Office of the Inspector General
U.S. Department of Justice

Report on the President's Surveillance Program

Volume I

July 2009

(Re-released with some previously redacted information unredacted)

Oversight and Review January 2016

REDACTED – FOR PUBLIC RELEASE

NOTE

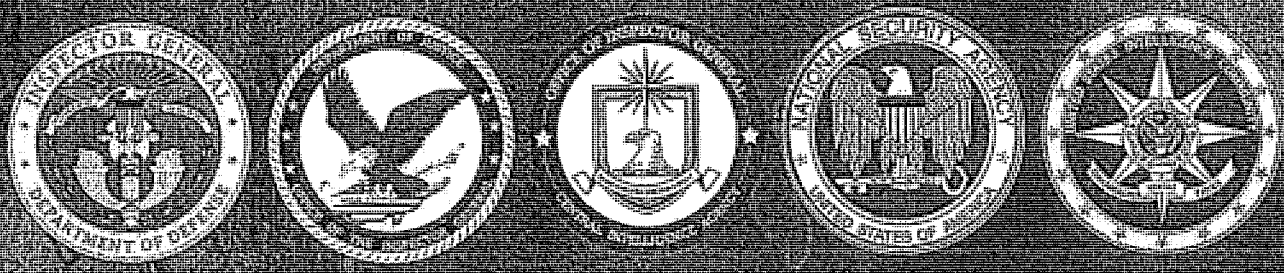
In connection with Freedom of Information Act litigation brought by *The New York Times* in the Southern District of New York, the OIG's July 2009 "Report on the President's Surveillance Program – Volume I" has been re-released with additional information declassified by agencies with the authority to do so. The following pages in this version of the report contain information that was previously redacted:

Volume	Pages
I	27
	53-54

(U) REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME I

10 JULY 2009



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

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-AS

10 July 2009

(U) Preface

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 required the Inspectors General (IGs) of the elements of the Intelligence Community that participated in the President's Surveillance Program (PSP) to conduct a comprehensive review of the Program. The IGs of the Department of Justice (DoJ), the Department of Defense (DoD), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Office of the Director of National Intelligence (ODNI) participated in the review required under the Act. The Act required the IGs to submit a comprehensive report on the review to the Senate Select Committee on Intelligence, the Senate Committee on the Judiciary, the House Permanent Select Committee on Intelligence, and the House Committee on the Judiciary.

(U) Because many aspects of the PSP remain classified, and in order to provide the Congressional committees the complete results of our review, we have prepared this classified report on the PSP. The report is in three volumes:

- Volume I summarizes the collective results of the IGs' review.
- Volume II contains the individual reports prepared and issued by the DoD, CIA, NSA, and ODNI IGs.
- Volume III contains the report prepared and issued by the DoJ IG.

(U) The unclassified report on the PSP required by Title III has been provided to the Congressional committees in a separately bound volume.

Unclassified When Separated
From Attachment

~~Derived From: NSA/CSSM 1-52, 2-400,~~
~~NSA/CSS M 1-52, 12-48~~
~~Dated: 20070108~~
~~Declassify On: 20340713~~

Glenn A. Fine
Inspector General
Department of Justice

Gordon S. Heddell
Acting Inspector General
Department of Defense

Patricia A. Lewis
Acting Inspector General
Central Intelligence Agency

George Ellard
Inspector General
National Security Agency

Roslyn A. Mazer
Inspector General
Office of the Director of
National Intelligence

(U) Table of Contents

(U) The President's Surveillance Program

(U) INTRODUCTION

~~(TS//SI//OC/NF)~~ In response to the terrorist attacks of 11 September 2001, on 4 October 2001, President George W. Bush issued a Top Secret authorization to the Secretary of Defense directing that the signals intelligence (SIGINT) capabilities of the National Security Agency (NSA) be used to detect and prevent further attacks in the United States. The Presidential Authorization stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under certain circumstances. For more than five years, the Presidential Authorization was renewed at 30- to 60-day intervals to authorize the highly classified NSA surveillance program, which is referred to throughout this report as the President's Surveillance Program (PSP).[1]

~~(TS//SI//OC/NF)~~ Under the Presidential Authorizations, the NSA intercepted the content of international telephone and Internet communications of both U.S. and non-U.S. persons. In addition, the NSA collected telephone and Internet metadata—communications signaling information showing contacts between and among telephone numbers and Internet communications addresses, but not including the contents of the communications. [redacted] The content and metadata information was analyzed by the NSA, working with other members of the Intelligence Community (IC), to generate intelligence reports. These reports were sent to the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and other intelligence organizations.

(U) The scope of collection permitted under the Presidential Authorizations varied over time. In stages between July 2004 and January 2007, NSA ceased PSP collection activities under Presidential authorization and resumed them under four separate court orders issued in accordance with the Foreign Intelligence Surveillance Act of 1978 as amended (FISA).[2]

(U) Scope of the Review

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISA Amendments Act)—signed into law on 10 July 2008—required the inspectors

---

[1] ~~(S//NF)~~ The cover term NSA uses to protect the President's Surveillance Program is STELLARWIND.

[2] (U) Unless otherwise indicated, references to FISA in this report are to the statute as it existed prior to being amended in 2008.

general of the elements of the IC that participated in the PSP to conduct a comprehensive review of the program.[3] The Act required that the review examine:

> (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
>
> (B) access to legal reviews of the Program and access to information about the Program;
>
> (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
>
> (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
>
> (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

(U) The Inspectors General (IGs) of the Department of Defense (DoD), the Department of Justice (DoJ), the CIA, the NSA, and the Office of the Director of National Intelligence (ODNI) conducted the review required under the Act. This report summarizes the collective results of the IGs' review. Conclusions and recommendations in this report that are attributed to a particular IG should be understood to represent that IG's opinion. Individual reports detail the results of each IG's review and are annexes to this report. All of the reports have been classified in accordance with the program's classification guide, which was revised during our review and re-issued on 21 January 2009.

(U) Title III of the FISA Amendments Act also required that the report of any investigation of matters relating to the PSP conducted by the DoJ, Office of Professional Responsibility (OPR) be provided to the DoJ IG, and that the findings and conclusions of such investigation be included in the DoJ IG's review. OPR intends to review whether any standards of professional conduct were violated in the preparation of the first series of legal memorandums supporting the PSP. OPR has not yet completed its review or provided its findings and conclusions to the DoJ IG.

(U) Methodology

(U) During the course of this review, the participating IGs conducted approximately 200 interviews. Among the individuals we interviewed were: former White House Counsel and Attorney General Alberto R. Gonzales; former Deputy Attorney General James B. Comey; FBI Director Robert S. Mueller, III; former Secretary of Defense

---

[3] (U) The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on 11 September 2001 and ending on 17 January 2007, including the program referred to by the President in a radio address on 17 December 2005 (commonly known as the Terrorist Surveillance Program).

Donald H. Rumsfeld; former NSA Director, Principal Deputy Director of National Intelligence, and CIA Director Michael V. Hayden; former Director of Central Intelligence (DCI) and CIA Director Porter J. Goss; NSA Director Lieutenant General Keith B. Alexander; former Directors of National Intelligence John D. Negroponte and J. M. McConnell; and former National Counterterrorism Center (NCTC) Director John O. Brennan. Certain other persons who had significant involvement in the PSP either declined or did not respond to our requests for an interview, including former Deputy Secretary of Defense Paul D. Wolfowitz; former Chief of Staff to President Bush Andrew H. Card; David S. Addington, former Counsel to Vice President Richard B. Cheney; former Attorney General John D. Ashcroft; former Deputy Assistant Attorney General John Yoo; and former DCI George J. Tenet.

~~(S//NF)~~ We interviewed former NSA [redacted] as well as leadership [redacted] within the NSA Signals Intelligence Directorate (SID). We interviewed personnel from the CIA [redacted]; senior FBI Counterterrorism Division officials; FBI special agents and intelligence analysts; senior officials from DoJ's Criminal and National Security Divisions; and current and former senior NCTC officials. We also interviewed DoJ officials and office of general counsel officials from the participating organizations who were involved in legal reviews of the PSP and/or had access to the memorandums supporting the legality of the PSP.

~~(S//NF)~~ We examined thousands of electronic and hardcopy documents, including the Presidential Authorizations, terrorist threat assessments, legal memorandums, applicable regulations and policies, briefings, reports, correspondence, and notes. We obtained access to an FBI database of PSP-derived leads that had been disseminated to FBI field offices. We used the database to confirm information obtained through interviews and to assist in our analysis of FBI investigations that utilized PSP information. We evaluated the justifications included in the requests for information (RFIs) submitted by the CIA to the NSA to determine whether they were in accordance with program guidelines. Reports of prior reviews and investigations of the PSP conducted by the NSA IG were also utilized in our review.

(b)(1), (b)(3), (b)(7)(E)

[redacted]

b1,
b3,
b7E

(U) INCEPTION OF THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) National Security Agency Counterterrorism Efforts Prior to 11 September 2001

~~(C//NF)~~ For more than a decade before the terrorist attacks of 11 September 2001, NSA was applying its SIGINT capabilities against terrorist targets in response to IC requirements.[3] The NSA, SID, Counterterrorism (CT) Product Line led these efforts. NSA was authorized by Executive Order (E.O.) 12333, *United States Intelligence Activities*, 4 December 1981, as amended, to collect, process, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes in accordance with DCI guidance and to support the conduct of military operations under the guidance of the Secretary of Defense. It is the policy of U.S. Government entities that conduct SIGINT activities that they will collect, retain, and disseminate only foreign communications. In September 2001, NSA's compliance procedures defined foreign communications as communications having at least one communicant outside the United States, communications entirely among foreign powers, or communications between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA was not authorized under E.O. 12333 to collect communications from a wire in the United States without a court order unless the communications originated and terminated outside the United States or met applicable exceptions to the requirement of a court order under FISA.

(U) FISA, 50 U.S.C. § 1801, et seq., was enacted in 1978 to "provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes." FISA authorizes the Federal Government to engage in electronic surveillance and physical searches, to use pen register and trap and trace devices, and to obtain business records to acquire foreign intelligence information by targeting foreign powers and agents of foreign powers inside the United States.[4] As a general rule, the FISC must first approve an application for a warrant before the government may initiate electronic surveillance.

~~(S//SI//NF)~~ Prior to the PSP, NSA authority to intercept foreign communications included the Director, NSA's authority to approve the targeting of communications with one communicant within the United States if technical devices could be employed to limit collection to communications where the target is a non-U.S. person located outside the United States, [redacted]

[4] (U) The term "pen register" is defined in 18 U.S.C. § 3127 as a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. The term "trap and trace device" is defined in 18 U.S.C. § 3127 as a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

[redacted] If technical devices could not be used to limit collection, the collection required approval by the Attorney General. The Director, NSA could exercise this authority, except when the collection was otherwise regulated, for example, under FISA for communications collected from a wire in the United States.

(U) NSA Initially Used Existing Authorities to Enhance Signals Intelligence (SIGINT) Collection After the September 2001 Terrorist Attacks

~~(TS//SI//NF)~~ On 14 September 2001, NSA Director Hayden used his E.O. 12333 authority to approve a SID CT Product Line request to target [redacted] foreign telephone numbers [redacted] He approved the tasking of the specified numbers, or selectors [redacted] This was an aggressive use of authority because of [redacted] Hayden's 14 September 2001 approval memorandum stated that the purpose of the targeting was to facilitate "dialing analysis/contact chaining."[5] NSA Office of General Counsel (OGC) personnel concurred with the proposed activity, but provided a handwritten note to Hayden stating that chaining was permitted only on foreign numbers, and no U.S. number could be chained without a court order. Collection of the content [redacted] was not addressed in the memorandum. However, other documentation indicates that NSA OGC and SID personnel understood that Hayden also had approved content collection and analysis. NSA OGC personnel told us that Hayden's action was a lawful exercise of his authority under E.O. 12333. In addition, according to NSA's Deputy General Counsel, Hayden had decided by 26 September 2001 that [redacted] would be presumed to be of foreign intelligence value and could be provided to the FBI. Hayden told us that his actions were a "tactical decision" and that he was operating in a unique environment because it was widely believed that more terrorist attacks on U.S. soil were imminent.

~~(S//NF)~~ In late September, Hayden informed Tenet that he had expanded SIGINT operations under E.O. 12333 authority. According to Hayden, Tenet later said that he had explained the NSA's expanded SIGINT operations to Vice President Cheney during a meeting at the White House. On 2 October 2001, Hayden briefed the House Permanent Select Committee on Intelligence on his decision to expand operations under E.O. 12333 and informed members of the Senate Select Committee on Intelligence by telephone.

---

5 (S//SI//NF) Dialing analysis/contact chaining is the process of [redacted] from the communications sent or received by targeted entities.

(U) NSA Explored Options to Improve SIGINT Collection and Address Intelligence Gaps on Terrorist Targets

~~(S//NF)~~ Hayden did not attend the meeting at the White House at which Tenet explained the NSA's expanded SIGINT operations to the Vice President. According to Hayden, Tenet told him that during the meeting the Vice President asked if the IC was doing everything possible to prevent another attack. The Vice President specifically asked Tenet if NSA could do more. Tenet then discussed the matter with Hayden. Hayden told Tenet that nothing more could be done within existing authorities. In a follow-up telephone conversation, Tenet asked Hayden what the NSA could do if it was provided additional authorities. To formulate a response, Hayden met with NSA personnel, who were already working to fill intelligence gaps, to identify additional authorities to support SIGINT collection activities that would be operationally useful and technically feasible. In particular, discussions focused on how NSA might bridge the "international gap," i.e., collection of international communications in which one communicant was within the United States.

(U) In the days immediately after 11 September 2001, the House Permanent Select Committee on Intelligence asked NSA for technical assistance in drafting a proposal to amend FISA to give the President authority to conduct electronic surveillance without a court order to obtain foreign intelligence information. On 20 September 2001, the NSA General Counsel wrote to White House Counsel Gonzales asking if the proposed amendment to FISA had merit. We found no record of a response to the NSA General Counsel's writing and could not determine why the proposal to amend FISA was not pursued at that time.

(U) Hayden said that, in his professional judgment, NSA could not address the intelligence gap using FISA. The process for obtaining FISC orders was slow; it involved extensive coordination and separate legal and policy reviews by several agencies. Although FISA's emergency authorization provision permitted 72 hours of surveillance before obtaining a court order, it did not allow the government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would satisfy the standards articulated in FISA and be acceptable to the FISC.

[redacted]

[redacted]

(U) Impediments to SIGINT Collection Against Terrorist Targets Were Discussed With the White House

~~(S//NF)~~ Hayden recalled that, after consulting with NSA personnel, he discussed with the White House how FISA constrained NSA collection of communications carried on a wire in the United States. Hayden explained that NSA could not collect from a wire in the United States, without a court order, content or metadata from communications that originated and/or terminated in the United States. Hayden also said that communications metadata do not have the same level of constitutional protection as the content of communications and that access to metadata concerning communications having one end in the United States would significantly enhance NSA's analytic capabilities. Hayden suggested that the ability to collect communications that originated or terminated in the United States without a court order would increase NSA's speed and agility. After two additional meetings with Vice President Cheney to discuss further how NSA collection capabilities could be expanded along the lines described at the White House meeting, the Vice President told Hayden to work out a solution with Counsel to the Vice President David Addington.

