seeking to use the pen register and trap and trace (PR/TT) devices covered by the application for purposes of 50 U.S.C. § 1842(c)(1).

- A declaration by Tenet describing the threat posed by (b)(1), (b)(3) to the United States.
- A certification from Ashcroft stating that the information likely to be obtained from the PR/TT devices was relevant to an ongoing investigation to protect against international terrorism, as required by 50 U.S.C. § 1842(c).
- A memorandum of law and fact in support of the application.

~~(TS//SI//OC/NF)~~ The objective of the application was to secure authority under FISA to collect (b)(1), (b)(3) bulk Internet metadata (b)(1), (b)(3) DoJ constructed its legal argument for this novel use of PR/TT devices around traditional authorities provided under FISA. (See 50 U.S.C. § 1842(a)(1).) The government argued that the NSA's proposed collection of metadata met the requirements of FISA by noting that the metadata sought comported with the "dialing, routing, addressing, or signaling information" type of data described in FISA's definitions of PR/TT devices. (See 18 U.S.C. § 3127(3) and (4).) The government next argued that the information likely to be obtained from the PR/TT devices was relevant to an ongoing investigation to protect against international terrorism, as certified by the Attorney General under 50 U.S.C. § 1842(c). In support of this "certification of relevance" the government stated that the FBI The government also stated that the NSA needed to collect metadata in bulk to effectively perform contact chaining (b)(1), (b)(3) that would enable the NSA to discover enemy communications. b1, b3, b7E

~~(TS//SI//NF)~~ The application requested that the NSA be authorized to collect metadata (b)(1), (b)(3) The application represented that for most of the proposed collection on it was "overwhelmingly likely" that at least one end of the transmitted communication either originated in or was destined for locations outside the United States, and that in some cases both ends of the communication were entirely foreign. However, the government acknowledged that (b)(1), (b)(3)

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

~~(TS//SI//NF)~~ The application proposed allowing 10 NSA analysts access to the database. The NSA analysts were to be briefed by NSA OGC personnel 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. The application proposed that queries of the Internet metadata archive would be performed when the Internet communication address met the following standard:

> [B]ased 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 (b)(1), (b)(3) [redacted]

~~(TS//SI//OC/NF)~~ The application and supporting documents explained that the NSA intended to use the Internet metadata to develop contact chaining (b)(1), (b)(3) [redacted] The NSA estimated that its queries of the database would generate approximately 400 tips to the FBI and CIA each year. Of these tips, 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)~~ On 14 July 2004, Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order (PR/TT Order) based on her findings that the proposed collection of Internet metadata and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. The PR/TT Order, which granted the government's application in all key respects, approved for a period of 90 days the collection within the United States of Internet metadata (b)(1), (b)(3) [redacted]

~~(TS//SI//NF)~~ The PR/TT Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. The FISC amended the government's proposed querying standard, consistent with 50 U.S.C. § 1842(c)(2), to include the proviso that the NSA may query the database based on its reasonable articulable suspicion that a particular known Internet communication address is associated with (b)(1), (b)(3) [redacted] "provided, however, that an (b)(1), (b)(3) [redacted] believed to be used by a U.S. person shall not be regarded as associated with (b)(1), (b)(3) [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution." Regarding the storing, accessing, and disseminating of the Internet metadata obtained by the NSA, the FISC ordered that the NSA store the information in a manner that ensures it is not commingled with other data, and "generate a log of auditing information for each occasion when the information is accessed, to include the ... retrieval request." The FISC also issued separate orders to (b)(1), (b)(3) [redacted] service providers (b)(1), (b)(3) [redacted] to assist the NSA with the installation and use of the PR/TT devices and to maintain the secrecy of the NSA's activities.

b1, b3, b7E

~~(TS//SI//NF)~~ Several officials told us that obtaining the PR/TT Order was seen as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk Internet metadata collection.

~~(TS//SI//NF)~~ The FISC first renewed the PR/TT Order on (b)(1), (b)(3) and then renewed it by subsequent orders at approximately 90-day intervals. In these renewals, the FISC (b)(1), (b)(3) that it approved with the 14 July 2004 PR/TT Order. Under the PR/TT renewal applications, the scope of authorized queries against the PR/TT database remained limited to queries that concerned (b)(1), (b)(3) b1, b3, b7E

[redacted]

(U) Department of Justice Notices of Compliance Incidents

~~(TS//SI//NF)~~ On (b)(1), (b)(3) DoJ OIPR filed a Notice of Compliance Incidents with the FISC describing certain "unauthorized collection" that had taken place following issuance of the PR/TT Order. (b)(1), (b)(3)

[redacted]

