

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

The Black Vault



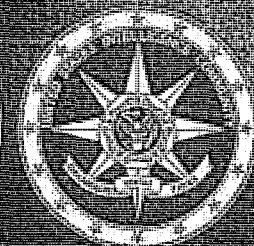
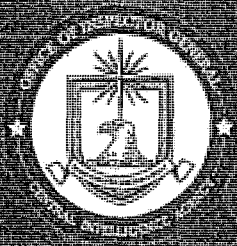
The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

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

(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-A

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100.

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.

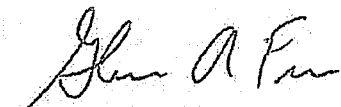
(U) Because many aspects of the PSP remain classified, and in order to provide the Congressional committees the complete results of our review, we have prepared this classified report on the PSP. The report is in three volumes:

- 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

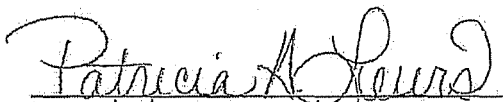
~~Derived From: NSA/CSSM 1-52, 2-400,
NSA/CSS M 1-52, 12-48
Dated: 20070108
Declassify On: 20340713~~



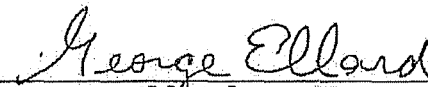
Glenn A. Fine
Inspector General
Department of Justice



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) INTRODUCTION..... | 1 |
| (U) Scope of the Review..... | 1 |
| (U) Methodology | 2 |
| (U) INCEPTION OF THE PRESIDENT'S SURVEILLANCE PROGRAM | 4 |
| (U) National Security Agency Counterterrorism Efforts Prior to
11 September 2001 | 4 |
| (U) NSA Initially Used Existing Authorities to Enhance Signals
Intelligence (SIGINT) Collection After the September 2001
Terrorist Attacks | 5 |
| (U) NSA Explored Options to Improve SIGINT Collection and
Address Intelligence Gaps on Terrorist Targets..... | 6 |
| (U) Impediments to SIGINT Collection Against Terrorist Targets
Were Discussed With the White House | 7 |
| (U) Authorization of the President's Surveillance Program | 7 |
| (U) SIGINT Activities Authorized Under the Program | 7 |
| (U) Content of the Presidential Authorizations and
Department of Justice Certification as to Form and Legality..... | 9 |
| (U) The Threat Assessment Memorandums Supporting
Presidential Authorization of the Program | 10 |
| (U) Early Revisions to the Presidential Authorizations..... | 11 |
| (U) DoJ Office of Legal Counsel Memorandums Supporting
Legality of the Program | 12 |
| (U) IMPLEMENTATION OF THE PRESIDENT'S SURVEILLANCE
PROGRAM | 16 |
| (U) NSA Implementation..... | 16 |
| | 17 |

| | |
|--|----|
| (TS//SI//NF) Telephone and Internet Communications
Content Collection and Analysis | 18 |
| (TS//SI//NF) Telephony and Internet Metadata Collection and
Analysis | 20 |
| (U) NSA Reporting From the President's Surveillance
Program | 21 |
| (U) NSA Managerial Structure and Oversight of the President's
Surveillance Program | 22 |
| (U) NSA Management Controls to Ensure Compliance With
Presidential Authorizations | 23 |
| (U) NSA Inspector General Oversight of the Program | 24 |
| (U) Access to the President's Surveillance Program | 25 |
| (U) Congressional Briefings on the Program | 26 |
| (U) Foreign Intelligence Surveillance Court Briefings on the
Program | 27 |
| (U) FBI Participation in the President's Surveillance Program | 28 |
| (U) CIA Participation in the President's Surveillance Program | 30 |
| (U) NCTC Participation in the President's Surveillance Program | 32 |
| (U) The President's Surveillance Program and the Foreign
Intelligence Surveillance Court | 33 |
| (U) Discovery Issues Associated With the President's
Surveillance Program | 35 |
| (U) LEGAL REASSESSMENT OF THE PRESIDENT'S SURVEILLANCE
PROGRAM (2003 - 2004) | 36 |
| (TS//SI//NF) Concern Over the [REDACTED]
[REDACTED] Collection | 36 |
| (U) A New Legal Basis for the Program Is Adopted | 37 |
| (U) Department of Justice Officials Convey Concerns About the
Program to the White House | 39 |
| (U) Conflict Between the Department of Justice and the White
House Over the Program | 40 |