(U) Authorization of the President's Surveillance Program

~~(TS//SI//NF)~~ According to Hayden, Addington drafted the first Presidential Authorization of the PSP. Hayden characterized himself as the "subject matter expert," and he said that no other NSA personnel, including the General Counsel, participated in drafting the authorization. Hayden also said that DoJ personnel had not been involved in his discussions with Addington concerning Presidential authorization of the PSP. The PSP came into existence on 4 October 2001, when President Bush signed the Presidential Authorization drafted by Addington. The authorization was entitled: *Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States*. Between 4 October 2001 and 8 December 2006, President Bush signed 43 authorizations, exclusive of modifications and other program-related memoranda to the Secretary of Defense.

(U) SIGINT Activities Authorized Under the Program

~~(TS//STLW//SI//OC/NF)~~ The 4 October 2001 Presidential Authorization directed the Secretary of Defense to "use the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance," provided the surveillance was intended to:

(a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which there is probable cause to believe that (b)(1), (b)(3) a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or an agent of such a group; or

(b) acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States or (ii) no party to such communication is known to be a citizen of the United States.

~~(TS//STLW//SI//OC/NF)~~ The first Presidential Authorization allowed NSA to intercept the content of (b)(1), (b)(3) any communication, including those to, from, or exclusively within the United States, where probable cause existed to believe one of the communicants was engaged in international terrorism. The authorization also allowed the NSA to acquire telephony and Internet metadata where one end of the communication was outside the United States or neither communicant was known to be a U.S. citizen. For telephone calls, metadata generally referred to "dialing-type information" (the originating and terminating telephone numbers, and the date, time, and duration of the call), but not the content of the call. For Internet communications, metadata generally referred to the "to," "from," "cc," "bcc," and "sent" lines of a message, but not the "subject" line or content. (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ The Secretary of Defense directed NSA, in writing, on 8 October 2001 to execute the authorization to conduct specified electronic surveillance on targets related to (b)(1), (b)(3) international terrorism.[6] Because the surveillance was conducted in the United States, included (b)(1), (b)(3) communications into or out of the United States, and a subset of these communications was to or from persons in the United States, the surveillance otherwise would have required a FISC order. NSA was also allowed to retain, process, analyze, and disseminate intelligence from communications acquired under the Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ In addition to allowing the interception of the content of communications into or out of the United States, paragraph (a)(ii) of the first Presidential Authorization allowed NSA to intercept the content of purely domestic communications. Hayden told us he did not realize this until Addington specifically raised the subject during

[6] ~~(S//NF)~~ Although the authorization "was not limited to the signals intelligence capabilities of the National Security Agency," DoD's operational involvement in the PSP was limited to activities undertaken by NSA.

a meeting to discuss renewing the authorization. According to Hayden, he told Addington that NSA would not collect domestic communications because NSA is a foreign intelligence agency, its infrastructure did not support domestic collection, and he would require such a high evidentiary standard to justify intercepting purely domestic communication that such cases might just as well go to the FISC.

(U) Content of the Presidential Authorizations and Department of Justice Certification as to Form and Legality

~~(S//NF)~~ Each of the Presidential Authorizations included a finding to the effect that terrorist groups of global reach possessed the intent and capability to attack the United States, that an extraordinary emergency continued to exist, and that these circumstances constituted an urgent and compelling governmental interest permitting electronic surveillance within the United States for counterterrorism purposes, without judicial warrants or court orders. The primary authorities cited for the legality of the electronic surveillance and related activities were Article II of the Constitution and the 18 September 2001 Authorization for Use of Military Force Joint Resolution (AUMF). The authorizations further provided that any limitation in E.O. 12333 or any other Presidential directive inconsistent with the Presidential Authorizations shall not apply, to the extent of the inconsistency, to the electronic surveillance authorized under the PSP. Each authorization also included the President's determination that, to assist in preserving the secrecy necessary to "detect and prevent acts of terrorism against the United States," the Secretary of Defense was to defer notification of the authorizations and the activities carried out pursuant to them to persons outside the Executive Branch. The President also noted his intention to inform appropriate members of the Senate and the House of Representatives of the program "as soon as I judge that it can be done consistently with national defense needs."

~~(S//NF)~~ Ashcroft certified the first Presidential Authorization as to "form and legality" on 4 October 2001. According to NSA records, this was the same day that Ashcroft was read into the PSP. There was no legal requirement that the Presidential Authorizations of the PSP be certified by the Attorney General or other DoJ officials. Former senior DoJ official Patrick F. Philbin told us he thought one purpose of the certification was to give the program a sense of legitimacy so that it not "look like a rogue operation."

[redacted]

Principal Deputy and Acting Assistant Attorney General Steven G. Bradbury told us that the DoJ certifications served as official confirmation that DoJ had determined that the activities carried out under the program were lawful.

~~(S//NF)~~ Gonzales told us that approval of the program as to form and legality was not required as a matter of law, but he believed that it "added value" to the Presidential Authorization for three reasons. First, NSA was being asked to do something it had not done before, and it was important to assure the NSA that the Attorney General had

approved the legality of the program [redacted] Third, for "purely political considerations," the Attorney General's approval of the program would have value "prospectively" in the event of Congressional or inspector general reviews of the program.

(U) The Presidential Authorizations were issued at intervals of approximately 30 to 60 days. Bradbury said that the main reason for periodically reauthorizing the program was to ensure that the Presidential Authorizations were reviewed frequently to assess the program's value and effectiveness. As the period for each Presidential Authorization drew to a close, the DCI prepared a threat assessment memorandum for the President describing the current state of potential terrorist threats to the United States.

(U) The Threat Assessment Memorandums Supporting Presidential Authorization of the Program

~~(S//NF)~~ From October 2001 to May 2003, the CIA prepared the threat assessment memorandums that supported Presidential authorization and periodic reauthorization of the PSP. The memorandums documented the current threat to the U.S. homeland and to U.S. interests abroad from al-Qa'ida and affiliated terrorist organizations. The first threat assessment memorandum—*The Continuing Near-Term Threat from Usama Bin Ladin*—was signed by the DCI on 4 October 2001.[7] Subsequent threat assessment memorandums were prepared every 30 to 60 days to correspond with the President's reauthorizations.

~~(S//NF)~~ The DCI Chief of Staff, John H. Moseman, was the CIA focal point for preparing the threat assessment memorandums. According to Moseman, he directed the CIA, [redacted] to prepare objective appraisals of the current terrorist threat, focusing primarily on threats to the homeland, and to document those appraisals in a memorandum. [redacted] analysts drew upon all sources of intelligence in preparing their threat assessments. Each of the memorandums focused primarily on the current threat situation and did not routinely provide information concerning previously reported threats or an assessment of the PSP's utility in addressing previously reported threats.

~~(S//NF)~~ After [redacted] completed its portion of the memorandums, Moseman added a paragraph at the end of the memorandums stating that the individuals and organizations involved in global terrorism (and discussed in the memorandums) possessed the capability and intention to undertake further terrorist attacks within the United States. Moseman recalled that the paragraph was provided to him initially by either Gonzales or Addington. The paragraph recommended that the President authorize the Secretary of Defense to employ within the United States the capabilities of DoD, including but not limited to NSA's SIGINT capabilities, to collect foreign intelligence by electronic surveillance. The paragraph described the types of communication and data that would be collected and the

[7] (U) The title of the threat assessment memorandums was changed to *The Global War Against Terrorism* in June 2002.

circumstances under which they could be collected. The draft threat assessment memorandums were reviewed by CIA Office of General Counsel attorneys assigned to [redacted] and CIA Acting General Counsel (Principal Deputy General Counsel), John A. Rizzo. Rizzo told us that the draft memorandums were generally sufficient, but there were occasions when, based on his experience with previous memorandums, he thought that draft memorandums contained insufficient threat information or did not present a compelling case for reauthorization of the PSP. In such instances, Rizzo would request that [redacted] provide additional available threat information or make revisions to the draft memorandums.

~~(S//NF)~~ The threat assessment memorandums were then signed by the DCI and forwarded to the Secretary of Defense to be co-signed. Tenet signed most of the threat memorandums prepared during his tenure as DCI. There were no occasions when the DCI or Acting DCI withheld their signature from the threat assessment memorandums. The threat assessment memorandums were reviewed by DoJ's OLC to assess whether there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. OLC then advised the Attorney General whether the constitutional standard of reasonableness had been met and whether the Presidential Authorization could be certified as to form and legality. After review and approval as to form and legality by the Attorney General, the threat assessment memorandums were delivered to the White House to be attached to the PSP reauthorization memorandums signed by the President.

~~(S//NF)~~ Responsibility for drafting the threat assessment memorandums was transferred from [redacted] to the newly-established Terrorist Threat Integration Center in May 2003. This responsibility was retained by TTIC's successor organization, NCTC. The DCI continued to sign the threat assessment memorandums through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence or his designee.

(U) Early Revisions to the Presidential Authorizations

~~(TS//STLW//SI//OC/NF)~~ On 2 November 2001, with the first authorization set to expire, President Bush signed a second Presidential Authorization of the PSP. The second authorization cited the same authorities in support of the President's actions, principally the Article II Commander-in-Chief powers and the AUMF. The second authorization also cited the same findings of a threat assessment concerning the magnitude of potential terrorist threats and the likelihood of their occurrence in the future. However, the scope of authorized content collection and metadata acquisition was redefined in the second Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ The language of the second Presidential Authorization changed in three respects the scope of collection and acquisition authorized under the PSP. First, the "probable cause to believe" standard for the collection of Internet communications and telephone content was replaced with "based on the factual and

practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe . . .." DoJ, Counsel for Intelligence Policy, James A. Baker told us this change was made by Addington because he believed the terms "probable cause" were "too freighted" with usage in judicial opinions. Baker also said he believed the change to more colloquial language was made because the standard was to be applied by non-lawyers at the NSA. Second, the newly defined standard was to be applied to the belief that the communication "originated or terminated outside the United States . . .." The new language therefore eliminated the authority that existed in the first authorization to intercept the content of purely domestic communications.

~~(TS//STLW//SI//OC/NF)~~ The third change in the scope of PSP collection and acquisition contained in the second Presidential Authorization was the inclusion of an additional (third) category of Internet and telephony metadata that could be acquired:

> (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor.

This language represented an expansion of collection authority to include metadata pertaining to certain communications even when both parties were U.S. persons, as long as there were facts giving reason to believe that the communication was related to international terrorism.

~~(TS//STLW//SI//OC/NF)~~ On 30 November 2001, the President signed a third authorization for the PSP. The third Authorization was virtually identical to the second (2 November 2001) authorization. [redacted]

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

~~(TS//STLW//SI//OC/NF)~~ The language in the Presidential Authorization of 9 January 2002 concerning scope of authorized collection and acquisition became the standard for subsequent Presidential Authorizations until the disputed authorization in March 2004, which is discussed later in this report. [redacted]

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

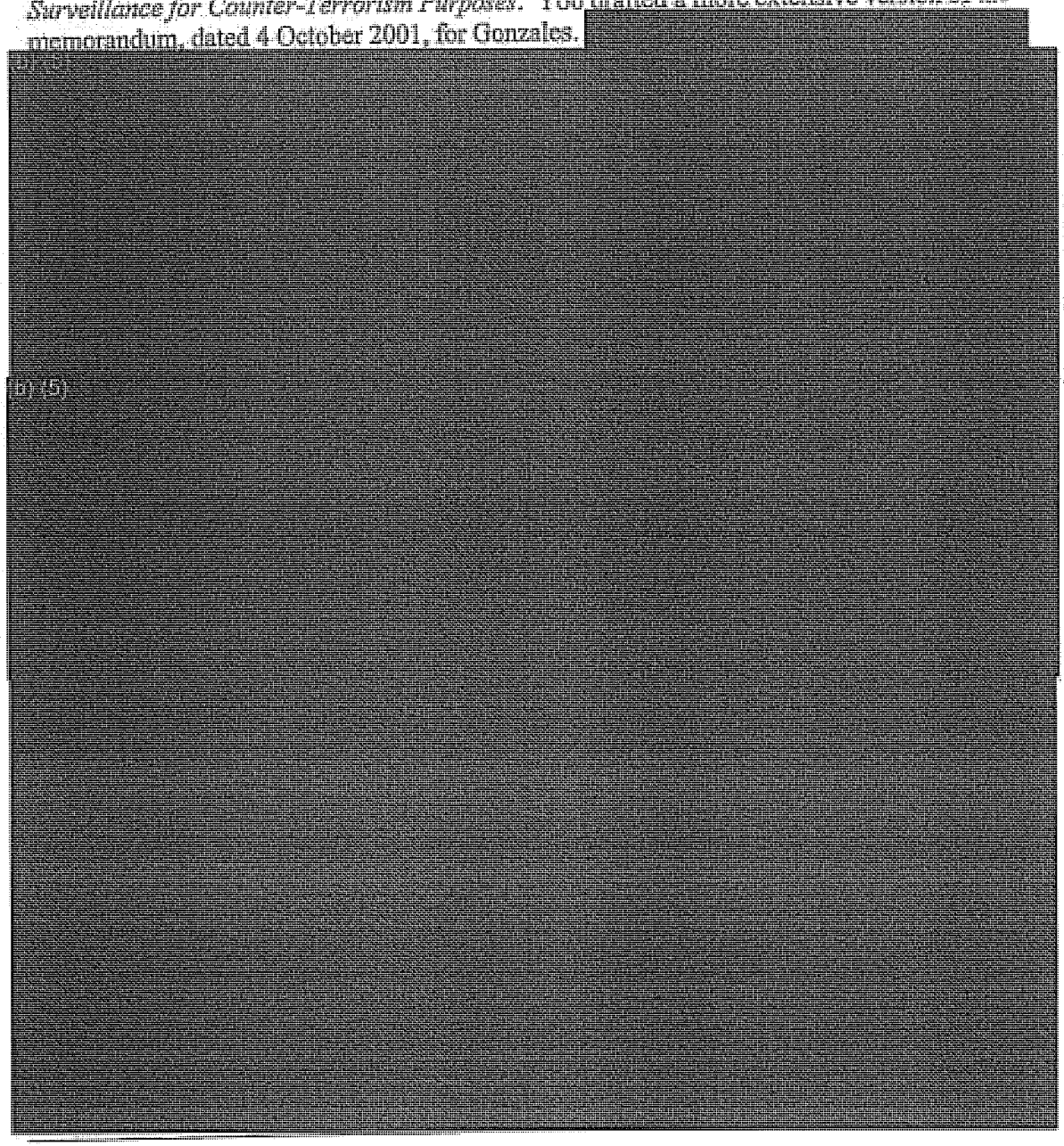
(U) DoJ Office of Legal Counsel Memorandums Supporting Legality of the Program

~~(S//NF)~~ OLC Deputy Assistant Attorney General John Yoo was responsible for drafting the first series of legal memorandums supporting the PSP. Yoo was the only OLC official read into the PSP from the program's inception until he left DoJ in May 2003.

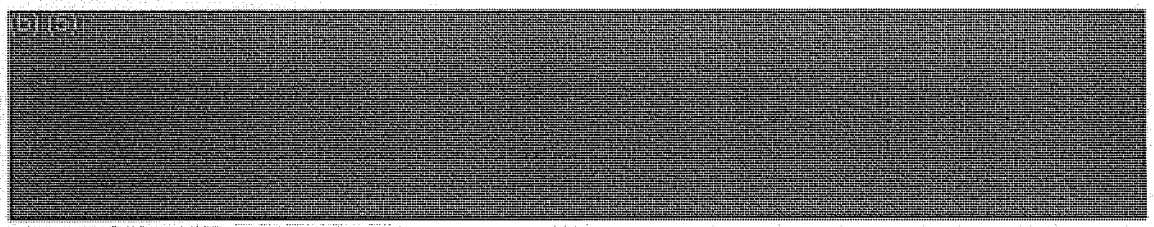
During Yoo's tenure at DoJ, he was one of only three DoJ officials read into the PSP. The other two were Ashcroft and Baker. OLC Assistant Attorney General Jay S. Bybee, Yoo's direct supervisor, was never read into the program.