~~(TS//SI//NF)~~ On (b)(1), (b)(3) the FISC issued a Compliance Order stating that the "NSA violated its own proposed limitations." The FISC stated that it was troubled by the duration of the violations, which extended from 14 July through (b)(1), (b)(3) and that the Court was reluctant to issue a renewal of the PR/TT Order as to (b)(1), (b)(3) However, Kollar-Kotelly signed a Renewal Order on (b)(1), (b)(3) allowing the NSA to continue collecting Internet metadata under FISA on terms similar to the original PR/TT Order. (b)(1), (b)(3)

[redacted]

(b)(3)

[redacted]

~~(TS//SI//NF)~~ Telephony Metadata Collection
Transition to Operation Under FISA Authority

~~(TS//SI//NF)~~ Another part of the PSP, bulk collection of telephony metadata, was brought under FISA authority in May 2006. As with Internet metadata, the bulk nature of the telephony metadata collection provided the NSA the ability to conduct contact chaining (b)(1), (b)(3) [redacted]

~~(TS//SI//NF)~~ The transition of bulk telephony metadata collection from Presidential authority to FISA authority relied on a provision in FISA that authorized the FBI to seek an order from the FISC 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 are commonly 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.[18] The "tangible things" sought in this Section 215 application were the telephone call detail records of certain telecommunications service providers.

~~(TS//SI//NF)~~ The timing of the decision in May 2006 to seek a FISC order for the bulk collection of telephony metadata was driven primarily by external events. A 16 December 2005 article in *The New York Times* entitled, "Bush Lets U.S. Spy on Callers Without Courts," described in broad terms the content collection aspect of the PSP. (b)(1), (b)(3) [redacted] On 17 December 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-Qa'ida and related terrorist organizations. On 19 January 2006, DoJ issued its White Paper—"Legal Authorities Supporting the Activities of the National Security Agency Described by the President"—that addressed in an unclassified form the legal basis for the collection activities described in *The New York Times* article and confirmed by the President.

[18] (U) Prior to the enactment of Section 215 of the USA PATRIOT Act, the FISA "business records" provisions were limited to obtaining information about a specific person or entity under investigation and only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities.

~~(TS//SI//NF)~~ According to Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper (b)(1), (b)(3) [redacted] Although *The New York Times* article did not describe this aspect of the PSP, reporters at *USA Today* asked about this aspect of the program in early 2006. Bradbury (b)(1), (b)(3) [redacted] anticipated that a *USA Today* article would attract significant public attention when published. As anticipated, on 11 May 2006, the *USA Today* published the results of its investigation in an article entitled, "NSA Has Massive Database of American Phone Calls."

~~(TS//SI//NF)~~ On 23 May 2006, the FBI filed with the FISC a Section 215 application seeking authority to collect telephony metadata to assist the NSA in finding and identifying members or agents of (b)(1), (b)(3) [redacted] in support of the (b)(1), (b)(3) [redacted] FBI investigations then pending and other IC operations. The application requested an order compelling certain telecommunications companies to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. According to the application, the majority of the telephony metadata provided to the NSA was expected to involve communications that were (1) between domestic and foreign locations, or (2) wholly within the United States, including local telephone calls. The application estimated that the collection would involve the NSA receiving approximately (b)(1), (b) [redacted] call detail records per day.[19] b1, b3, b7E

~~(TS//SI//NF)~~ The application acknowledged that the vast collection would include communications records 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 find (b)(1), (b)(3) [redacted] and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons, by using contact chaining [redacted] (b)(1), (b)(3) [redacted] As was done under the PSP, the call detail records would be entered in an NSA database and analysts would query the data with particular telephone numbers to identify connections with other numbers (b)(1), (b)(3) [redacted] The proposed query standard in the Section 215 application essentially was the same standard applied under the PSP in connection with telephony metadata, and the same standard the FISC authorized in the PR/TT Order for Internet metadata. The Section 215 application also included in the proposed query standard the First Amendment proviso that the FISC added to the PR/TT query standard. b1, b3, b7E

[19] ~~(TS//SI//NF)~~ The actual average amount of telephony metadata collected per day (b)(1), (b)(3) [redacted] call detail records rather than (b)(1), (b) [redacted] estimated in the application.

~~(TS//SI//NF)~~ On 24 May 2006, the FISC approved the Section 215 application, finding that there were reasonable grounds to believe that the telephony metadata records sought were relevant to authorized investigations the FBI was conducting to protect against international terrorism. The FISC Section 215 order incorporated each of the procedures proposed in the government's application relating to access to and use of the metadata, which were nearly identical to those included in the Internet metadata PR/TT Order.