| | |
|--|----|
| (S//NF) White House Counsel Certifies Presidential Authorization Without Department of Justice Concurrence..... | 44 |
| (TS//SI//NF) White House Agrees to [REDACTED]..... | 48 |
| (U) Restrictions on Access to the President's Surveillance Program Impeded Department of Justice Legal Review | 50 |
| (U) TRANSITION OF PRESIDENT'S SURVEILLANCE PROGRAM ACTIVITIES TO FOREIGN INTELLIGENCE SURVEILLANCE ACT AUTHORITY | 50 |
| (TS//SI//NF) Internet Metadata Collection Transition to Operation Under FISA Authority | 50 |
| (U) Department of Justice Notices of Compliance Incidents | 53 |
| (TS//SI//NF) Telephony Metadata Collection Transition to Operation Under FISA Authority | 54 |
| (TS//SI//NF) Content Collection Transition to Operation Under FISA Authority..... | 57 |
| (U) IMPACT OF THE PRESIDENT'S SURVEILLANCE PROGRAM ON INTELLIGENCE COMMUNITY COUNTERTERRORISM EFFORTS | 60 |
| (U) Senior Intelligence Community Officials Believe That the President's Surveillance Program Filled an Intelligence Gap | 60 |
| (U) Difficulty in Assessing the Impact of the President's Surveillance Program..... | 61 |
| (U) Impact of the President's Surveillance Program on FBI Counterterrorism Efforts..... | 61 |
| (U) FBI Efforts to Assess the Value of the Program..... | 62 |
| (U) FBI Judgmental Assessments of the Program..... | 62 |
| (U) Impact of the President's Surveillance Program on CIA Counterterrorism Operations | 63 |
| (U) The CIA Did Not Systematically Assess the Effectiveness of the Program..... | 63 |
| (U) Several Factors Hindered CIA Utilization of the Program | 64 |

| | |
|--|----|
| (U) Impact of the President's Surveillance Program on NCTC Counterterrorism Efforts..... | 65 |
| (U) Counterterrorism Operations Supported by the President's Surveillance Program..... | 65 |
| (U) ATTORNEY GENERAL GONZALES'S TESTIMONY ON THE PRESIDENT'S SURVEILLANCE PROGRAM..... | 68 |
| (U) CONCLUSIONS..... | 69 |

(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.

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)



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.¹ 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]

[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] [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.

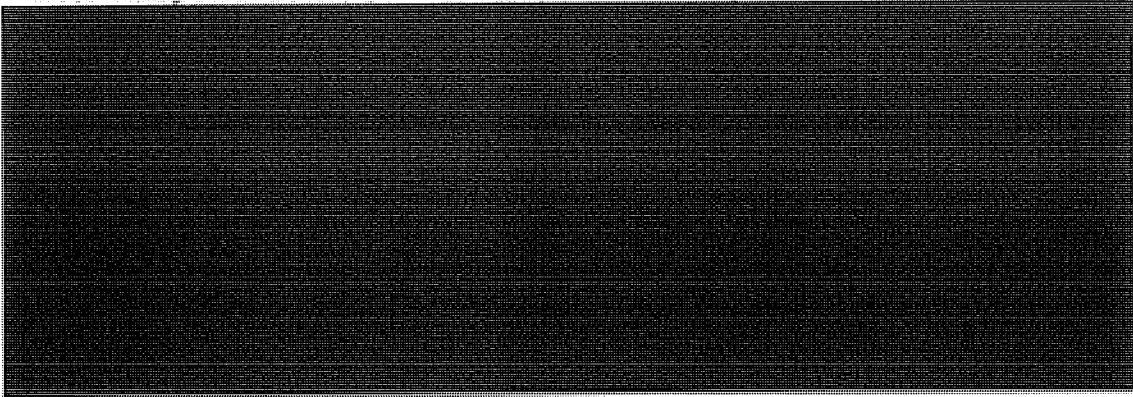
⁵ ~~(S//SI//NF)~~ Dialing analysis/contact chaining is the process of [REDACTED] from the communications sent or received by targeted entities.