~~(S//NF)~~ Before the President authorized the PSP on 4 October 2001, Yoo had prepared a memorandum evaluating the legality of a hypothetical electronic surveillance program within the United States to monitor communications of potential terrorists. His memorandum, dated 17 September 2001, was addressed to Deputy White House Counsel Timothy E. Flanigan and was entitled *Constitutional Standards on Random Electronic Surveillance for Counter-Terrorism Purposes*. Yoo drafted a more extensive version of the memorandum, dated 4 October 2001, for Gonzales.

(b) (5)

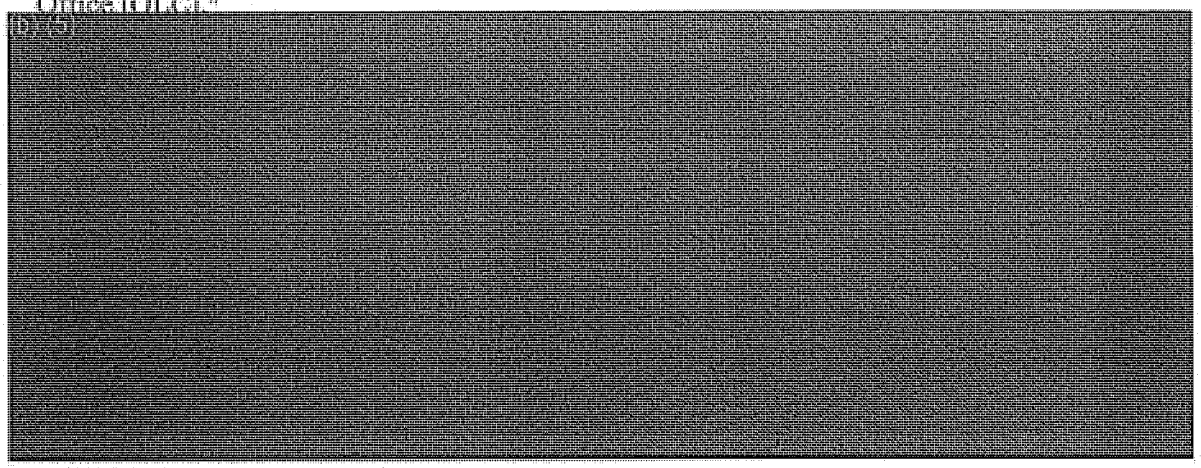


(b)(1)
(b)(3)



~~(S//NF)~~ The first OLC memorandum explicitly addressing the legality of PSP was not drafted until after the program had been formally authorized by the President and after Ashcroft had certified the program as to form and legality. The first OLC opinion directly supporting the legality of the PSP was dated 2 November 2001, and was drafted by Yoo. Yoo acknowledged at the outset of his 2 November memorandum that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]."

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



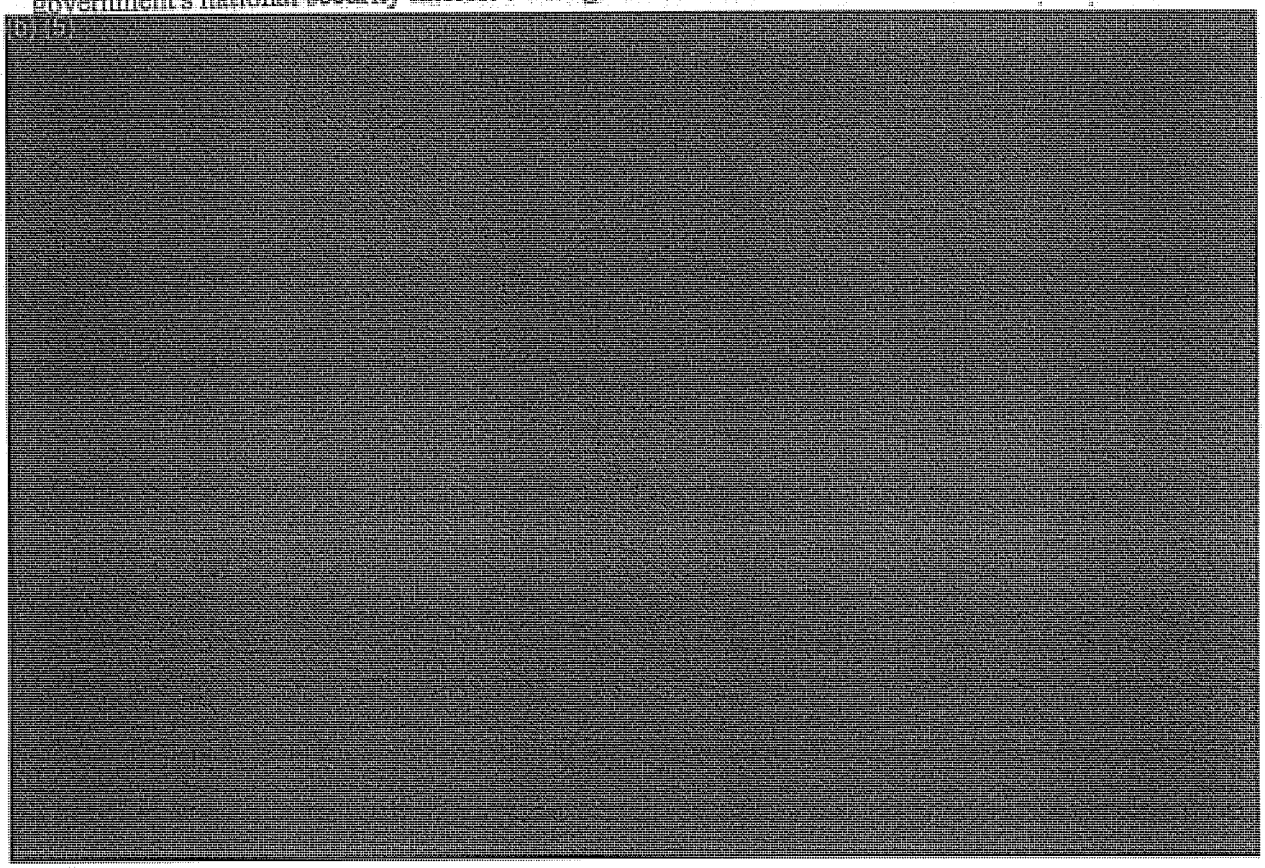
~~(S//NF)~~ Yoo acknowledged in his 2 November 2001 memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence." But Yoo then opined that "[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities." Citing advice of OLC and DoJ's position as presented to Congress during passage of the USA PATRIOT Act several weeks earlier, Yoo characterized FISA as merely providing a "safe harbor for electronic surveillance," adding that it "cannot restrict the President's ability to engage in warrantless searches that protect the national security."

~~(S//NF)~~ Regarding whether the activities conducted under the PSP could be conducted under FISA, Yoo described the same potential impediments that he had cited in his 4 October memorandum. Noting that the Presidential Authorization could be viewed as a violation of FISA's civil and criminal sanctions in 50 U.S.C. §§ 1809-10, Yoo opined that in this regard FISA represented an unconstitutional infringement on the President's Article II powers. According to Yoo, the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA.

~~(S//NF)~~ Yoo wrote that reading FISA to restrict the President's inherent authority to conduct foreign intelligence surveillance would raise grave constitutional questions which, under the doctrine of constitutional avoidance, would require resolving the issue in a manner that preserves the President's (b) (5) "[U]nless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area—which it has not—then the statute must be construed to avoid such a reading."

~~(TS//SI//NF)~~ Yoo's 2 November 2001 memorandum dismissed Fourth Amendment concerns to the extent that the authorized collection involved non-U.S. persons outside the United States. Regarding those aspects of the program that involved interception of the international communications of U.S. persons within the United States, Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing U.S. international borders and that interceptions of communications into or out of the United States fell within the "border crossing exception." Yoo further opined that electronic surveillance in "direct support of military operations" did not trigger constitutional protection against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses. Finally, Yoo wrote that the electronic surveillance described in the Presidential Authorizations was "reasonable" under the Fourth Amendment and therefore did not require a warrant, i.e., in this situation the government's national security interest outweighed the individual's privacy interest.

(b) (5)



~~(TS//SI//NF)~~ In October 2002, at Ashcroft's request, Yoo drafted another opinion concerning the PSP. The memorandum, dated 11 October 2002, reiterated the same basic analysis as Yoo's 2 November 2001 memorandum in support of the legality of the PSP.

(b)(5)

[redacted]

(U) IMPLEMENTATION OF THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) NSA Implementation

~~(S//NF)~~ On 4 October 2001, Hayden received the initial Presidential Authorization of the PSP and briefed the NSA SIGINT Director and other key NSA personnel on the authorization. (b)(3)

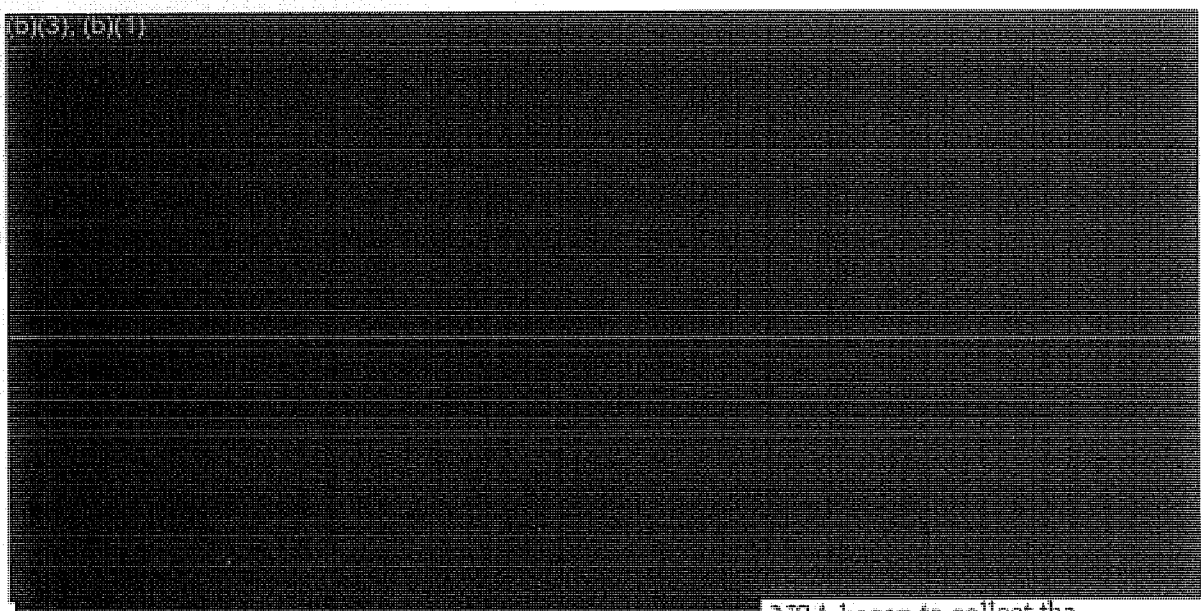
[redacted]

He also said that the NSA General Counsel had reviewed the authorization and concluded that the authorized activities were legal.

(b)(3)

[redacted]

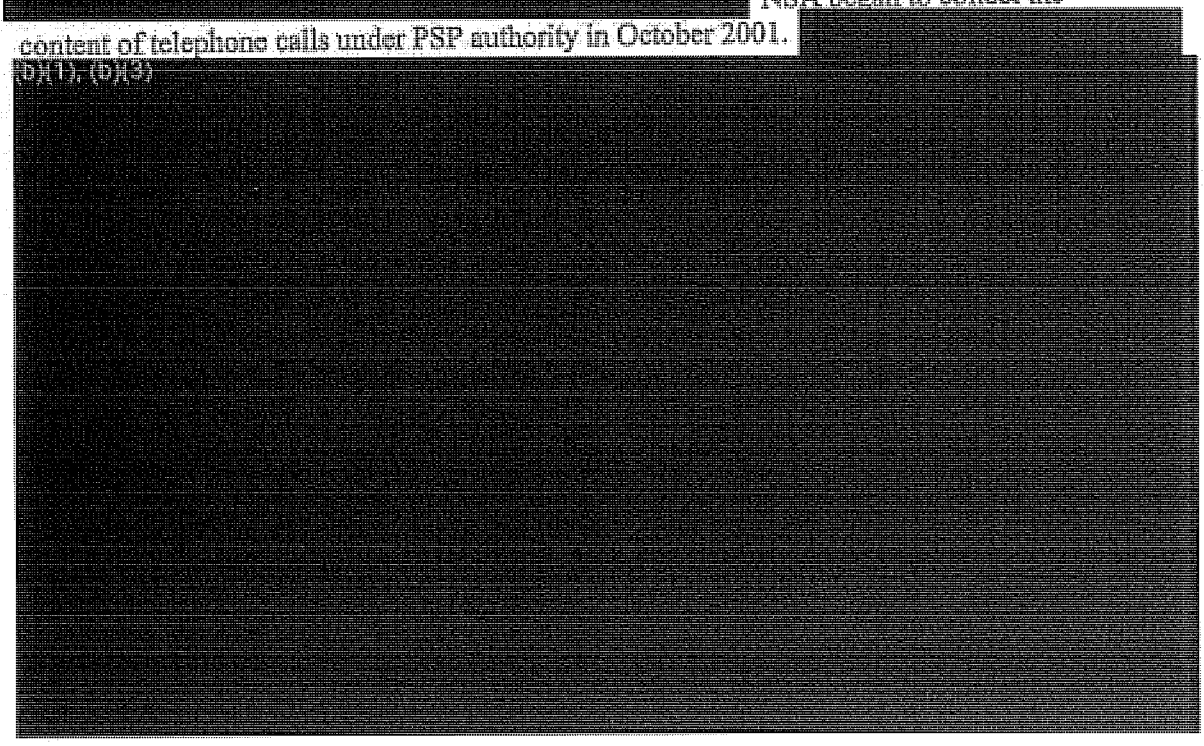
(b)(3), (b)(1)



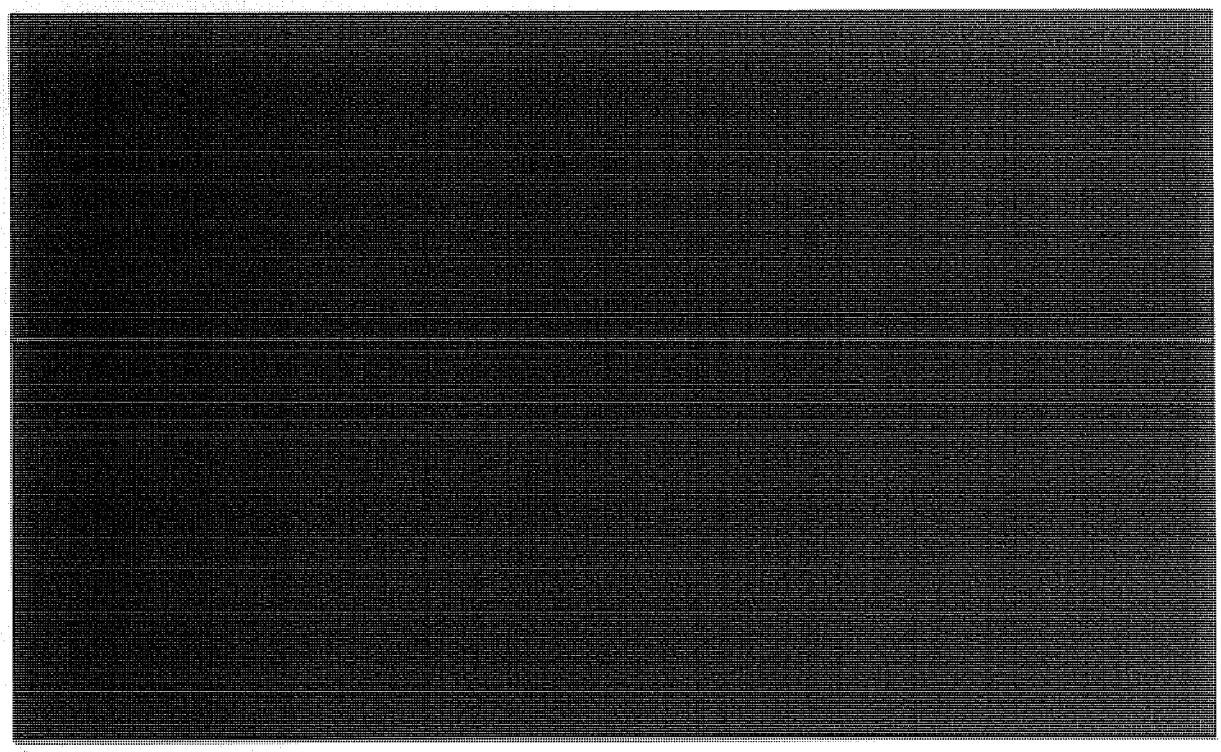
b1,
b3,
b7D,
b7E

NSA began to collect the content of telephone calls under PSP authority in October 2001.