~~(TS//SI//NF)~~ Through March 2009, the FISC renewed the authorities granted in the 24 May 2006 order at approximately 90-day intervals, with some modifications sought by the U.S. government. For example, the FISC granted an August 2006 motion requesting (b)(1), (b)(3) [redacted] Except for these and other minor modifications, the terms of the FISC's grant of Section 215 authority for the bulk collection of telephony metadata remained essentially unchanged from the first approval in May 2006 until March 2009. (b)(1), (b)(3) [redacted] Further, the FISC's Section 215 Orders did not require the NSA to modify its use of the telephony metadata from an analytical perspective. NSA analysts were authorized to query the data as they had under the PSP, conduct metadata analysis, and disseminate the results to the FBI, the CIA, and other customers.

~~(TS//SI//NF)~~ However, the FISC drastically changed the authority contained in its March 2009 Section 215 Order after it was notified in January 2009 that the NSA had been querying the metadata in a manner that was not authorized by the court's Section 215 Orders. Specifically, the NSA, on a daily basis, was automatically querying the metadata with (b)(1), (b)(3) telephone numbers from an alert list that had not been determined to satisfy the reasonable articulable suspicion standard required by the FISC to access the telephony metadata for search or analysis purposes.

~~(TS//SI//NF)~~ On 2 March 2009, the FISC issued an order that addressed the compliance incidents that had been reported in January 2009, the government's explanation for their occurrence, and the remedial and prospective measures being taken in response. The FISC stated its concerns with the telephony metadata 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." Nonetheless, the FISC authorized the government to continue collecting telephony metadata under the Section 215 Orders. The FISC explained that in light of the government's repeated representations that the collection of the telephony metadata is vital to national security, taken together with the court's prior determination that the collection properly administered conforms with the FISA statute, that "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 FISC prohibited the government from accessing the metadata 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." The government may, on a case-by-case basis, request authority from the FISC to query the metadata with a specific telephone number to obtain foreign intelligence. The FISC also authorized the government to query the metadata without court approval to protect against an imminent threat to human life, provided the government notifies the court within the next business day.

~~(TS//SI//NF)~~ Content Collection Transition to Operation Under FISA Authority

~~(TS//SI//NF)~~ The last part of the PSP brought under FISA authority was telephone and Internet communications content collection. As explained below, the effort to accomplish this transition was legally and operationally complex and required an enormous effort on the part of the government and the FISC. The FISC judge who ruled on the initial application approved the unconventional legal approach the government proposed to fit PSP's content collection activities within FISA. However, the FISC judge responsible for considering the government's renewal application rejected the legal approach. This resulted in significant diminution in authorized surveillance activity involving content collection and hastened the enactment of legislation that significantly amended FISA and provided the government surveillance authorities broader than those authorized under the PSP.

[redacted]

~~(TS//SI//NF)~~ The government filed the content collection application with the FISC on 13 December 2006. The application sought authority to intercept the content of telephone and electronic communications of [redacted] The application sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular telephone number or Internet communication address was being used or about to be used by members or agents of a foreign power. In the place of the individualized process, the application proposed that the FISC establish broad parameters for the interception of communications—the groups that can be targeted and the locations where the surveillance can be conducted—and that NSA officials, rather than FISC judges, determine within these parameters the particular selectors to be collected against. [redacted]

[redacted] albeit with FISC review and supervision. The government's approach in the FISA application rested on a broad interpretation of the statutory term "facility" and the use of minimization procedures by NSA officials to make probable cause determinations about individual selectors, rather than have a FISC judge make such determinations.

~~(TS//SI//NF)~~ In short, the government's content application asked the FISC to find probable cause to believe that [redacted] engaged in international terrorism, and that [redacted] Then, within these parameters, NSA officials would make probable cause findings (subsequently reviewed by the FISC) about whether individual telephone numbers or Internet communications addresses are used by members or agents of [redacted] and whether the communications of those numbers and addresses are to or from a foreign country. When probable cause findings were made, the NSA could direct the telecommunications companies to provide the content of communications associated with those telephone numbers and Internet communications addresses.

~~(TS//STLW//SI//OC/NF)~~ On 10 January 2007, Judge Malcolm J. Howard approved the government's 13 December 2006 content application as it pertained to foreign selectors—telephone numbers and Internet communications addresses reasonably believed to be used by individuals outside the United States. The effort to implement the order was a massive undertaking for DoJ and NSA. At the time of the order, the NSA was actively tasking for content collection approximately [redacted] foreign selectors—Internet communications addresses or telephone numbers—under authority of the PSP. Approximately [redacted] of these were filed with Howard on an approved schedule of rolling submissions over the 90-day duration of the order.