**(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.



**(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)

[REDACTED] 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)

[REDACTED]

~~(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."



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.

(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.

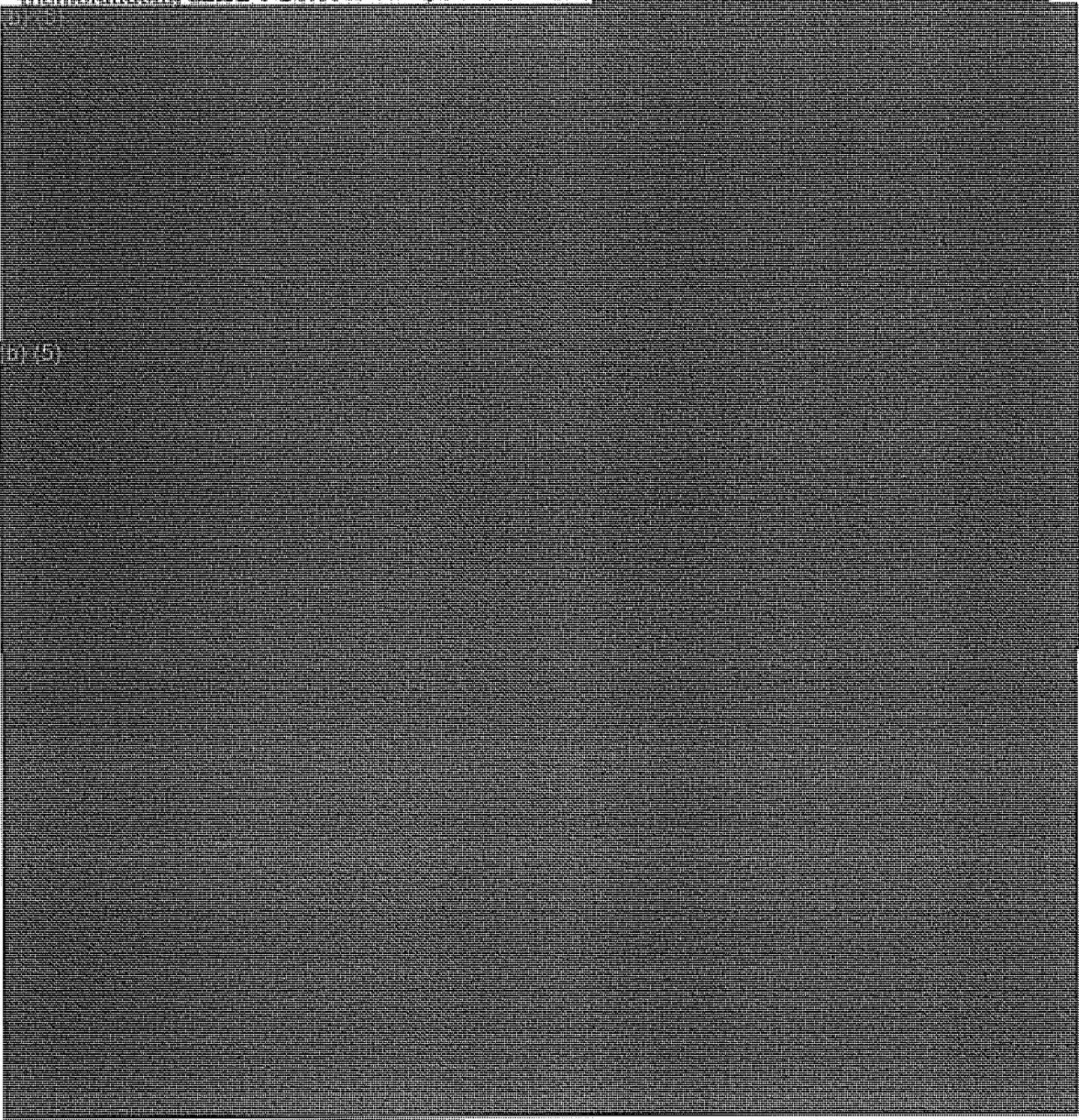
(b)(1), (b)(3)

