether they lead to a conclusion, rather than accepting someone else's conclusion. If you don't have enough facts to make a determination, ask for them.
>
> ~~(TS//STLW//SI//OC/NF)~~ In addition, the standard does not require certain knowledge, or even necessarily a better than 50/50 chance that the user of a phone or e-mail is a member of al Qaeda or an affiliated organization. It requires only that a reasonable and prudent person exercising good judgment would conclude that there are grounds for believing the thing to be proved. It is not mere hunch or mere suspicion, nor is it proof beyond a reasonable doubt or even a preponderance of the evidence; rather, the standard requires some degree of concrete and articulable evidence or information on which to base a conclusion.

(U) Approvals for Metadata Analysis

[redacted]

[redacted]

~~(TS//SI//NF)~~ If the standard for establishing a link to al-Qa'ida could not be met based solely on the information provided in the RFI or lead, analysts could search NSA and Intelligence Community databases and chain under non-PSP authorities to find additional facts to substantiate the link.

~~(TS//SI//NF)~~ Shift coordinators were not required to approve all alert-list selectors that might have generated [redacted] chaining. One individual, the equivalent of a shift coordinator, managed and monitored the alert process.

~~(TS//SI//NF)~~ When NSA personnel identified erroneous metadata collection, usually caused by technical collection system problems or inappropriate application of the Authorization, minimization procedures required them to report the violation or incident through appropriate channels and to delete the collection from all NSA databases. Early in the Program, NSA reported three violations in which the Authorization was not properly applied and took measures to correct them.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA chained on numbers associated with [redacted] In this case, the target was foreign, but there was no link to terrorism.

- (TS//STLW//SI//OC/NF) In [redacted] NSA chained on a domestic telephone number provided by the FBI that was related to a [redacted] investigation. In this case, the target posed a terrorist threat inside the United States, but there was no known link to international terrorism.

- (TS//STLW//SI//OC/NF) In [redacted] NSA chained on metadata based on two telephone numbers provided by FBI related [redacted] While the selectors were associated with international terrorism, [redacted] did not pose a threat of terrorist attacks inside the United States.

(TS//SI//NF) Bulk Metadata Needed for Effective Contact Chaining

(TS//STLW//SI//OC/NF) Effective contact chaining requires large amounts of metadata, sometimes called bulk metadata, because more data yields more complete chains. [redacted]

(TS//STLW//SI//OC/NF) Under PSP authority, NSA obtained a daily average of approximately [redacted] telephony metadata records and an estimated [redacted] Internet metadata records. Metadata obtained under PSP authorities was stored in a protected database, to which only cleared and trained personnel were given access. NSA analysts were able to access and chain through metadata records, but they could view only records associated with an approved foreign intelligence target. This was a small fraction of the metadata available. For example, in August 2006, NSA estimated that only 0.000025 percent or one in every four million archived bulk telephony records was expected to be viewed by trained SIGINT analysts.[15]

---

[15] (TS//SI//NF) This estimate was presented in the August 2006 application for the Business Records Order, the FISC Order that permitted NSA's collection of call detail records. Although this estimate applies to collection and analysis of telephony metadata conducted under the Business Records Order, the same processes and

~~(TS//SI//NF)~~ PSP Operations: Content

~~(TS//STLW//SI//OC/NF)~~ (b)(3) [redacted] PSP content operations involved three separate activities: tasking selectors for content collection, collecting the content of communications associated with tasked selectors, and analyzing the content collected. To comply with the Authorization, NSA management combined standard minimization procedures and specially designed procedures to task domestic selectors, collect the resulting communications, and analyze and report the foreign intelligence they contained. Over the life of the Program, NSA tasked approximately (b)(1), [redacted] foreign and domestic selectors for content collection.

~~(TS//SI//NF)~~ *Tasking Selectors for Content Collection*

~~(TS//STLW//SI//OC/NF)~~ "Tasking" is the direct levying of SIGINT collection requirements on designated collectors. Analysts must task selectors to obtain a target's communications.

~~(TS//STLW//SI//OC/NF)~~ Under the PSP, (b)(1), (b)(3) [redacted] Before NSA personnel tasked target selectors for PSP content collection, the Authorization required that target selectors comply with two criteria. First, they had to determine that "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe a party to such communication is an agent of al Qa'ida, or a group affiliated with al-Qa'ida," as described in guidance issued by OGC in 2005. Second, the purpose of the collection had to be the prevention and detection of terrorist attacks in the United States. The OGC provided the same guidance for tasking selectors for content collection as it had for contact chaining. Specifically, because the President had determined that al-Qa'ida presented a threat within the United States, regardless of where its members were located, linking a target selector to designated international terrorist groups or al-Qa'ida and its affiliates, established that the collection was for the purpose of detection and prevention of terrorist acts within the United States.