~~(TS//SI//NF)~~ However, Howard did not approve the government's 13 December 2006 content application as it pertained to domestic selectors—telephone numbers and Internet communications addresses reasonably believed to be used by individuals in the United States. Howard advised DoJ to file a separate application for the international calls of domestic selectors that took a more traditional approach to FISA. A more traditional approach meant that the facilities targeted by the FISA application should be particular telephone numbers and Internet communication addresses and that the probable cause determination for a particular selector would reside with the FISC. DoJ did this in an application filed on 9 January 2007, which Howard approved the following day. The FISC renewed the domestic selectors order approved by Howard for the final time in [redacted] and it has since expired.

~~(TS//SI//NF)~~ DoJ's first renewal application to extend the foreign selectors authorities was filed on 20 March 2007 with Judge Roger Vinson, the FISC duty judge that week. On 29 March 2007, Vinson orally advised DoJ that he could not approve the application and, on 3 April 2007, he issued an order and Memorandum Opinion explaining the reasoning for his conclusion. Vinson wrote that DoJ'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 Vinson's view, the question was whether probable cause determinations are required to be made by the FISC through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Vinson concluded, based on past practice under FISA and the Congressional intent underlying the statute, that probable cause determinations must be made by the FISC.

~~(TS//SI//NF)~~ Vinson also wrote that he was mindful of the government's argument that the government's proposed approach to foreign selectors was 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 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 FISC must apply the statute's procedures. He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and Internet communications addresses. Vinson rejected this position, stating, "the [FISA] statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States." 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 . . .." Vinson's suggestion was a spur to Congress to consider FISA modernization legislation in the summer of 2007.

~~(TS//STLW//SI//OC/NF)~~ In May 2007, DoJ filed, and Vinson approved, a revised foreign selectors application that took a more traditional approach to FISA. Although the revised approach sought to preserve some of the "speed and agility" the government had under Howard's order, the comparatively laborious process for targeting foreign selectors under Vinson's order caused the government to place only a fraction of the desired foreign selectors under coverage. The number of foreign selectors on collection dropped from abou[redacted] under the January 2007 order to about[redacted] under the May 2007 order. The situation 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 5 August 2007, accomplished this objective by authorizing the NSA to intercept inside 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. The Protect America Act effectively superseded Vinson's foreign

selectors order and the government therefore did not seek to renew the order when it expired on 24 August 2007.

~~(TS//SI//NF)~~ The DOJ IG concluded that several considerations favored initiating PSP's transition from Presidential authority to FISA authority earlier than March 2004, especially as the program became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool. These considerations included PSP's substantial effect on privacy interests of U.S. persons, the instability of the legal reasoning on which the program rested for several years, and the substantial restrictions placed on FBI agents' and analysts' access to and use of program-derived information due to the highly classified status of the PSP. The DOJ IG also recommended that DoJ carefully monitor the collection, use, and retention of the information that is now collected under FISA authority and, together with other agencies, continue to examine its value to the government's ongoing counterterrorism efforts.

(U) IMPACT OF THE PRESIDENT'S SURVEILLANCE PROGRAM ON INTELLIGENCE COMMUNITY COUNTERTERRORISM EFFORTS

(U) Senior Intelligence Community Officials Believe That the President's Surveillance Program Filled an Intelligence Gap

~~(TS//SI//NF)~~ Hayden, Goss, McLaughlin, and other senior IC officials we interviewed told us that the PSP addressed a gap in intelligence collection. The IC needed increased access to international communications that transited domestic U.S. communication wires, particularly international communications that originated or terminated within the United States. However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat. [redacted] During the May 2006 Senate hearing on his nomination to be Director of the CIA, Hayden said that, had 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//OC/NF)~~ According to senior NSA officials, the PSP gave NSA the capability to exploit a key terrorist vulnerability. [redacted] With PSP authority, NSA could collect communications between terrorists in the United States and members of al-Qa'ida [redacted] located in foreign countries. The PSP provided SIGINT coverage at the seam between foreign and

domestic intelligence collection. Hayden cited as an important consequence of the PSP the NSA's ability to collect more

[redacted]

~~(S//NF)~~ Hayden told us that he always felt the PSP was worthwhile and successful. His expectation was that the CIA and the FBI would be customers of program-derived information and integrate it into their respective operations.

[redacted] Hayden told us that the program helped to determine that terrorist cells were not embedded within the United States to the extent that had been feared.

(U) Difficulty in Assessing the Impact of the President's Surveillance Program

~~(S//SI//NF)~~ It was difficult to assess the overall impact of PSP on IC counterterrorism efforts. Except for the FBI, IC organizations that participated in the PSP did not have systematic processes for tracking how PSP reporting was used.