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



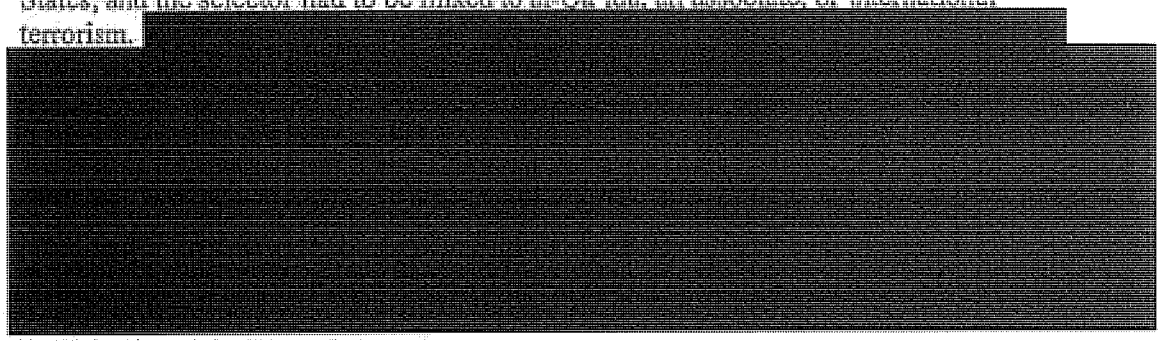
b1,
b3,
b7E



b1, b3, b7E

~~(TS//SI//NF)~~ **Telephone and Internet Communications Content Collection and Analysis**

~~(TS//SI//NF)~~ Content collection and analysis under the PSP was conducted in the same manner as collection and analysis conducted previously by the NSA under E.O. 12333 authority. NSA management applied standard minimization and specially designed procedures to task domestic selectors such as telephone numbers and e-mail addresses. Selectors had to meet two criteria before being tasked under the PSP: the purpose of the collection had to be to prevent and detect terrorist attacks in the United States; and the selector had to be linked to al-Qa'ida, an associate, or international terrorism.



~~(TS//SI//NF)~~ NSA collection managers were responsible for ensuring that telephony and Internet communications selectors were appropriately added or removed from collection. Content collection for domestic selectors was sometimes approved for specific

time periods. Data collected under the PSP were stored in compartmented NSA databases, and access to the databases was strictly controlled.

~~(TS//SI//OC/NF)~~ The majority of targets for content collection under the PSP were foreign telephone numbers and Internet communications addresses. In 2008, NSA reported that [redacted] foreign telephone numbers and in excess of [redacted] foreign Internet communications addresses had been targeted from October 2001 through December 2006. NSA reported in 2008 tha[redacted] domestic telephone numbers and [redacted] domestic Internet communications addresses were targeted for PSP content collection from October 2001 to January 2007. Although targeted domestic telephone numbers and Internet communications addresses were located in the United States, they were not necessarily used by U.S. citizens.

[redacted]

~~(S//NF)~~ PSP program officials told us that the NSA did not seek to collect domestic communications under the PSP. However, NSA managers said that there are no readily available technical means 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, and are not unique to the PSP. Over the life of the program, the NSA reported [redacted] incidents of unintentional collection of domestic communications or non-targeted communications. In such cases, the NSA IG determined that personnel followed established procedures in reporting the incidents, adjusting collection, and purging unauthorized collection records from NSA databases.

~~(TS//SI//NF)~~ NSA analysis of content collected under the PSP involved the same practices and techniques used in analyzing information from other SIGINT operations. Telephone content was made available to NSA analysts through a voice processing system; Internet communications content was available from the database in which it was stored. Analysis involved more than listening to, or reading the content of, a communication and transcribing and disseminating a transcript. Analysis also involved coordinating and collaborating with other IC analysts, applying previous knowledge of the target, and integrating other relevant intelligence.

~~(TS//SI//NF)~~ Telephony and Internet Metadata Collection and Analysis

~~(TS//SI//OC/NF)~~ [redacted] NSA personnel used PSP metadata to perform contact chaining. Although the NSA had the capability to collect bulk telephony and Internet metadata before the PSP, collection was limited because the NSA was not authorized to collect metadata from a wire inside the United States without a court order when one end of the communication was in the United States. NSA could "chain" to, but not through, domestic selectors. Access to large amounts of metadata is required for effective contact chaining, and the PSP increased the data available to NSA analysts and allowed them to perform more thorough contact chaining.

~~(TS//SI//OC/NF)~~ Although NSA analysts could search bulk-collected metadata under the PSP, the analysts' searches were limited to targets that were approved under the standards set forth in the Presidential Authorizations. As such, only a small fraction of the metadata collected under the PSP was ever accessed. In August 2006, the NSA estimated that 0.000025 percent of the telephone records in the PSP database (or one of every four million records) could be expected to be seen by NSA analysts through chaining analysis.

[redacted]

~~(TS//SI//NF)~~ NSA analysts conduct contact chaining by entering a target selector—a telephone number or Internet communication address—in a specialized metadata analysis tool, which searches the metadata and identifies contacts between the selector and other telephone numbers or Internet communications addresses. The resulting contact graph is analyzed for intelligence and to develop investigative leads. [redacted] Although the Presidential Authorizations did not prohibit chaining more than two degrees of separation from the target, NSA analysts determined that it was not analytically useful to do so.

~~(TS//SI//NF)~~ An automated process was created to alert and automatically chain new and potentially reportable telephone numbers using what was called an "alert list." Telephone numbers on the alert list were automatically run against incoming metadata to look for contacts. [redacted]

[redacted]

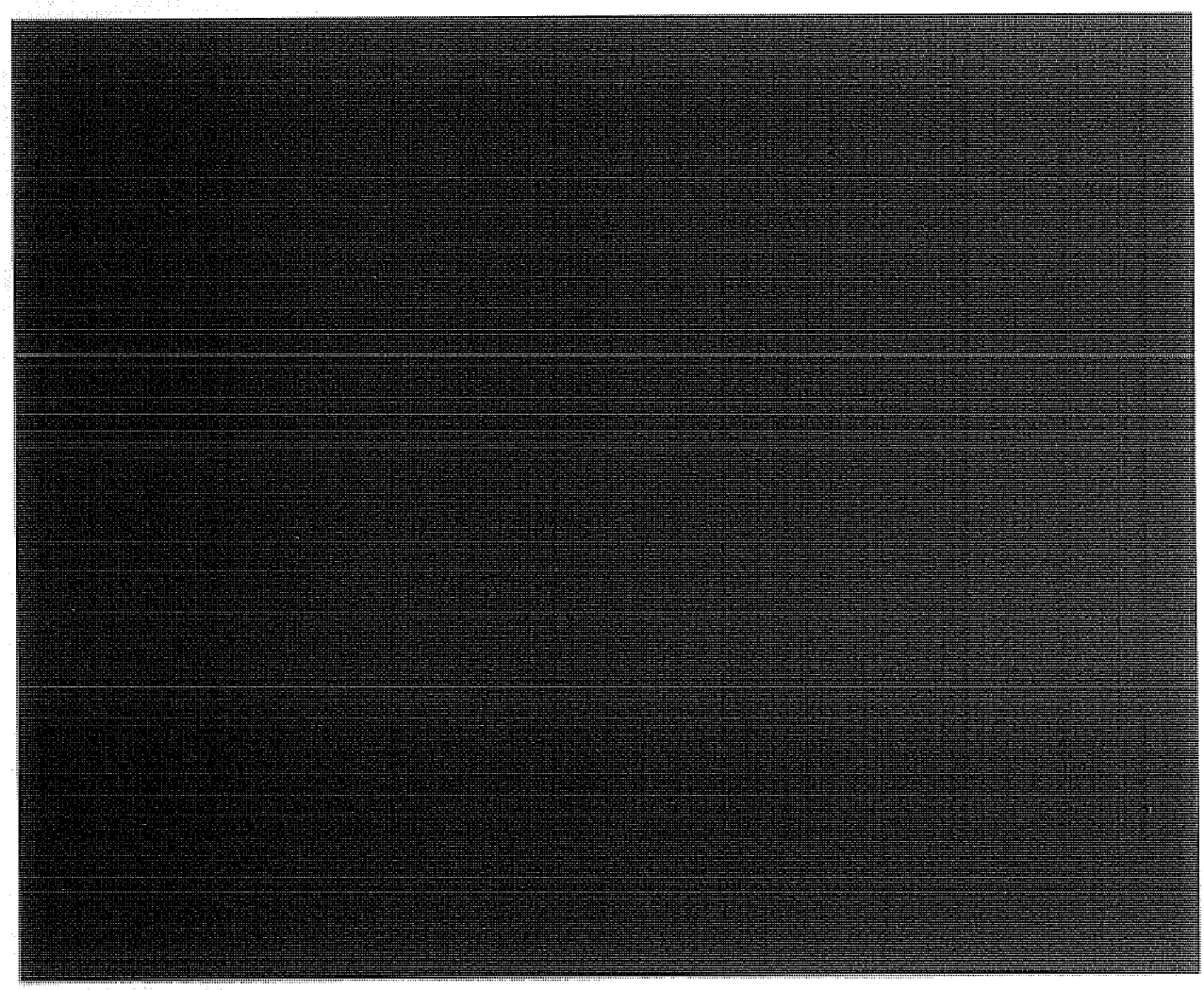
~~(TS//SI//NF)~~ When NSA personnel identified erroneous metadata collection—usually caused by technical problems or inappropriate application of the authorization—they were directed to report the violation or incident through appropriate channels and to delete the collection from all NSA databases. NSA reported three such violations early in the program and took measures to correct them.

(U) NSA Reporting From the President's Surveillance Program

~~(TS//SI//OC/NF)~~ PSP information was disseminated in [redacted] types of reports: "tippers," which provided metadata analysis; content reports, which provided NSA analysis of content collection; [redacted] Tippers were sent to the FBI and the CIA by e-mail on a secure communications network. Some tippers contained "tear line" information that allowed for wider distribution of a sanitized version of the information. From October 2001 through January 2007, the NSA issued [redacted] tippers to the FBI and the CIA.[8]

[redacted]

[8] [redacted]



(U) NSA Managerial Structure and Oversight of the President's Surveillance Program

~~(S//NF)~~ Analysis and reporting associated with the PSP was conducted within SID at NSA's Fort Meade, Maryland headquarters. PSP activities were not conducted at NSA field sites. The Director and Deputy Director of NSA exercised senior operational control and authority over the program. The individual who was SIGINT Director in 2001 told us that, aside from ensuring that the PSP had appropriate checks and balances, she left direct management of the program to the NSA Director, the Deputy Director, and the Office of General Counsel. She noted that Hayden took personal responsibility for the program and managed it carefully.

~~(S//NF)~~ By 2004, specific managerial authorities concerning PSP collection, analysis, and reporting activities had been delegated to the SIGINT Director. The SIGINT Director further delegated managerial authority to the PSP program manager and mission execution responsibilities to the Chief of the CT Product Line. The PSP program manager position was restructured to provide the incumbent authority and responsibility for oversight of PSP

activity across SID, and the PSP program manager was provided additional staff. Over the life of the program, there were five PSP program managers, who reported directly to the SIGINT Director or the Chief of the CT Product Line.

~~(TS//STLW//SI//OC/NF)~~ The NSA supported the operation of the PSP with approximately [redacted] from fiscal years (FYs) 2002 through 2006. Funds were used for the acquisition of [redacted]

(U) NSA PSP Costs From FY 2002 through FY 2006
(dollars in thousands, personnel costs not included)

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

[redacted]

(U) NSA Management Controls to Ensure Compliance With Presidential Authorizations

~~(S//NF)~~ NSA management took steps to protect U.S. person information and ensure compliance with the Presidential Authorizations. [redacted]

[redacted]

~~(S//NF)~~ The NSA General Counsel was read into the PSP on 4 October 2001, the day the first Presidential Authorization was signed. On 6 October 2001, the General Counsel provided Hayden and his deputy talking points for use in briefing NSA personnel on the new program's authorities. The talking points included the fact that Hayden had directed the NSA General Counsel and the NSA Associate General Counsel for Operations to review and oversee PSP activities. The NSA Associate General Counsel for Operations provided most of the program oversight before the NSA IG was read into the PSP in August 2002. The Associate General Counsel for Operations oversaw program implementation, reviewed proposed target packages for compliance with the authorizations, and coordinated program-related issues with DoJ.

(U) NSA Inspector General Oversight of the Program

~~(S//NF)~~ The NSA IG and other NSA Office of Inspector General personnel were read into the PSP beginning in August 2002. Over the life of the program, the NSA IG conducted:

- Three investigations in response to specific incidents and violations of the Presidential Authorizations to determine the cause, effect, and remedy.
- Ten reviews to determine the adequacy of management controls to ensure compliance with the authorization and related authorities, assess the mitigation of risk associated with program activities, and identify impediments to meeting the requirements of the authorizations.

~~(TS//SI//NF)~~ Ten of the NSA IG reports included a total of [redacted] recommendations to NSA management to strengthen internal controls and procedures over the PSP. The NSA IG identified no intentional misuse of the PSP. Significant findings from NSA IG reviews of the PSP include the following:

- In 2005, the NSA IG found [redacted] errors when comparing records of domestic telephone and communications selectors approved for PSP content collection with selectors actually on collection. The errors included selectors that were not removed from collection after being detasked, selectors that were not put on collection when approved, and selectors that were mistakenly put on collection due to typographical errors. NSA management took steps to correct the errors and establish procedures to reconcile approved selectors with selectors actually on collection.
- During a 2006 review, the NSA IG found that all items in a randomly selected sample of domestic selectors met Presidential Authorization criteria. Using a statistically valid sampling methodology, the IG concluded with 95 percent confidence that 95 percent or more of domestic

selectors tasked for PSP content collection were linked to al-Qa'ida, its associates, or international terrorist threats inside the United States.

~~(S//NF)~~ In addition to NSA IG report recommendations, in March 2003, the NSA IG recommended to Hayden that he report violations of the Presidential Authorizations to the President. The NSA IG prepared [redacted] Presidential notifications for the NSA Director concerning violations of the authorizations.