---

techniques were used under the PSP, making this a reasonable comparison. This estimate was based on data available in August 2006 and cannot be replicated.

~~(TS//SI//NF)~~ Approvals to Task Domestic Selectors for Content Collection

~~(TS//SI//NF)~~ NSA analysts determined whether foreign selectors met the Authorization criteria and tasked them without further approval. However, because NSA leadership considered selectors located in the United States to be extremely sensitive, the associated tasking process required extra documentation, reviews, and approvals than foreign selector tasking under the PSP.

[redacted]

[redacted]

[16](U) From 2005 to 2007, SID, Analysis and Production leadership titles changed. The Primary Production Center Manager became the primary approval authority for tasking packages.

[redacted]

~~(TS//SI//NF)~~ **Most Selectors Tasked for Content Collection Were Foreign.**

[redacted]

~~(TS//STLW//SI//OC/NF)~~ In 2008, NSA reported to a member of Congress that [redacted] domestic telephone numbers and [redacted] domestic Internet addresses were tasked for PSP content collection from October 2001 to January 2007. Domestic selectors were located in the United States and associated with al-Qa'ida or international terrorism and were not necessarily used by U.S. citizens. In a 2008 Attorney General Certification, NSA reported that [redacted] foreign telephone numbers and in excess of [redacted] foreign Internet addresses had been targeted from October 2001 through December 2006, which spans all but one month of the Program. NSA could not precisely estimate the number of

foreign Internet addresses targeted because the tools used by analysts before September 2005 did not accurately account for the number of individual addresses targeted.

~~(TS//SI//NF)~~ In 2006, the OIG Found that Justifications for Tasking Domestic Selectors Met Authorization Criteria.

~~(TS//STLW//SI//OC/NF)~~ During a 2006 review, the OIG found that all items in a randomly selected sample of tasked domestic selectors met Authorization criteria. Based on a statistically valid sampling methodology, the OIG was able to conclude with 95 percent confidence that 95 percent or more of domestic selectors tasked for PSP content collection could be linked to al-Qa'ida, its associates, or international terrorist threats inside the United States. Justification packages for all sample items tested were supported by one or more of the following types of information:

[redacted]

- Information associated with or obtained through FBI investigations.

(U) Process to Task Selectors

[redacted]

[redacted]

~~(TS//SI//NF)~~ In 2005, the OIG found that the largely manual process to task and detask selectors for content collection was unreliable. Specifically, the OIG found [redacted] errors when comparing records of domestic telephone numbers and Internet identifiers approved for PSP content collection as of November 2004 with those actually on collection. The errors consisted of selectors that had not been removed from collection after being detasked, had not been put on collection after having been approved, had been put on collection because of a typographical error, or had not been accurately recorded in the [redacted] In response to the OIG finding, management took immediate steps to correct the errors and set up a process to reconcile approved tasked selectors with selectors actually on collection.

~~(TS//SI//NF)~~ Collecting the Content of Communications

(U//~~FOUO~~) Collection refers to the process of obtaining communications after selectors associated with intelligence targets are tasked for collection at designated sites. Data collected under the PSP was stored in protected partitions in NSA databases. Access to the partitions was restricted to PSP-cleared personnel.

~~(TS//SI//NF)~~ The Authorization required that a collected communication originate or terminate outside the United States. NSA did not intentionally collect domestic communications under the PSP. [redacted] and the CT Product Line to ensure that collected data was as intended and authorized. According to PSP program officials, NSA's [redacted] Its purpose was to collect international communications. However, management stated that:

> There are no readily available technical solutions within the [redacted] to guarantee that no [domestic] calls will be collected. Issues of this kind inevitably arise from time to time in other SIGINT operations, as foreseen by Executive Order 12333, and are thus not peculiar to [the PSP].