[redacted] We were repeatedly told that the PSP was one of a number of intelligence sources and analytic tools that were available to IC personnel, and that, because PSP reporting was used in conjunction with reporting from other intelligence sources, it was difficult to attribute the success of particular counterterrorism operations exclusively to the PSP.

(U) Impact of the President's Surveillance Program on FBI Counterterrorism Efforts

~~(S//NF)~~ The DoJ IG found it difficult to assess or quantify the impact of the PSP on FBI counterterrorism efforts. However, based on our interviews of FBI managers and agents and our review of documents, we concluded that, although PSP information had value in some counterterrorism investigations, the program generally played a limited role in the FBI's overall counterterrorism efforts. Several officials we interviewed suggested that the program provided an "early warning system" to allow the IC to detect potential

terrorist attacks, even if the program had not specifically uncovered evidence of preparations for such attacks.

(U) FBI Efforts to Assess the Value of the Program

~~(TS//SI//NF)~~ The FBI made several attempts to assess the value of the PSP to FBI counterterrorism efforts. In 2004 and again in 2006, FBI's Office of General Counsel (OGC) attempted to assess the value to the FBI of PSP information. This first assessment relied on anecdotal information and informal feedback from FBI field offices. The 2006 assessment was limited to the aspect of the PSP disclosed in *The New York Times* article and subsequently confirmed by the President, i.e., content collection.

~~(S//NF)~~ The FBI undertook two more efforts to study PSP's impact on FBI operations in early 2006. In both of these statistical studies, the FBI sought to determine what percentage of PSP tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." The FBI considered a tipper significant if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists.

~~(TS//SI//OC/NF)~~ The first study examined a sample of leads selected from the [redacted] tippers the NSA provided the FBI from approximately October 2001 to December 2005. The study found that 1.2 percent of the leads made significant contributions, as defined above. The study extrapolated this figure to the entire population of leads and determined that one could expect to find that [redacted] leads made significant contributions to FBI counterterrorism efforts. The second study, which reviewed all of the [redacted] leads the NSA provided the FBI from August 2004 through January 2006, identified no instances of significant contributions to FBI counterterrorism efforts. The studies did not include explicit conclusions on the program's usefulness. However, based in part on the results of the first study, FBI executive management, including Mueller and Deputy Director John Pistole, concluded that the PSP was "of value." b1, b3, b7E

(U) FBI Judgmental Assessments of the Program

~~(S//NF)~~ We interviewed FBI headquarters and field office personnel who regularly handled PSP information for their assessments of the impact of program information on FBI counterterrorism efforts. The FBI personnel we interviewed were generally supportive of the PSP as "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward". Even though most leads were determined not to have any connection to terrorism, many of the FBI officials believed the mere possibility of a terrorist connection made investigating the tips worthwhile.

~~(S//NF)~~ However, the exceptionally compartmented nature of the program created some frustration for FBI personnel. Some agents criticized PSP reports for providing insufficient details about the foreign individuals allegedly involved in terrorism. Others occasionally were frustrated by the prohibition on using [redacted] information in judicial processes, such as in FISA applications, although none of the FBI field office agents we interviewed could identify an investigation in which the restrictions adversely affected the case. Agents who managed counterterrorism programs at the FBI field offices we visited were critical of the [redacted] project for failing to adequately prioritize threat information and, because of the program's special status, for limiting the managers' ability to prioritize the leads in the manner they felt was warranted by the information. b1, b3, b7E

~~(S//NF)~~ Mueller told us that the PSP was useful. He said the FBI must follow every lead it receives in order to prevent future terrorist attacks and that to the extent such information can be gathered and used legally it must be exploited. He stated that he "would not dismiss the potency of a program based on the percentage of hits." Mueller added that, as a general matter, it is very difficult to quantify the effectiveness of an intelligence program without "tagging" the leads that are produced in order to evaluate the role the program information played in any investigation.

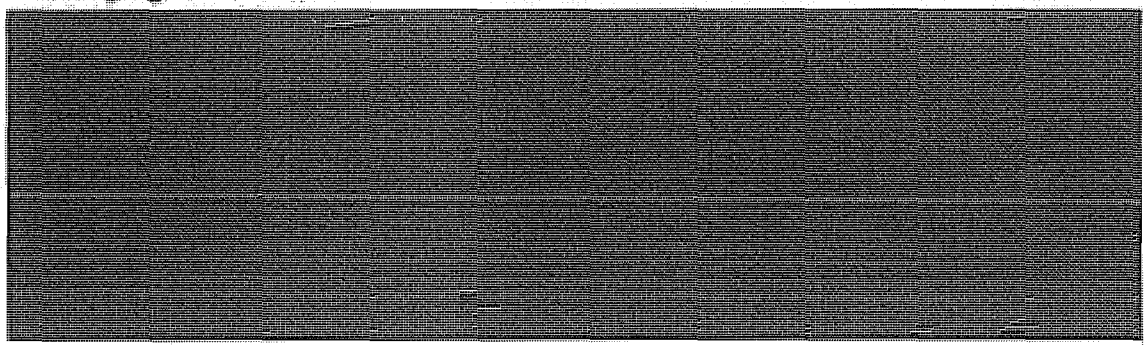
(U) Impact of the President's Surveillance Program on CIA Counterterrorism Operations