~~(S//NF)~~ Beginning in January 2007, violations involving collection activities conducted under PSP authority as well as violations related to former PSP activities that were operating under FISA authority were reported quarterly to the President's Intelligence Oversight Board, through the Assistant to the Secretary of Defense for Intelligence Oversight.

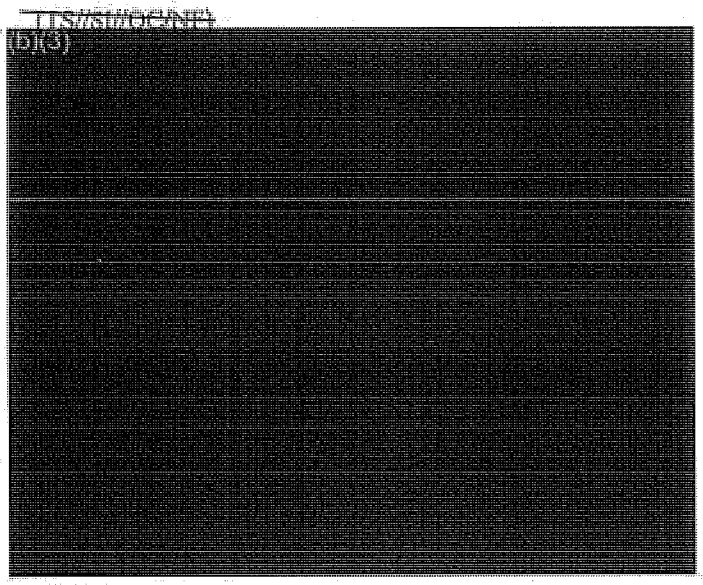
~~(TS//SI//NF)~~ The NSA IG learned in late 2008, that from approximately [redacted] collection of [redacted] All related collection records were purged from NSA databases in 2004; therefore, it was not possible to determine the exact nature and extent of the collection. NSA OIG will close out this incident in its upcoming report to the President's Intelligence Oversight Board.

~~(TS//SI//NF)~~ On 15 January 2009, the DoJ reported to the FISC that the NSA had been using an "alert list" to compare FISA-authorized metadata against telephone numbers associated with counterterrorism targets tasked by the NSA for SIGINT collection. The NSA had reported to the FISC that the alert list consisted of telephone numbers for which NSA had determined the existence of a reasonable, articulable suspicion that the numbers were related to a terrorist organization associated with [redacted] In fact, such a determination had not been made for the majority of the selectors on the alert list. The NSA IG reported this incident to the President's Intelligence Oversight Board, and has provided updates as required. The alert list and a detailed NSA 60-day review of processes related to the business records FISC order were the subject of several recent submissions to the FISC and of NSA briefings to the Congressional oversight committees.

(U) Access to the President's Surveillance Program

[redacted]

(U) PSP Cumulative Clearance Totals
(as of 17 January 2007)



~~(S//NF)~~ Knowledge of the PSP was strictly controlled and limited at the express direction of the White House. Hayden eventually delegated his PSP clearance approval authority for NSA, FBI, and CIA operational personnel to the NSA PSP program manager. Hayden was required to obtain approval from the White House to clear members of Congress, FISC Judges, the NSA IG, and others.

~~(S//NF)~~ The NSA IG was not read into the PSP until August 2002. According to the NSA General Counsel at the time, the President would not allow the IG to be briefed prior to that date. Although Hayden did not recall why the IG had not been cleared earlier, he thought that it would have been inappropriate to clear him when the length of the program was unknown and before operations had stabilized. By August 2002, Hayden and the NSA General Counsel wanted to institutionalize PSP oversight with the involvement of the NSA IG. Hayden recalled having to "make a case" to the White House to have the NSA IG read in. The ODNI IG found that ODNI oversight of the PSP was limited by ODNI oversight personnel not being provided timely access to the program.

(U) Congressional Briefings on the Program

~~(TS//SI//NF)~~ On 25 October 2001, Hayden conducted a briefing on the PSP for the Chairman and the Ranking Member of the House Permanent Select Committee on Intelligence, Nancy P. Pelosi and Porter J. Goss; and the Chairman and the Vice Chairman of the Senate Select Committee on Intelligence (SSCI), D. Robert Graham and Richard C. Shelby. Between 25 October 2001 and 17 January 2007, Hayden and current NSA Director Alexander, sometimes supported by other NSA personnel, conducted

49 briefings to members of Congress and their staff. Hayden told us that during the many PSP briefings to members of Congress, no one ever suggested that the NSA should stop the program. Hayden emphasized that he did more than just "flip through slides" during the briefings, which lasted as long as attendees had questions.

(U) Foreign Intelligence Surveillance Court Briefings on the Program

~~(TS//SI//OC/NF)~~ On 31 January 2002, the FISC Presiding Judge Royce Lamberth became the first member of the court to be read into the PSP. He was briefed on the program after James Baker, the head of DoJ's Office of Intelligence Policy and Review (OIPR) raised concerns with the White House over PSP-derived information being included in FISA applications. White House officials initially rejected the idea of reading in members of the FISC. Lamberth's briefing was conducted at the DoJ and was attended by Ashcroft, Hayden, Mueller, Yoo, and Baker.

~~(TS//SI//OC/NF)~~ Ashcroft provided Lamberth a brief summary of the President's decision to create the PSP, and Ashcroft stated that he had determined, based upon the advice of John Yoo, an attorney in DoJ's Office of Legal Counsel (OLC), that the President's actions were lawful under the Constitution. Ashcroft also emphasized to Lamberth that the FISC was not being asked to approve the program. Following Ashcroft's summary, Hayden described for Lamberth how the program functioned operationally, Yoo discussed legal aspects of the program, and Baker proposed procedures for handling international terrorism FISA applications that contained PSP-derived information. For the next four months, until the end of his term in May 2002, Lamberth was the only FISC judge read into the PSP.

~~(TS//SI//OC/NF)~~ Judge Colleen Kollar-Kotelly succeeded Lamberth as the FISC Presiding Judge and was briefed on the PSP on 17 May 2002. The briefing was similar in form and substance to that provided to Lamberth. In response to several questions from Kollar-Kotelly about the scope of the President's authority to conduct warrantless surveillance, DoJ prepared a letter to Kollar-Kotelly, signed by Yoo, that, according to Kollar-Kotelly, "set out a broad overview of the legal authority for conducting [the PSP], but did not analyze the specifics of the [PSP] program." The letter, which Kollar-Kotelly reviewed at the White House but was not permitted to retain, essentially replicated Yoo's 2 November 2001 memorandum regarding the legality of the PSP. Kollar-Kotelly was the only sitting FISC judge read into the PSP until January 2006, when the other FISC judges were read in.

~~(TS//SI//OC/NF)~~ Baker was read into the PSP only after he came upon "strange, unattributed" language in a FISA application that suggested the existence of a compartmented program. Baker advised that the FISC needed to be read into the program, but the White House initially resisted this idea. As noted, eventually Lamberth, and later his successor, Kollar-Kotelly, were read in. The DoJ IG believes that not having OIPR officials and members of the FISC read into the PSP, while program-derived information was being disseminated as investigative leads to the FBI and finding its way into FISA

applications, put at risk the DoJ's important relationship with the FISC. The DoJ IG agrees with Baker's assessment that, as the government's representative before the FISC, good relations between the DoJ and the FISC depend on candor and transparency.

(U) FBI Participation in the President's Surveillance Program

~~(TS//SI//NF)~~ As a user of PSP-derived information, the FBI disseminated leads—tippers—to FBI field offices. Tippers primarily consisted of domestic telephone numbers and Internet communications addresses that NSA analysts had determined through metadata analysis were connected to individuals involved with al-Qa'ida or its affiliates. Domestic telephone numbers represented the overwhelming majority of PSP-derived information contained in tippers. Tippers also provided information derived from content collection under the PSP.

~~(TS//SI//NF)~~ The FBI's principal objective during the earliest months of the PSP was to disseminate program information to FBI field offices for investigation while protecting the source of the information and the methods used to collect it. The FBI initially assigned responsibility for this to its Telephone Analysis Unit (TAU), which developed procedures to disseminate information from NSA's PSP reports in a non-compartmented, Secret-level format. The resulting [redacted] Electronic Communications (ECs) included restrictions on how the information could be used, i.e., FBI field offices were to use the information "for lead purposes only" and not use the information in legal or judicial proceedings. b1, b3, b7E

~~(S//NF)~~ The FBI's participation in the PSP evolved over time as the program became less a temporary response to the September 11 attacks and more a permanent surveillance capability. To improve the effectiveness of its participation in the program, the FBI initiated the [redacted] project in [redacted] to manage its involvement in the PSP. In February 2003, the FBI assigned a team of FBI personnel—"Team 10"—to work full-time at the NSA to manage the FBI's participation in the program. b1, b3, b7E

~~(TS//SI//NF)~~ Team 10's primary responsibility was to disseminate PSP information through [redacted] ECs to FBI field offices for investigation or other purposes. However, over time, Team 10 began to participate in the PSP in other ways. For example, Team 10 occasionally submitted telephone numbers and Internet communications addresses to the NSA to be searched against the bulk metadata collected under the PSP. The NSA conducted independent analysis to determine whether telephone numbers or Internet communications addresses submitted by Team 10 met the standards established by the Presidential Authorizations. Team 10 also regularly contributed to NSA's PSP process by reviewing draft reports and providing relevant information from FBI databases. b1, b3, b7E

~~(S//NF)~~ FBI field offices were not required to investigate every tipper disseminated by Team 10 under the [redacted] project. Rather, the type of lead that the [redacted] EC assigned—"action," "discretionary," or "for information"—drove the field office's b1, b3, b7E

response to a tipper.[9] The vast majority of FBI investigative activity related to PSP information involved responding to [redacted] telephone number tippers that assigned action leads. Team 10 generally assigned action leads for telephone numbers that were not already known to the FBI or telephone numbers that Team 10 otherwise deemed a high priority, such as a number that had a relationship to a major FBI investigation. From approximately [redacted] when [redacted] was established, to [redacted] action leads instructed field offices to obtain subscriber information for the telephone numbers within its jurisdiction and to conduct any "logical investigation to determine terrorist connections." Some agents complained that action leads lacked guidance about how to make use of the tippers, which was of particular concern because agents were not confident that [redacted] communications provided sufficient predication to open national security investigations. b1, b3, b7E

~~(TS//SI//NF)~~ Two changes to FBI procedures in 2003 addressed some FBI agents' concerns. [redacted] FBI Headquarters assumed responsibility from field offices for issuing national security letters (NSLs) to obtain subscriber information about PSP-tipped telephone numbers and Internet communications addresses. [redacted] the Attorney General issued new guidelines for FBI national security investigations that created a new category of investigative activity called a "threat assessment." Under a threat assessment, FBI agents are authorized to investigate or collect information on individuals, groups, and organizations of possible investigative interest without opening a preliminary or full national security investigation. Beginning [redacted] action leads assigned by [redacted] metadata tippers instructed field offices to conduct threat assessments and advised that FBI headquarters would issue NSLs to obtain subscriber information. b1, b3, b7E

~~(S//NF)~~ In general, an FBI threat assessment involved searching several FBI, public, and commercial databases for information about the tipped telephone number, and requesting that various state and local government entities conduct similar searches. Sometimes these searches identified the subscriber to the telephone number before FBI Headquarters obtained the information with an NSL. In other cases, the threat assessments continued after the field office received the NSL results.

~~(S//NF)~~ The [redacted] leads frequently were closed after conducting a threat assessment interview with the subscriber and determining that there was no nexus to terrorism or threat to national security. In other cases, the leads were closed based solely on the results of database checks. b1, b3, b7E

~~(S//NF)~~ Beginning [redacted] FBI field offices were required to report the results of their threat assessments to FBI headquarters. FBI field offices typically reported all of the information that was obtained about the tipped telephone numbers, including the details of any subscriber interviews, and then stated that the office had determined that the b1, b3, b7E