**(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) (5)

~~(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) (5)

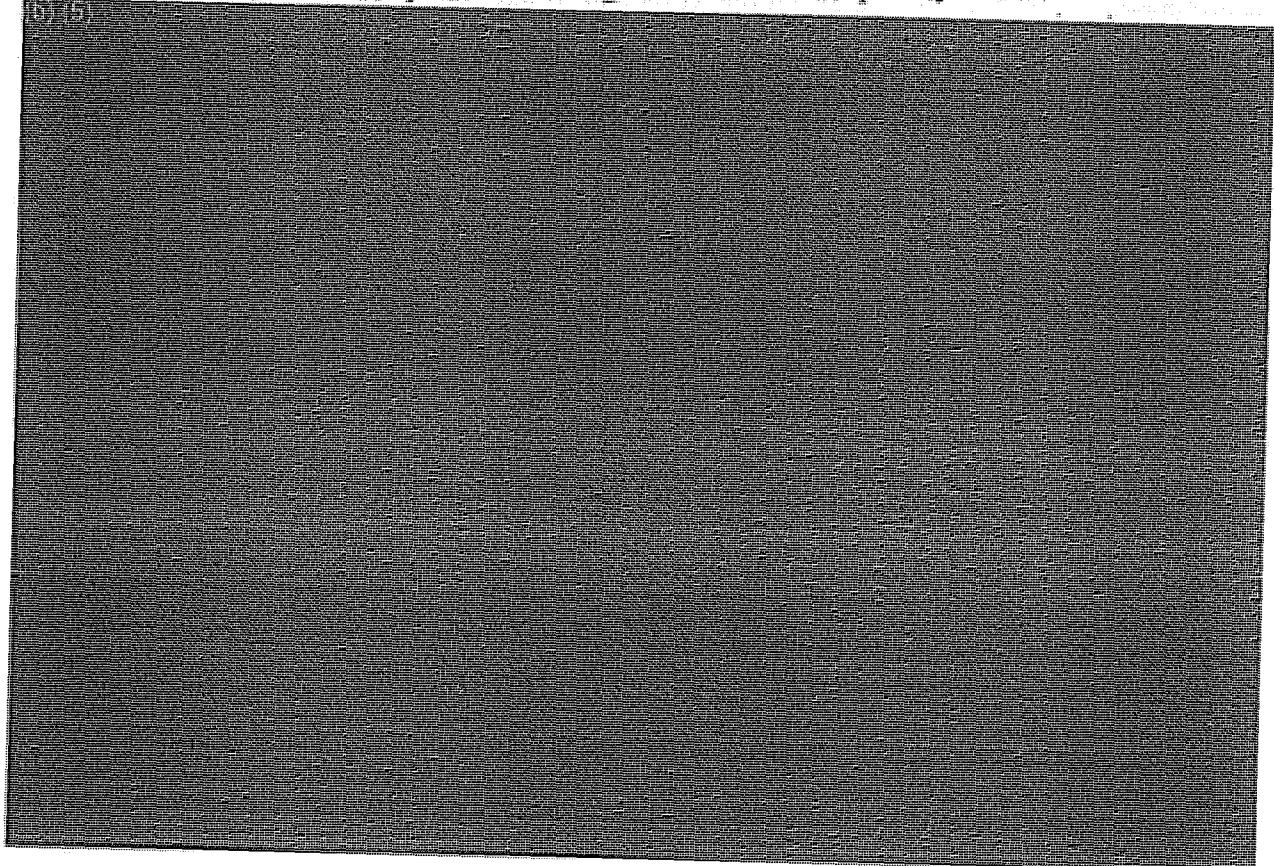
~~(S//NF)~~ Yoo acknowledged in his 2 November 2001 memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence." But Yoo then opined that "[s]uch a 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)} [REDACTED]

[REDACTED] "[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.