(U) The CIA Did Not Systematically Assess the Effectiveness of the Program

~~(S//NF)~~ The CIA did not implement procedures to systematically assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials, including Hayden, told us that PSP reporting was used in conjunction with reporting from other intelligence sources; consequently, it is difficult to attribute the success of particular counterterrorism operations exclusively to the PSP. In a May 2006 briefing to the SSCI, the Deputy Director, [redacted] said that PSP reporting was rarely the sole basis for an intelligence success, but that it frequently played a supporting role. He went on to state that the program was an additional resource to enhance the CIA's understanding of terrorist networks and to help identify potential threats to the homeland. Other [redacted] officials we interviewed said that the PSP was one of many tools available to them, and that the tools were often used in combination.

~~(S//NF)~~ [redacted] However, because there is no means to comprehensively track how PSP information was used, CIA officials were able to provide

only limited information on how program reporting contributed to successful operations, and the CIA IG was unable to independently draw any conclusion on the overall usefulness of the program to CIA.



(U) Several Factors Hindered CIA Utilization of the Program

~~(S//NF)~~ The CIA IG concluded that several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. At the program's inception, a disproportionate number of the CIA personnel who were read into the PSP were senior CIA managers. [redacted] the disparity between the number of senior CIA managers read into PSP and the number of working-level CIA personnel read into the program resulted in too few CIA personnel to fully utilize PSP information for targeting and analysis.

~~(S//NF)~~ [redacted] working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP.

~~(S//NF)~~ CIA officers said that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. There was no formal training on the use of the PSP beyond the initial read in to the program. Many CIA officers we interviewed said that the instruction provided in the read-in briefing was not sufficient and that they were surprised and frustrated by the lack of additional guidance. Some officers told us that there was insufficient legal guidance on the use of PSP-derived information.

~~(S//NF)~~ The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the

program.

[redacted]

(U) Impact of the President's Surveillance Program on NCTC Counterterrorism Efforts

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

~~(S//NF)~~ [redacted] NCTC analysts characterized the PSP as a useful tool, but they also noted that the program was only one of several valuable sources of information available to them. In their view, PSP-derived information was not of greater value than other sources of intelligence. Although NCTC analysts we interviewed could not recall specific examples where PSP information provided what they considered actionable intelligence, they told us they remember attending meetings where the benefits of the PSP were regularly discussed.

(U) Counterterrorism Operations Supported by the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ Our efforts to independently identify how PSP information impacted terrorism investigations and counterterrorism operations were hampered by the nature of these activities, which as previously stated, frequently are predicated on multiple sources of information. Many IC officials we interviewed had difficulty citing specific instances where PSP reporting contributed to a counterterrorism success. The same handful of cases tended to be cited as PSP successes by personnel we interviewed from each of the participating IC organizations and in reports, briefing charts, and other documents we reviewed. b1, b3, b6, b7C, b7E

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

[redacted] These cases, and others identified to us as PSP successes, are discussed below.

~~(TS//STLW//SI//OC/NF)~~ Among the more significant PSP successes was [redacted]

b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~ In [redacted] the FBI arrested [redacted] and [redacted] later pled guilty to [redacted] After [redacted] arrest, [redacted] provided valuable information to the law enforcement and intelligence communities. [redacted]

b1, b3, b6, b7C, b7E

[redacted] NSA Director Alexander cited reporting on [redacted] as the most significant success of the PSP. Alexander said that PSP reporting on [redacted] "probably saved more lives" than any other PSP information produced by NSA.

~~(TS//STLW//SI//OC/NF)~~ An [redacted] tipper, dated [redacted] reported that [redacted] Additional [redacted] reporting, in [redacted] provided telephone contacts between and among [redacted] and several individuals with suspected terrorist ties located in [redacted] The FBI learned more about [redacted] ties to terrorist groups from evidence seized [redacted] evidence gathered through several interviews [redacted] The FBI arrested [redacted] on [redacted] and [redacted] was indicted on [redacted] was convicted on [redacted] on [redacted] and was sentenced to [redacted] prison term. [redacted]

b1, b3, b6, b7C, b7E

- ~~(TS//STLW//SI//OC/NF)~~ In an undated summary of PSP successes, the NSA characterized [redacted] as:

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~ Other examples of PSP successes cited in IC records and briefings include the [redacted] cases.