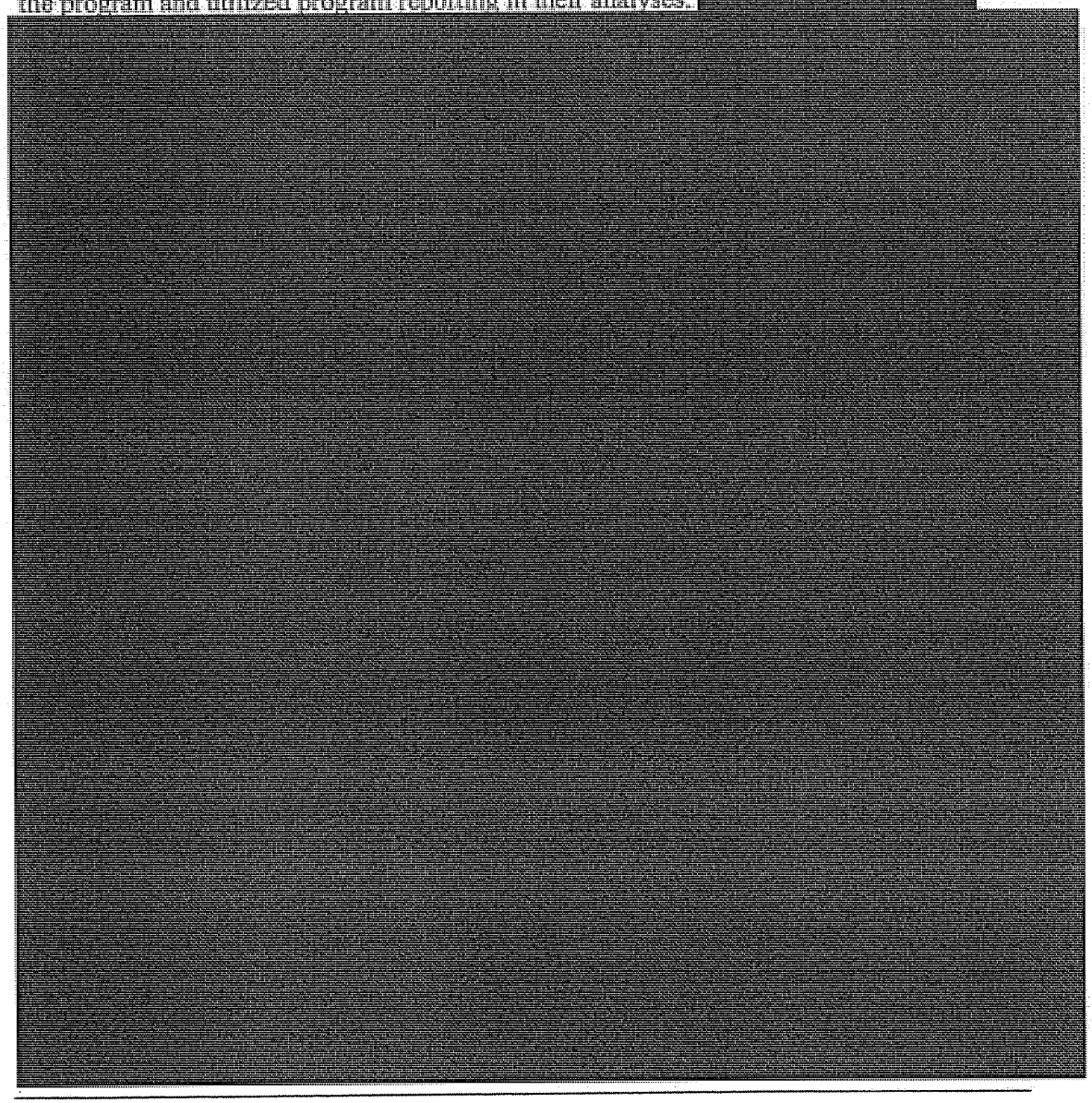
---

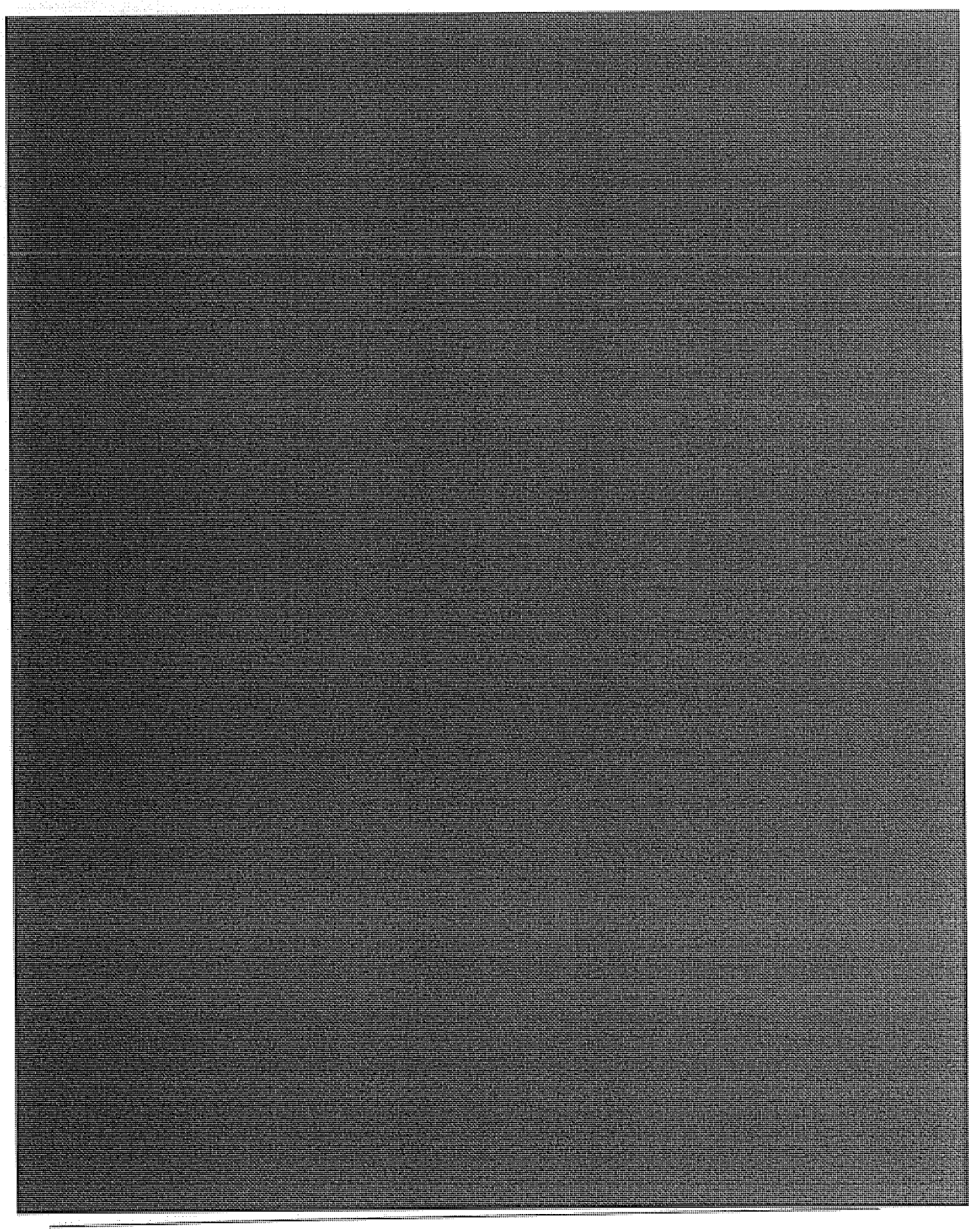
[9] ~~(S//NF)~~ An action lead instructs an FBI field office to take a particular action in response. A discretionary lead allows the field office to make a determination whether the information provided warrants investigative action. A field office is not expected to take any specific action on a for information lead.

telephone number did not have a nexus to terrorism and considered the lead closed. Much less frequently, field offices reported that a preliminary investigation was opened. Regardless of whether any links to international terrorism were identified in a threat assessment, the results of the threat assessments and the information that was collected about subscribers generally were reported to FBI headquarters and uploaded to FBI databases.

(U) CIA Participation in the President's Surveillance Program

~~(S//NF)~~ CIA analysts and targeters, as PSP consumers, requested information from the program and utilized program reporting in their analyses.





[redacted]

(U) NCTC Participation in the President's Surveillance Program

~~(TS//SI//NF)~~ The ODNI IG found that the ODNI's primary role in the PSP was the preparation of the threat assessments that summarized the al-Qa'ida threat to the United States and were used to support periodic reauthorization of the program. The ODNI IG found that the threat assessments were drafted by experienced NCTC personnel who prepared the documents in a memorandum style following an established DoJ format. The ODNI IG also determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide variety of IC sources. ODNI personnel said that during the period when the ODNI prepared the threat assessments, the IC had access to fully evaluated intelligence that readily supported an assessment that al-Qa'ida remained a significant threat to the United States.

~~(TS//SI//NF)~~ [redacted] The NCTC analysts told us that PSP information was subject to stringent security protections [redacted]

~~(S//NF)~~ The NCTC analysts said that they handle NSA surveillance information, including PSP information, consistent with the standard rules and procedures for handling NSA intelligence information including minimization of U.S. person identities. On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the PSP, the analysts told us they reviewed program information in the same manner as other incoming NSA intelligence products. If appropriate, NCTC analysts then incorporated the PSP information into analytical products being prepared for the Director of National Intelligence (DNI) and other senior intelligence officials. They identified the President's Terrorism Threat Report and the Senior Executive Terrorism Report as examples of the types of finished intelligence products that would, at times, contain PSP information.

(U) The President's Surveillance Program and the Foreign Intelligence Surveillance Court

~~(TS//SI//NF)~~ DoJ, initially with the FISC's concurrence and later at the court's direction, developed and implemented procedures—referred to as "scrubbing" procedures—to account for and make the court aware of instances when PSP-derived information was included in FISA applications. Lamberth required that all FISA applications that contained PSP-derived information, or that would result in simultaneous collection against particular targets under both the PSP and a FISC order, be filed with him only. Baker told us that Lamberth wanted to be informed of applications that contained PSP information and of dual coverage situations. According to Baker, the scrubbing procedures were a means of meeting his ethical duty of candor to the FISC without disclosing the existence of the PSP to uncleared judges.

~~(TS//SI//NF)~~ DoJ effectuated the scrubbing procedures by compiling lists of information contained in initial and renewal FISA applications that was attributed to the NSA and of all facilities targeted for electronic surveillance in the applications. These lists were sent to the NSA to determine whether any of the NSA-attributed information was PSP-derived and whether any of the facilities also were targeted under the PSP. The NSA communicated the results back to DoJ, which then filed the applications with the FISC consistent with the scrubbing procedures.

~~(TS//SI//NF)~~ Kollar-Kotelly continued the procedures that had been developed by Baker and agreed to by Lamberth for handling FISA applications that contained PSP-derived information. However, Kollar-Kotelly required DoJ to excise from FISA applications any information obtained or derived from the PSP. But Kollar-Kotelly also instructed Baker to alert her to any instances where an application's basis for the requisite probable cause showing under FISA was weakened by excising PSP information. In such cases, Kollar-Kotelly would then assess the application with the knowledge that additional relevant information had been excised.

~~(TS//SI//OC/NF)~~ Kollar-Kotelly also instructed DoJ to discontinue the practice employed under Lamberth of including in applications a descriptive phrase associated with [redacted] as a means of indicating that facilities targeted by the applications were also targeted under the PSP. Baker told us that while Kollar-Kotelly understood that instances of dual coverage would occur, she did not want to appear to judicially sanction PSP coverage. b1, b3, b7E

~~(TS//SI//NF)~~ In March 2004, Kollar-Kotelly was informed of operational changes made to the PSP following a dispute between DoJ and the White House about the legal basis for certain aspects of the program. Kollar-Kotelly responded by imposing an additional scrubbing requirement to further ensure, to the extent possible, that PSP-derived information was not included in FISA applications. The FBI, in coordination with DoJ and NSA, was to determine whether a facility included in a FISA application—not just a targeted telephone number or Internet communication address—also appeared in a PSP report. Kollar-Kotelly permitted any such facility to remain in the application if it could be

demonstrated that the FBI had developed, independent of the PSP, an investigative interest in the facility, or that the FBI inevitably would have identified the facility in question through normal investigative steps. An OIPR official who was responsible for discussing such cases with Kollar-Kotelly told us that the judge generally accepted DoJ's assessment that there was a non-PSP investigative basis for a facility in question, or that the facility inevitably would have been discovered even in the absence of PSP-derived leads to the FBI.

~~(S//NF)~~ Implementing the scrubbing procedures, both under Lamberth and Kollar-Kotelly, was a complicated and time-consuming endeavor for OIPR staff. Baker, who until March 2004 was the only individual in OIPR read into the PSP, found himself having to ask OIPR attorneys to compile information about their cases, and sometimes to make changes to their FISA applications, without being able to provide an explanation other than that he had spoken to the Attorney General and the FISC about the situation. Baker regularly told attorneys that they did not have to sign applications that they were not comfortable with, and, in some instances, international terrorism cases had to be reassigned for this reason.

~~(S//NF)~~ The situation was further complicated by the fact that, until August 2003, only one of the two DoJ officials authorized by statute to approve FISA applications—Attorney General Ashcroft and Deputy Attorney General Larry Thompson—was read into the PSP. Thompson, who served as Deputy Attorney General from May 2001 to August 2003, was never read into the PSP, despite Ashcroft's request to the White House.

~~(TS//SI//NF)~~ Similarly, Kollar-Kotelly, who by November 2004 was handling approximately [redacted] percent of all FISA applications as a result of her requirement that scrubbed applications be filed with her only, made unsuccessful requests for additional FISC judges to be cleared for the program. Kollar-Kotelly decided in November 2004 that in view of the scrubbing procedures that were in operation, international terrorism FISA applications could be decided by other judges based on the information contained in the applications.

~~(TS//SI//NF)~~ DoJ, together with the FBI and the NSA, continue to apply the scrubbing procedures to international terrorism FISA applications. Since January 2006, all members of the FISC have been briefed on the PSP and all of the judges handle applications that involve the issue of PSP-derived information. Although compliance with the scrubbing procedures has been burdensome, we did not find instances when the government was unable to obtain FISA surveillance coverage on a target because of the requirement. However, the DoJ IG concluded that once the PSP began to affect the functioning of the FISA process, OIPR and the FISC effectively became part of the PSP's operations, and more OIPR staff and FISC judges should have been read into the PSP to address the impact. Instead, access to the PSP was limited for years to a single OIPR official and one FISC judge.

(U) Discovery Issues Associated With the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ DoJ was aware as early as (b)(1), (b)(3) that information collected under the PSP could have implications for DoJ's litigation responsibilities under Rule 16 of the Federal Rules of Criminal Procedure and *Brady v. Maryland*, 373 U.S. 83 (1963). Analysis of the discovery issue was first assigned to Yoo in [redacted] (b)(1), (b)(3), (b)(6), (b)(7)

b1, b3, b6, b7C, b7E

[redacted] (b)(1), (b)(3)

b1, b3, b6, b7C b7E

~~(S//NF)~~ No DoJ attorneys with terrorism prosecution responsibilities were read into the PSP until mid-2004, and as a result, DoJ did not have access to the advice of attorneys who were best equipped to identify and examine discovery issues associated with the PSP. The DoJ IG believes that, since then, DoJ has taken steps to respond (b)(1), (b)(3) [redacted] to [redacted] discovery motions (b)(1), (b)(3) [redacted] DoJ's responses to the discovery motions involve the use of the Classified Information Procedures Act, 18 U.S.C. App. 3, to file *ex parte* in camera pleadings with federal courts to describe potentially responsive PSP-derived information. [redacted] (b)(3), (b)(1)

~~(S//NF)~~ [redacted] the DoJ IG recommends that DoJ assess its discovery obligations regarding PSP-derived information in international terrorism prosecutions, carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. The DoJ IG also recommends that DoJ, in coordination with the NSA, implement a procedure to identify PSP-derived information that may be associated with international terrorism cases

currently pending or likely to be brought in the future and evaluate whether such information should be disclosed in light of the government's discovery obligations under Rule 16 and *Brady*.

(U) LEGAL REASSESSMENT OF THE PRESIDENT'S SURVEILLANCE PROGRAM (2003 – 2004)

~~(TS//SI//NF)~~ Concern Over the [redacted] Collection

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

~~(TS//SI//NF)~~ Yoo was the sole OLC attorney who advised Ashcroft and White House officials on the PSP from the program's inception in October 2001 through Yoo's resignation from DoJ in May 2003. Upon Yoo's departure, Patrick Philbin was selected by the White House to be read into the PSP to assume Yoo's role as advisor to the Attorney General concerning the program.

~~(TS//SI//NF)~~ Philbin told us that when he reviewed Yoo's legal memorandums about the PSP, he realized that Yoo had omitted from his analysis any reference to the FISA provision allowing the interception of electronic communications without a warrant for a period of 15 days following a Congressional declaration of war. (See 50 U.S.C. § 1811.) Philbin stated that Yoo's OLC opinions were premised on the assumption that FISA did not expressly apply to wartime operations, an assumption that from Philbin's perspective made the opinions "problematic."

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

[redacted]

(b) (5), (b)(1), (b)(3)

~~(S//NF)~~ In August 2003, Philbin told Ashcroft that there were problems with the legal analysis supporting the PSP but probably not with the conclusions reached, and he therefore advised Ashcroft to continue to certify the program "as to form and legality." Philbin also recommended that a new OLC memorandum assessing the legality of the PSP be drafted, and with Ashcroft's concurrence he began drafting the memorandum.

(U) A New Legal Basis for the Program Is Adopted

~~(S//NF)~~ Goldsmith was sworn in as the Assistant Attorney General for OLC on 6 October 2003, replacing Bybee, who had left that position several months earlier to serve as a judge on the U.S. Court of Appeals for the Ninth Circuit. Philbin told us that he pressed hard to have Goldsmith read into the PSP, and that Addington told Philbin he would have to justify the request before Addington would take it to the President for a decision. Addington subsequently read Goldsmith into the program on 17 November 2003.

~~(TS//SI//NF)~~ After reviewing Yoo's memorandums and Philbin's new draft analysis of the PSP, Goldsmith agreed with Philbin's concerns about the existing legal analysis supporting the program.