~~(S//NF)~~ The Program Management Office identified four ways that NSA might have unintentionally collected non-target data:

- A target could have been correctly tasked using valid selectors, but, in addition to collecting the desired target communications, non-target communications were inadvertently collected.
- A valid target selector could have generated target-specific collection that ultimately proved the target not to be related to al-Qa'ida.
- A technical, human, or procedural error in the target identification or tasking process could have resulted in unintentional collection of communications not related to al-Qa'ida.
- Technical collection system problems could have resulted in unintentional collection of non-al-Qa'ida related targets, even when all steps in the target identification and tasking process had been properly executed.

~~(S//NF)~~ Over the life of the Program, NSA reported [redacted] incidents of unintentional collection of domestic communications and [redacted] incidents in which the wrong selector had been tasked. (See Appendix F for details.) In those cases, personnel followed USSID SP0018 procedures and were given detailed instructions to report the violations or incidents, adjust tasking, and delete collection records from NSA and other databases.

~~(TS//SI//NF)~~ *Analyzing the Content of Collected Communications*

~~(TS//SI//NF)~~ Analysis of content collected under the PSP involved the same practices and techniques used in non-PSP operations. One NSA manager described the PSP as "just one more tool in the analysts' tool kit." [redacted] Collected communications were then transcribed, if necessary, and processed to make them useful for intelligence analysis and reporting. Analysis included not only listening to or reading the contents of a communication, but drawing on target knowledge, coordinating and collaborating with other analysts, and integrating collateral information, metadata, and information from databases and published intelligence

reports to determine whether the communications included foreign intelligence that was timely, unique, actionable, and reportable.

[redacted]

[redacted]

[redacted]

---

[17](U//~~FOUO~~) A serialized report is a formatted intelligence product produced pursuant to USSID CR1400 that has a reference serial number, contains foreign intelligence information derived from SIGINT, and goes to approved users of intelligence.

[18]~~(TS//STLW//SI//OC/NF)~~ NSA issued [redacted] additional reports between 17 January 2007 and December 2008 that were based on analysis of data previously collected under PSP authority.

[redacted]

~~(TS//SI//NF)~~ Metadata Analysis Reports (Tippers)

~~(TS//STLW//SI//OC/NF)~~ Reports based on metadata analysis were referred to as "tippers." [redacted]

b1, b3, b7E

~~(TS//STLW//SI//OC/NF)~~ NSA retained documentation of the analysis, supporting customer request or lead information, and a description of the link to terrorism for tippers based on PSP collection. Documentation of analysis was not retained unless a tipper was written. Counterterrorism personnel updated information in a computer tracking system to reflect the disposition of all metadata analysis requests. From October 2001 through January 2007, NSA issued [redacted] tippers to FBI and CIA:

b1, b3, b7E

- [redacted] tippers were based on Internet metadata analysis.
- [redacted] tippers were based on telephony metadata analysis when telephone numbers had only direct contact (one degree of separation) with a known terrorist as defined by the Authorization.

b1, b3, b7E

- [redacted] tippers were based on more detailed telephony metadata analysis that included contacts with two degrees of separation from known terrorists. b1, b3, b7E
- [redacted] tippers were based on telephony and Internet metadata analysis.

~~(TS//SI//NF)~~ Content Reports

~~(TS//STLW//SI//OC/NF)~~ PSP content reports contained NSA's analysis of communications [redacted] b1, b3, b7E

(U//~~FOUO~~) Protection of U.S. Person Information in Reporting

~~(TS//SI//NF)~~ Before sending PSP reports to customers, NSA removed unnecessary U.S. person information, as required by minimization procedures in *USSID SP0018*. The CT Product Line reviewed PSP reports to ensure that they had been written in accordance with these procedures. SID's Oversight and Compliance office then reviewed PSP reports containing U.S. person information. Oversight and Compliance personnel reviewed U.S. person information in reports, determined if it was necessary to understand the foreign intelligence in the reports, and submitted recommendations for the inclusion of U.S. person information to SID, Chief of Information Sharing Services for final approval. For example, if an individual's name was not necessary to understand the foreign intelligence in the report, the name was deleted or changed to "a U.S. person."

~~(TS//SI//NF)~~ Oversight and Compliance did not review tippers based on metadata analysis. When NSA began to issue tippers based on the content of communications, SID adapted its procedures for the dissemination of U.S. person information. Additional Oversight and Compliance personnel were cleared for the Program to assist with reviews. They gave PSP and other terrorism reporting priority for review over other Agency reporting.

(U) Use of SIGINT Product

~~(TS//SI//NF)~~ As NSA's primary customers for PSP information, [redacted] All products included this statement:

> This information is provided only for intelligence purposes in an effort to develop potential investigative leads. It cannot be used in court proceedings, subpoenas, or for other legal or judicial purposes.