[redacted] PSP analysis and reporting helped to identify and locate [redacted] who was arrested in [redacted] Subsequent PSP analysis of [redacted] identified [redacted] This information generated several leads for the FBI. b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~ [redacted] According to internal FBI briefing materials, PSP reporting was "instrumental in [redacted] becoming the subject of a Full Investigation [redacted]." However, the FBI's Counterterrorism Division told the DoJ OIG that "no [redacted] reporting factored into [redacted] investigation." [redacted] PSP reporting assisted in locating his network's worldwide associates [redacted] b1, b3, b6, b7C, b7E

[redacted]

[redacted]

(U) ATTORNEY GENERAL GONZALES'S TESTIMONY ON THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) As part of this review, the DoJ IG examined whether Attorney General Gonzales made false, inaccurate, or misleading statements to Congress related to the PSP. Aspects of the PSP were first disclosed publicly in a series of articles in *The New York Times* in December 2005. In response, the President publicly confirmed a portion of the PSP—which he called the terrorist surveillance program—describing it as the interception of the content of international communications of people reasonably believed to have links to al-Qaeda and related organizations. Subsequently, Gonzales was questioned about NSA surveillance activities in two hearings before the Senate Judiciary Committee in February 2006 and July 2007.

~~(S//NF)~~ Through media accounts and Comey's Senate Judiciary Committee testimony in May 2007, it was publicly revealed that DoJ and the White House had a major disagreement related to the PSP, which brought several senior DoJ and FBI officials to the brink of resignation in March 2004. In his testimony before the Senate Judiciary Committee, Gonzales stated that the dispute at issue between DoJ and the White House did not relate to the "Terrorist Surveillance Program" that the President had confirmed, but rather pertained to other intelligence activities. We believe this testimony created the misimpression that the dispute concerned activities entirely unrelated to the terrorist surveillance program, which was not accurate. In addition, we believe Gonzales's testimony that DoJ attorneys did not have "reservations" or "concerns" about the program the "President has confirmed" was incomplete and confusing [redacted] and that these concerns had been conveyed to the White House over a period of months before the issue was resolved.

~~(S//NF)~~ The DoJ IG recognizes that Gonzales was in the difficult position of testifying about a highly classified program in an open forum. However, Gonzales, as a participant in the March 2004 dispute between DoJ and the White House and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need not to be misleading in his testimony. Although we believe that Gonzales did not intend to mislead Congress, we believe his testimony was confusing, inaccurate, and had the effect of misleading those who were not knowledgeable about the program.

(U) CONCLUSIONS

(U) Pursuant to Title III of the FISA Amendments Act of 2008, the Inspectors General of the DoD, the DoJ, the CIA, the NSA, and the ODNI conducted reviews of the PSP. In this report and the accompanying individual reports of the participating IGs, we describe how, following the terrorist attacks of 11 September 2001, the President enhanced the NSA's SIGINT collection authorities in an effort to "detect and prevent acts of terrorism against the United States."

~~(TS//SI//NF)~~ Pursuant to this authority, the NSA, [redacted] collected significant new information, such as the content of communications into and out of the United States, where one party to the communication was reasonably believed to be a member of al-Qa'ida, or its affiliates, or a group the President determined was in armed conflict with the United States. In addition, the President authorized the collection of significant amounts of telephony and Internet metadata. The NSA analyzed this information for dissemination as leads to the IC, principally the CIA and the FBI. As described in the IG reports, the scope of this collection authority changed over the course of the PSP.