(b) (5), (b)(1), (b)(3)

~~(S//SI//NF)~~

(b) (5), (b)(1), (b)(3)

(b) (5), (b)(1), (b)(3)

(b)(5), (b)(1), (b)(3)

~~(TS//SI//NF)~~ Goldsmith concluded that the NSA's interception of (b)(5), (b)(1), (b)(3) did not comply with FISA's requirement to obtain judicial authorization, and did not fall within any of the exceptions to this requirement. Goldsmith later wrote in a 6 May 2004 legal memorandum reassessing the legality of the program that a proper analysis of the PSP "must not consider FISA in isolation" but rather must consider whether Congress, by authorizing the use of military force against al-Qa'ida, also "effectively exempts" such surveillance from FISA. Goldsmith believed that this reading of the AUMF was correct because the AUMF authorized the President to use "all necessary and appropriate force" against the enemy that attacked the United States on 11 September 2001, and to "prevent any future acts of international terrorism against the United States" by such enemy—authority that has long been recognized to include the use of SIGINT as a military tool. Alternatively, Goldsmith reasoned that even if the AUMF did not exempt surveillance under the program from the restrictions imposed by FISA, the question was sufficiently ambiguous to warrant the application of the doctrine of constitutional avoidance, and therefore should be construed not to prohibit the activity.[11]

(b)(5), (b)(1), (b)(3)

[11] ~~(TS//SI//NF)~~ (b)(5), (b)(1), (b)(3)

~~(TS//SI//NF)~~ In late 2003, Philbin and Goldsmith were the only two DoJ officials in a position to brief the Attorney General and White House officials on the status of their legal reassessment and its potential ramifications for the operation of the program. Goldsmith advised Ashcroft that, despite concerns about the program, Ashcroft should certify the 9 December 2003 Presidential Authorization. Goldsmith later advised Ashcroft to certify the 14 January 2004 authorization as well. Goldsmith told us that he made these recommendations to Ashcroft with the caveat that although he believed Yoo's memorandums to be flawed, Goldsmith had not yet concluded that the program itself was illegal.

(U) Department of Justice Officials Convey Concerns About the Program to the White House

~~(TS//SI//NF)~~ In December 2003, Goldsmith and Philbin met with Addington and Gonzales at the White House to express their growing concerns about the legal underpinnings for the program. Goldsmith said he told them that OLC was not sure the program could survive in its current form. According to Goldsmith's contemporaneous notes of these events, these discussions did not contemplate an interruption of the program, although the White House officials represented that they would "agree to pull the plug" if the problems with the program were found to be sufficiently serious. Goldsmith told us that the White House—typically through Addington—told him "several times" that it would halt the program if DoJ found that it could not be legally supported.

~~(TS//SI//NF)~~ On 18 December 2003, Goldsmith met again with Addington and Gonzales and wrote in his notes that during this meeting he conveyed with "more force" his "serious doubts and the need to get more help to resolve the issue [as soon as possible]." Goldsmith told us that during this meeting he also asked to have Deputy Attorney General Comey read into the program. According to Goldsmith's notes, Addington and Gonzales "bristle[d]" at that suggestion. Goldsmith told us that he requested that Comey be read in because he believed he would need Comey's assistance to help "make the case" to the White House that the program was legally flawed. In addition, he said he wanted Comey read in because, as the Deputy Attorney General, Comey was Philbin's direct supervisor.

~~(TS//SI//NF)~~ Goldsmith's efforts to gain the White House's permission to have additional attorneys, and especially Comey, read into the program continued through January 2004. According to Goldsmith's notes, both Addington and Gonzales pressed Goldsmith on his reason for the request and continued to express doubt that additional DoJ personnel were needed. However, in late January 2004 the White House agreed to allow Comey to be read in, and Comey was briefed into the PSP on 12 March 2004 by Hayden.

~~(S//NF)~~ After his briefing, Comey discussed the program with Goldsmith, Philbin, and other DoJ officials, and agreed that the concerns with Yoo's legal analysis were well-founded.[12] Comey told us that of particular concern to him and Goldsmith was the notion that Yoo's legal analysis entailed ignoring an act of Congress, and doing so without full Congressional notification.

~~(TS//SI//NF)~~ Comey told us that in early March 2004 the sense at DoJ was that "we can get there" with regard to (b)(1), (b)(3) albeit by using an aggressive legal analysis. However, he agreed with Goldsmith's conclusion that (b)(1), (b)(3) would require (b)(1), (b)(3)

(U) Conflict Between the Department of Justice and the White House Over the Program

(U) Comey told us that he met with Ashcroft for lunch on 4 March 2004 to discuss the PSP, and that Ashcroft agreed with Comey and the other DoJ officials' assessment of the potential legal problems with the program. Three hours after their lunch meeting, Ashcroft became ill and was admitted to the George Washington University Hospital.[13] On 5 March 2004, Goldsmith advised Comey by memorandum that under the circumstances of Ashcroft's medical condition and hospitalization, a "clear basis" existed for Comey to exercise the authorities of the Attorney General allowed by law as Deputy Attorney General or Acting Attorney General. The "cc" line of Goldsmith's memorandum to Comey indicated that a copy of the memorandum was sent to Gonzales.

~~(TS//SI//NF)~~ On 5 March 2004—six days before the Presidential Authorization then in effect was set to expire—Goldsmith and Philbin met with Addington and Gonzales at the White House to again convey their concerns about the PSP. (b) (5), (b)(1), (b)(3) Later that day, Gonzales called Goldsmith to request a letter from OLC stating that Yoo's prior OLC opinions "covered the program." Philbin told us that Gonzales was not requesting a new opinion that the program itself was legal, but only a letter stating that the prior opinions had concluded that it was.

---

[12] ~~(TS//SI//OC/NF)~~ The other officials included Counsel for Intelligence Policy Baker, Counselor to the Attorney General Levin, and Comey's Chief of Staff Chuck Rosenberg. Both Levin and Rosenberg had been read into the PSP while at the FBI. Comey also discussed DoJ's concerns about the legality of the program with FBI Director Mueller on 1 March 2004. Mueller told us that this was the first time he had been made aware of DoJ's concerns.

[13] (U) Ashcroft's doctors did not clear Ashcroft to resume his duties as Attorney General until 31 March 2004.

~~(TS//SI//NF)~~ As a result of Gonzales's request, Goldsmith, Philbin, and Comey re-examined Yoo's memorandums with a view toward determining whether they adequately described the actual collection activities of the NSA under the Presidential Authorizations. They concluded that the memorandums did not. According to Goldsmith, the conclusion that Yoo's memorandums failed to accurately describe, let alone provide a legal analysis of (b) (5), (b)(1), (b)(3) meant that OLC could not tell the White House that the program could continue under the authority of those legal memorandums.

~~(TS//SI//NF)~~ On 6 March 2004, Goldsmith and Philbin, with Comey's concurrence, went to the White House to meet with Addington and Gonzales to convey their conclusions that (b) (5), (b)(1), (b)(3) According to Goldsmith's notes, Addington and Gonzales "reacted calmly and said they would get back with us." On Sunday, 7 March 2004, Goldsmith and Philbin met again with Addington and Gonzales at the White House. According to Goldsmith, the White House officials informed Goldsmith and Philbin that they disagreed with their interpretation of Yoo's memorandums and on the need to change the scope of the NSA's collection under the PSP.

~~(S//NF)~~ On 9 March 2004, Gonzales called Goldsmith to the White House in an effort to persuade him that his criticisms of Yoo's memorandums were incorrect and that Yoo's analysis provided sufficient legal support for the program. (b) (5) After Goldsmith stated that he disagreed, Gonzales next argued for a "30-day bridge" to get past the expiration of the current Presidential Authorization on 11 March 2004. Gonzales reasoned that Ashcroft, who was still hospitalized, was not in any condition to sign a renewal of the authorization, and that a "30-day bridge" would move the situation to a point where Ashcroft would be well enough to approve the program. Goldsmith told Gonzales he could not agree to recommend an extension because aspects of the program lacked legal support.

~~(TS//SI//NF)~~ At noon on 9 March, another meeting was held at the White House in Card's office. According to Mueller's notes, Mueller, Card, Vice President Cheney, Deputy Director of Central Intelligence John E. McLaughlin, Hayden, Gonzales, and other unspecified officials were present. Comey, Goldsmith, and Philbin were not invited to this meeting. After a presentation on the value of the PSP by NSA and CIA officials, it was then explained to the group that Comey "has problems" with (b)(1), (b)(3) Mueller's notes state that the Vice President suggested that "the President may have to reauthorize without [the] blessing of DoJ," to which Mueller responded, "I could have a problem with that," and that the FBI would "have to review legality of continued participation in the program."

~~(TS//SI//NF)~~ A third meeting at the White House was held on 9 March, this time with Comey, Goldsmith, and Philbin present. Gonzales told us that the meeting was held to make sure that Comey understood what was at stake with the program and to demonstrate its value. Comey said the Vice President stressed that the program was "critically

important" and warned that Comey would risk "thousands" of lives if he did not agree to recertify it. Comey said he stated at the meeting that he, as Acting Attorney General, could support reauthorizing (b)(1), (b)(3) provided the collection was (b)(1), (b)(3) However, he told the group "we can't get there" on (b)(1), (b)(3) According to Comey, the White House officials said they could not agree to that modification.

~~(S//NF)~~ Gonzales told us that after President Bush was advised of the results of the 9 March meetings, he instructed the Vice President on the morning of 10 March to call a meeting with Congressional leaders to advise them of the impasse with DoJ. That afternoon, Gonzales and other White House and IC officials, including Vice President Cheney, Card, Hayden, McLaughlin, and Tenet, convened an "emergency meeting" with Congressional leaders in the White House Situation Room. The Congressional leaders in attendance were Senate Majority and Minority Leaders William H. "Bill" Frist and Thomas A. Daschle; Senate Select Committee on Intelligence Chairman Pat Roberts and Vice Chairman John D. Rockefeller, IV; Speaker of the House J. Dennis Hastert and House Minority Leader Nancy Pelosi; and House Permanent Select Committee on Intelligence Chair Porter Goss and Ranking Member Jane Harman. No DoJ officials were asked to be present at the meeting.

~~(S//NF)~~ According to Gonzales's notes of the meeting, individual Congressional leaders expressed thoughts and concerns related to the program. Gonzales told us that the consensus was that the program should continue. Gonzales also said that following the meeting with Congressional leaders, President Bush instructed him and Card to go to the George Washington University Hospital to speak to Ashcroft, who was in the intensive care unit recovering from surgery.

(U) According to notes from Ashcroft's FBI security detail, at 18:20 on 10 March 2004, Card called the hospital and spoke with an agent in the security detail, advising the agent that President Bush would be calling shortly to speak with Ashcroft. Ashcroft's wife told the agent that Ashcroft would not accept the call. Ten minutes later, the agent called Ashcroft's Chief of Staff David Ayres at DoJ to request that Ayres speak with Card about the President's intention to call Ashcroft. The agent conveyed to Ayres Mrs. Ashcroft's desire that no calls be made to Ashcroft for another day or two. However, at 18:45, Card and the President called the hospital and, according to the agent's notes, "insisted on speaking [with Attorney General Ashcroft]." According to the agent's notes, Mrs. Ashcroft took the call from Card and the President and was informed that Gonzales and Card were coming to the hospital to see Ashcroft regarding a matter involving national security.

(U) At approximately 19:00, Ayres was advised that Gonzales and Card were on their way to the hospital. Ayres then called Comey, who at the time was being driven home by his security detail, and told Comey that Gonzales and Card were on their way to the

hospital. Comey told his driver to take him to the hospital. According to his May 2007 testimony before the Senate Judiciary Committee, Comey then called his Chief of Staff, Chuck Rosenberg, and directed him to "get as many of my people as possible to the hospital immediately." Comey next called Mueller and told him that Gonzales and Card were on their way to the hospital to see Ashcroft, and that Ashcroft was in no condition to receive visitors, much less make a decision about whether to recertify the PSP. According to Mueller's notes, Comey asked Mueller to come to the hospital to "witness [the] condition of AG." Mueller told Comey he would go to the hospital right away.

(U) Comey arrived at the hospital between 19:10 and 19:30. Comey said he began speaking to Ashcroft, and that it was not clear that Ashcroft could focus and that he "seemed pretty bad off." Goldsmith and Philbin also had been summoned to the hospital and arrived within a few minutes of each other. Comey, Goldsmith, and Philbin met briefly in an FBI "command post" that had been set up in a room adjacent to Ashcroft's room. Moments later, the command post was notified that Card and Gonzales had arrived at the hospital and were on their way upstairs to see Ashcroft. Comey, Goldsmith, and Philbin entered Ashcroft's room and, according to Goldsmith's notes, Comey and the others advised Ashcroft "not to sign anything."

(U) Gonzales and Card entered Ashcroft's hospital room at 19:35. Gonzales told us that he had with him in a manila envelope the 11 March 2004, Presidential Authorization for Ashcroft to sign. According to Philbin, Gonzales first asked Ashcroft how he was feeling. Ashcroft replied, "not well." Gonzales then said words to the effect, "You know, there's a reauthorization that has to be renewed . . .." Gonzales told us that he may also have told Ashcroft that White House officials had met with Congressional leaders "to pursue a legislative fix."

~~(TS//SI//NF)~~ Comey testified to the Senate Judiciary Committee that at this point Ashcroft told Gonzales and Card "in very strong terms" his objections to the PSP, which Comey testified Ashcroft drew from his meeting with Comey about the program a week earlier. Goldsmith's notes indicate that Ashcroft complained in particular that NSA's collection activities exceeded the scope of the authorizations and the OLC memorandums. Comey testified that Ashcroft next stated:

> "But that doesn't matter, because I'm not the Attorney General. There is the Attorney General," and he pointed to me—I was just to his left. The two men [Gonzales and Card] did not acknowledge me; they turned and walked from the room.

(U) Moments after Gonzales and Card departed, Mueller arrived at the hospital. Mueller met briefly with Ashcroft and later wrote in his notes, "AG in chair; is feeble, barely articulate, clearly stressed."

(U) Before leaving the hospital, Comey received a call from Card. Comey testified that Card was very upset and demanded that Comey come to the White House immediately. Comey told Card that he would meet with him, but not without a witness, and that he intended that witness to be Solicitor General Theodore B. Olson.

(U) Comey and the other DoJ officials left the hospital at 20:10 and met at DoJ. They were joined there by Olson. During this meeting, a call came from the Vice President for Olson, which Olson took on a secure line in Comey's office while Comey waited outside. Comey told us he believes the Vice President effectively read Olson into the program during that conversation. Comey and Olson then went to the White House at about 23:00 that evening and met with Gonzales and Card. Gonzales told us that little more was achieved at this meeting than a general acknowledgement that a "situation" continued to exist because of the disagreement between DoJ and the White House regarding the program.

~~(S//NF)~~ White House Counsel Certifies Presidential Authorization Without Department of Justice Concurrence

~~(TS//STLW//SI//OC/NF)~~ On the morning of 11 March 2004, with the Presidential Authorization set to expire, President Bush signed a new authorization for the PSP. In a departure from the past practice of having the Attorney General certify the authorization as to form and legality, the 11 March authorization was certified by White House Counsel Gonzales. The 11 March authorization also differed markedly from prior authorizations in three other respects.

~~(TS//STLW//SI//OC/NF)~~ The first significant difference between the 11 March 2004 Presidential Authorization and prior authorizations was the President's explicit assertion that the exercise of his Article II Commander-in-Chief authority "displace[s] the provisions of law, including the Foreign Intelligence Surveillance Act and chapter 119 of Title 18 of the United States Code (including 18 U.S.C. §2511(f) relating to exclusive means), to the extent of any conflict between the provisions and such exercises under Article II." Subsequent Presidential Authorizations did not include this particular language.

~~(TS//STLW//SI//OC/NF)~~ Second, to narrow the gap between the authority given on the face of prior authorizations and the actual operation of the program by the NSA, the terms governing the collection of telephony and Internet metadata were clarified. The underlying language for "acquiring" both telephony and Internet metadata remained as it had been, giving the NSA authority to "acquire" the metadata:

> when (i) at least one party to such communication is outside the United States, (ii) no party to such communication is known to be a citizen of the United States, or (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor. [Presidential Authorization, 11 March 2004, para. 4(b).]