(U//~~FOUO~~) Value of the PSP

~~(TS//SI//NF)~~ Referring to portions of the PSP in 2005, General Hayden said there were probably no communications more important to NSA efforts to defend the nation than those involving al-Qa'ida. NSA collected communications when one end was inside the United States and one end was associated with al-Qa'ida or international terrorism in order to detect and prevent attacks inside the United States. General Hayden stated that "the program in this regard has been successful." During the May 2006 Senate hearing on his nomination to be CIA Director, General Hayden said that, had the PSP been in place before the September 2001 attacks, hijackers Khalid Almihdhar and Nawaf Alhazmi almost certainly would have been identified and located.

~~(TS//SI//NF)~~ In May 2009, General Hayden told us that the value of the Program was in knowing that NSA SIGINT activities under the PSP covered an important "quadrant" (terrorist communications between foreign countries and the United States). This coverage provided confidence that there were "not additional terrorist cells in the United States." NSA's Deputy Director, who was the SID Deputy Director for Analysis and Production on 11 September 2001, echoed

General Hayden's comment: "The value of the PSP was in the confidence it provided that someone was looking at the seam between the foreign and domestic intelligence domains."

~~(TS//SI//NF)~~ The former SID Deputy Director for Data Acquisition said that the possibility of a large terrorist presence in the United States [redacted] The PSP gave NSA a capability to exploit a key vulnerability in terrorists' communications: [redacted] With PSP authority, NSA could collect communications between [redacted] al-Qa'ida [redacted]

~~(TS//STLW//SI//OC/NF)~~ Current NSA Director General Alexander cited SIGINT reporting on [redacted] as the most important SIGINT success of the PSP. NSA analysis of PSP metadata and content collection placed [redacted] General Alexander said, "probably saved more lives" than any other PSP information produced by NSA because the information [redacted]

b1, b3, b6, b7C, b7E

~~(TS//SI//NF)~~ From an operational standpoint, the PSP enabled NSA to:

- Support customers
- Provide SIGINT that contributed to customers' investigative work

[redacted]

(U//~~FOUO~~) Support to Customers

~~(TS//SI//NF)~~ From April 2002 to January 2007, NSA responded to [redacted] and more than [redacted] from FBI. These numbers do not account for requests submitted before NSA began to use an automated tracking system in April 2002.

~~(TS//SI//NF)~~ Based on information obtained under PSP authority, NSA sent [redacted]

and FBI. In the early days of the Program, the FBI said that the large number of tippers from NSA was causing them unnecessary work because agents treated each tipper as a lead requiring action. General Hayden said that NSA's intention was that SIGINT information be added to FBI's knowledge base, not that the FBI act on each piece of information. When NSA realized that it was sending too much data to the FBI, the Agency made appropriate adjustments.

(U//~~FOUO~~) PSP Reporting Contributed to Customers' Investigative Work.

(TS//STLW//SI//OC/NF) [redacted] For example, an FBI briefing dated 4 May 2006 stated that "STELLARWIND continues to provide timely and carefully vetted intelligence to support FBI's investigations in connection with [redacted] operations]."

~~(TS//STLW//SI//OC/NF)~~ [redacted] FBI did not routinely provide feedback on NSA reporting under the PSP, and NSA had no mechanism to track and assess the effectiveness of SIGINT reporting in general or PSP reporting in particular.[19] Tracking PSP contributions was also difficult because customers did not know that [redacted] General Hayden noted that success stories decreased over time as intelligence became more integrated and it became more difficult to attribute success to any one activity.

~~(TS//STLW//SI//OC/NF)~~ The Program Management Office provided the following examples of PSP reporting that helped redirect FBI resources [redacted] viewed as vulnerable to terrorism targeting. The examples also include cases in which NSA provided reporting that contributed to FBI investigations, FBI confidential human sources, FISA warrants, arrests, and convictions.

---

[19] ~~(C//NF)~~ In July 2007, SID initiated a formal effort to assess the effectiveness of its CT efforts. By the fall of 2007, that effort was struggling.

(U) Case Name	(U) PSP Contribution
(b)(1), (b)(3) [redacted]	

b1, b3, b6, b7C, b7D, b7E

(U) Case Name	(U) PSP Contribution
(b)(1); (b)(3)	[redacted]

b1,
b3,
b6,
b7C,
b7E