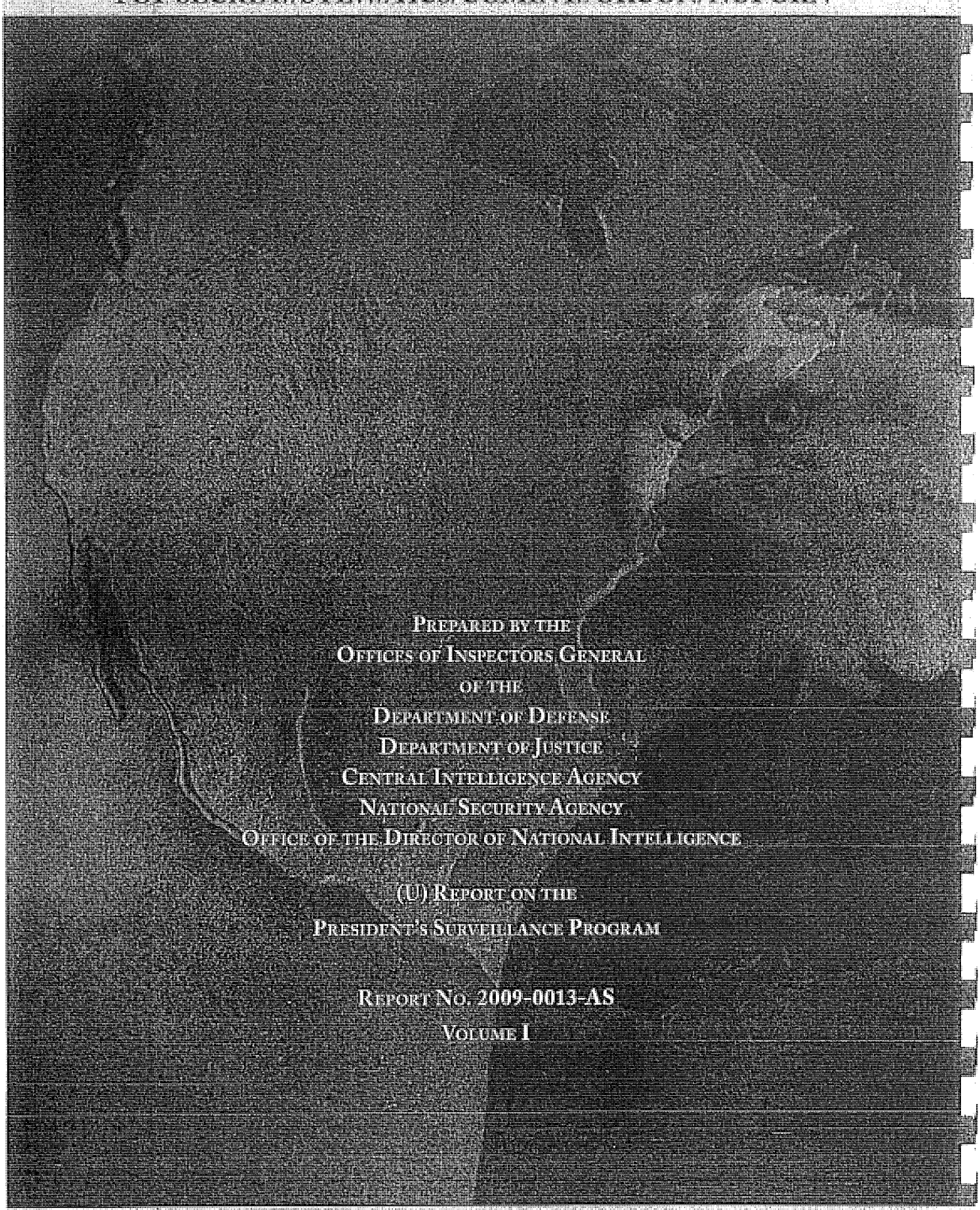
(U//~~FOUO~~) The IG reports describe the role of each of the participating agencies in the PSP, including the NSA's management and oversight of the collection, analysis, and reporting process; the CIA's and FBI's use of the PSP-derived intelligence in their counterterrorism efforts; the ODNI's support of the program by providing periodic threat assessments; and the DoJ's role in analyzing and certifying the legality of the PSP and managing use of PSP information in the judicial process.

(U) The IG reports also describe the conflicting views surrounding the legality of aspects of the PSP during 2003 and 2004, the confrontation between officials from DoJ and the White House about the legal basis for parts of the program and the resolution of that conflict. The ensuing transition of the PSP, in stages, from presidential authority to statutory authority under FISA, is also described in the IG reports.

(U) The IGs also examined the impact of PSP information on counterterrorism efforts. Many senior IC officials believe that the PSP filled a gap in intelligence collection thought to exist under FISA by increasing access to international communications that transited domestic U.S. communication wires, particularly international communications that originated or terminated within the United States. Others within the IC Community, including FBI agents, CIA analysts and managers, and other officials had difficulty evaluating the precise contribution of the PSP to counterterrorism efforts because it was most often viewed as one source among many available analytic and intelligence-gathering tools in these efforts. The IG reports describe several examples of how PSP-derived information factored into specific investigations and operations.

(U) The collection activities pursued under the PSP, and under FISA following the activities' transition to operation under that authority, as described in this report, resulted in unprecedented collection of communications content and metadata. We believe the retention and use by IC organizations of information collected under the PSP and FISA, particularly information on U.S. persons, should be carefully monitored.

This page intentionally left blank.



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS
VOLUME I