However, this language was now qualified by the following two subparagraphs:

> (i) the Department of Defense may obtain and retain header/router/addressing-type information, including telecommunications dialing-type data, (b)(1), (b)(3) provided that search and retrieval from such obtained header/router/addressing-type information, including telecommunications dialing-type data, shall occur only in accordance with this authorization; and
>
> (ii) header/router/addressing-type information, including telecommunications dialing-type data, is "acquired" for purposes of subparagraph 4(b) above when, and only when, the Department of Defense has searched for and retrieved such header/router/addressing-type information, including telecommunications dialing-type data (and not when the Department obtains such header/router/addressing-type information, including telecommunications dialing-type data, such as (b)(1), (b)(3) for retention). [Id. at para. 4(b)(i) & (ii).]

~~(TS//STLW//SI//OC/NF)~~ The 11 March 2004 authorization for the first time sought to make clear that the NSA could "obtain and retain" telephony and Internet metadata in bulk (b)(1), (b)(3) but the metadata collected could only be queried ("acquired") in accordance with any of the three conditions set forth in paragraph 4(b). The language clarifying what the term "acquire" meant was included in every successive Presidential Authorization for the remainder of the program. (b)(5), (b)(1), (b)(3)

~~(TS//SI//NF)~~ The third departure from prior authorizations was the inclusion of a statement that "the Attorney General of the United States approved as to form and legality [all prior Presidential Authorizations] authorizing the same activities as are extended by this authorization." (Id. at para. 10.)[14]

~~(TS//SI//NF)~~ Card informed Comey by telephone on the morning of 11 March 2004 that the President had signed the new authorization that morning. At approximately 12:00, Gonzales called Goldsmith to inform him that the President, in issuing the authorization, had made an interpretation of law concerning his authorities and that DoJ should not act in contradiction of the President's determinations.

~~(TS//SI//NF)~~ Also at 12:00 on 11 March, Mueller met with Card at the White House. According to Mueller's notes, Card summoned Mueller to his office to bring Mueller up-to-date on the events of the preceding 24 hours, including the briefing of the Congressional leaders the prior afternoon and the President's issuance of the new authorization without DoJ's certification as to legality. In addition, Card told Mueller that if no "legislative fix" could be found by 6 May 2004, when the 11 March authorization was set to expire, the program would be discontinued.

~~(TS//SI//NF)~~ According to Mueller's notes, Card acknowledged to Mueller that President Bush had sent him and Gonzales to the hospital to seek Ashcroft's certification for the 11 March 2004 authorization, but that Ashcroft had said he was too ill to make the determination and that Comey was the Acting Attorney General. Mueller wrote that he told Card that the failure to have DoJ representation at the Congressional briefing and the attempt to have Ashcroft certify the authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." Card responded that he and Gonzales were unaware at the time of the hospital visit that Comey was the Acting Attorney General, and that they had only been following the directions of the President.

~~(S//NF)~~ Several senior DoJ and FBI officials, including Comey, Goldsmith, and Mueller considered resigning after the 11 March 2004 Presidential Authorization was signed without DoJ's concurrence. These officials cited as reasons for considering resignation the manner in which the White House had handled its dispute with DoJ and the treatment of Ashcroft, among other reasons.

~~(S//NF)~~ On 12 March 2004, Mueller drafted by hand a letter stating, in part: "[A]fter reviewing the plain language of the FISA statute, and the order issued yesterday by the President . . . and in the absence of further clarification of the legality of the program from the Attorney General, I am forced to withdraw the FBI from participation in the program.

---

[14] (b) (5)

Further, should the President order the continuation of the FBI's participation in the program, and in the absence of further legal advice from the AG, I would be constrained to resign as Director of the FBI." Mueller told us he planned on having the letter typed and then tendering it, but that based on subsequent events his resignation was not necessary.

~~(TS//SI//NF)~~ Mueller sent Comey a memorandum seeking guidance on how the FBI should proceed in light of developments related to the Presidential Authorizations. The memorandum asked whether FBI agents detailed to the NSA to work on the PSP should be recalled; whether the FBI should continue to receive and investigate tips based on [redacted] (b)(1), (b)(3) and whether (b)(1), (b)(3) [redacted] b1, b3, b7E

(U) On the morning of 12 March, Comey and Mueller attended the regular daily threat briefing with the President in the Oval Office. Comey said that, following the briefing, President Bush called him into the President's private study for an "unscheduled meeting." Comey told the President of DoJ's legal concerns regarding the PSP. According to Comey, the President's response indicated that he had not been fully informed of these concerns. Comey told the President that the President's staff had been advised of these issues "for weeks." According to Comey, the President said that he just needed until May 6 (the date of the next authorization), and that if he could not get Congress to fix FISA by then he would shut down the program. The President emphasized the importance of the program and that it "saves lives."

~~(TS//SI//NF)~~ The President next met with Mueller. According to Mueller's notes, Mueller told the President of his concerns regarding the FBI's continued participation in the program without an opinion from the Attorney General as to its legality, and that he was considering resigning if the FBI were directed to continue to participate without the concurrence of the Attorney General. The President directed Mueller to meet with Comey and other PSP principals to address the legal concerns so that the FBI could continue participating in the program "as appropriate under the law." Comey decided not to direct the FBI to cease cooperating with the NSA in conjunction with the PSP. Comey's decision is documented in a one-page memorandum from Goldsmith to Comey in which Goldsmith explained that the President, as Commander-in-Chief and Chief Executive with the constitutional duty to "take care that the laws are faithfully executed," made a determination that the PSP, as practiced, was lawful. Goldsmith concluded that this determination was binding on the entire Executive Branch, including Comey in his exercise of the powers of the Attorney General.

~~(TS//SI//NF)~~ The same day, an interagency working group was convened to continue reanalyzing the legality of the PSP. In accordance with the President's directive to Mueller, officials from the FBI, NSA, and CIA were brought into the process, although the OLC maintained the lead role. On 16 March 2004, Comey drafted a memorandum to Gonzales setting out Comey's advice to the President regarding the PSP. Comey advised that the President may lawfully continue (b)(1), (b)(3) [redacted] Comey further

wrote that DoJ remained unable to find a legal basis to support (b)(1), (b)(3) and he advised that such (b)(1), (b)(3) Finally, Comey cautioned that he believed the ongoing collection of (b)(1), (b)(3) raised "serious issues" about Congressional notification, "particularly where the legal basis for the program is the President's decision to assert his authority to override an otherwise applicable Act of Congress."

(U) Gonzales replied by letter on the evening of 16 March. The letter stated, in part:

> Your memorandum appears to have been based on a misunderstanding of the President's expectations regarding the conduct of the Department of Justice. While the President was, and remains, interested in any thoughts the Department of Justice may have on alternative ways to achieve effectively the goals of the activities authorized by the Presidential Authorization of March 11, 2004, the President has addressed definitively for the Executive Branch in the Presidential Authorization the interpretation of the law.

~~(TS//SI//NF)~~ White House Agrees to (b)(1), (b)(3)

~~(TS//SI//NF)~~ Notwithstanding Gonzales's letter, on 17 March 2004 the President decided to (b)(1), (b)(3) The President's directive was expressed in two modifications to the 11 March 2004 Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ On 19 March 2004, the President signed, and Gonzales certified as to form and legality, a modification of the 11 March 2004 Presidential Authorization. The modification made two significant changes to the current authorization and a third important change affecting all subsequent authorizations. First, the modification (b)(1), (b)(3) Second, the modification (b)(1), (b)(3)

[redacted] Third, the modification authorized
(b)(1), (b)(3)
[redacted]

~~(TS//STLW//SI//OC/NF)~~ On 2 April 2004, President Bush signed, and Gonzales certified as to form and legality, a second modification of the 11 March 2004, Presidential Authorization. This modification addressed only [redacted] of the PSP.
(b)(1), (b)(3)
[redacted]

~~(S//NF)~~ On 6 May 2004, Goldsmith and Philbin completed an OLC legal memorandum assessing the legality of the PSP as it was then operating. The memorandum stated that the AUMF passed by Congress shortly after the attacks of 11 September 2001 gave the President authority to use both domestically and abroad "all necessary and appropriate force," including SIGINT capabilities, to prevent future acts of international terrorism against the United States. According to the memorandum, the AUMF was properly read as an express authorization to conduct targeted electronic surveillance against al-Qa'ida and its affiliates, the entities responsible for attacking the United States, thereby supporting the President's directives to conduct these activities under the PSP. Much of the legal reasoning in the 6 May 2004 OLC memorandum was publicly released by DoJ in a "White Paper"—"Legal Authorities Supporting the Activities of the National Security Agency Described by the President"—issued on 19 January 2006 after the content

---

(b) (5), (b)(1), (b)(3)
(b)(1), (b)(3)
[redacted]

collection portion of the program was revealed in *The New York Times* and publicly confirmed by the President in December 2005.

(U) Restrictions on Access to the President's Surveillance Program Impeded Department of Justice Legal Review

~~(TS//SI//OC/NF)~~ The DoJ IG found it extraordinary and inappropriate that a single DoJ attorney, John Yoo, was relied upon to conduct the initial legal assessment of the PSP, and that the lack of oversight and review of Yoo's work, which was contrary to the customary practice of OLC, contributed to a legal analysis of the PSP that, at a minimum, was factually flawed. Deficiencies in the legal memorandums became apparent once additional DoJ attorneys were read into the program in 2003 and those attorneys sought a greater understanding of the PSP's operation. The White House's strict controls over access to the PSP undermined DoJ's ability to provide the President the best available advice about the program. The DoJ IG also concluded that the circumstances plainly called for additional DoJ resources to be applied to the legal review of the program, and that it was the Attorney General's responsibility to be aware of this need and to take steps to address it. However, the DoJ OIG could not determine whether Ashcroft aggressively sought additional read-ins to assist with DoJ's legal review of the program prior to 2003 because Ashcroft did not agree to be interviewed.

(U) TRANSITION OF PRESIDENT'S SURVEILLANCE PROGRAM ACTIVITIES TO FOREIGN INTELLIGENCE SURVEILLANCE ACT AUTHORITY

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

~~(TS//SI//OC/NF)~~ [redacted] (b)(1), (b)(3)

~~(TS//SI//NF)~~ The government's FISA application, entitled "Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes," was filed [redacted] (b)(1), (b)(3) The application package included:

- A proposed order authorizing the collection activity and secondary orders mandating carriers to cooperate.
- A declaration by Hayden explaining the technical aspects of the proposed Internet metadata collection and identifying the government official

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.

~~(TS//SI//NF)~~ A second major compliance incident was brought to the FISC's attention in February 2005. Baker told us that he learned that the NSA was using information (b)(1), (b)(3) to satisfy the reasonable articulable suspicion standard for querying Internet metadata collected under FISC PR/TT Orders. Baker informed Kollar-Kotelly of this and on 17 February 2005, Kollar-Kotelly

entered an order requiring that this practice cease as to all newly targeted Internet communications addresses. The order also directed the NSA to perform an audit of all queries conducted under authority of the PR/TT Order to determine the extent to which the NSA (b)(1), (b)(3) as a basis for the queries. Further, on 15 March 2005, the FISC ordered that no Internet communication addres (b)(1), (b)(3) reasonable articulable suspicion be used to query the Internet metadata.

~~(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)

~~(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) 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) 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) 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) in support of the (b)(1), (b)(3) 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) 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) 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 (b)(1), (b)(3) 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) 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) call detail records rather than (b)(1), (b) 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) 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) 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 abou[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.

[redacted]

(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." b1, b3, b6, b7C, b7E

[redacted] PSP reporting assisted in locating his network's worldwide associates [redacted]

[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.

(b) (5), (b)(1), (b)(3)

~~(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.

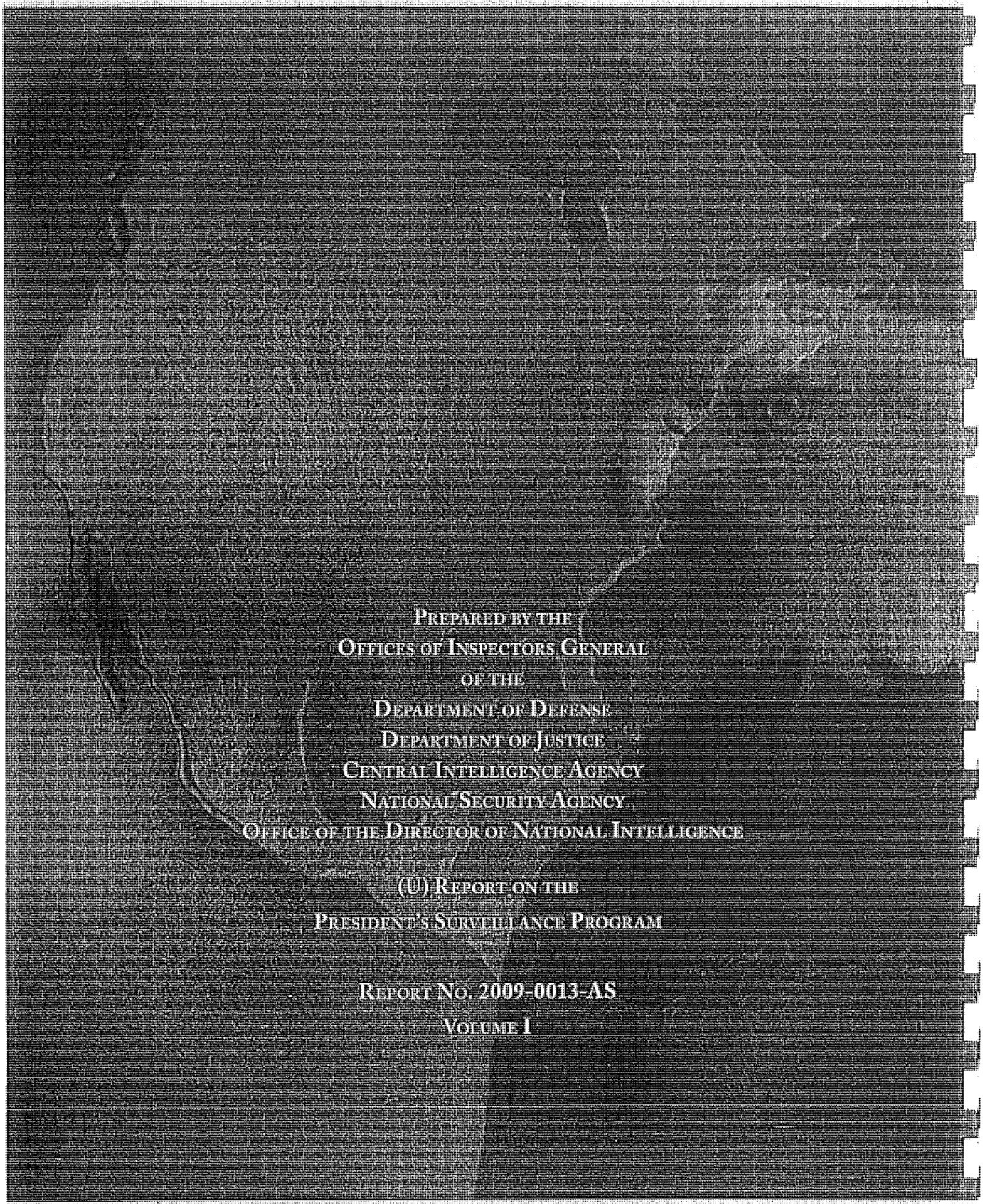
(U//~~FOUO~~) The IG reports describe the role of each of the participating agencies in the PSP, including the NSA's management and oversight of the collection, analysis, and reporting process; the CIA's and FBI's use of the PSP-derived intelligence in their counterterrorism efforts; the ODNI's support 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

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig

REDACTED – FOR PUBLIC RELEASE