~~(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)



**(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)



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

(b) (3)



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



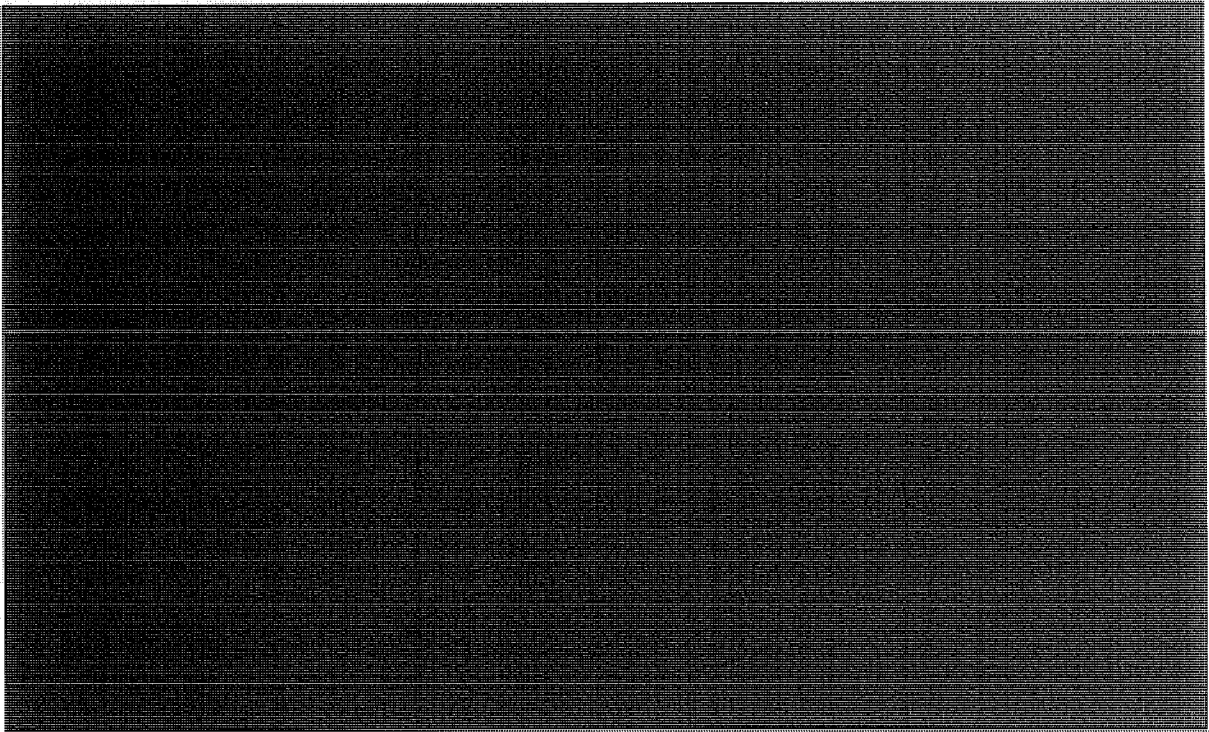
b1,
b3,
b7D,
b7E

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

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



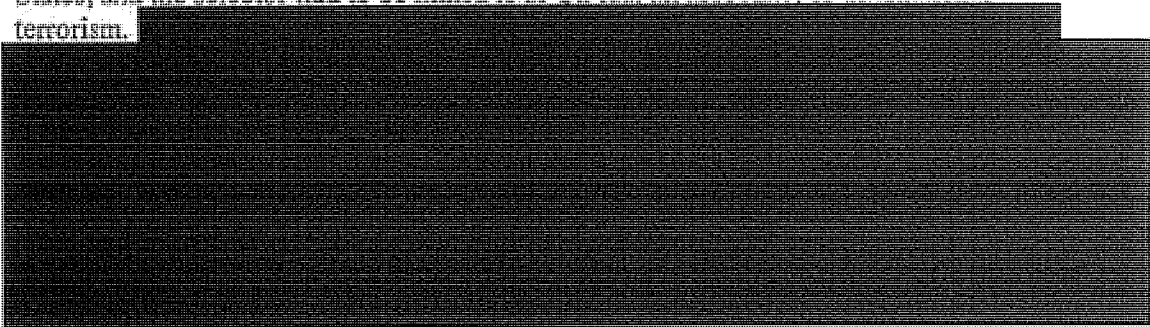
b1,
b3,
b7E



b1, b3,
b7E

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

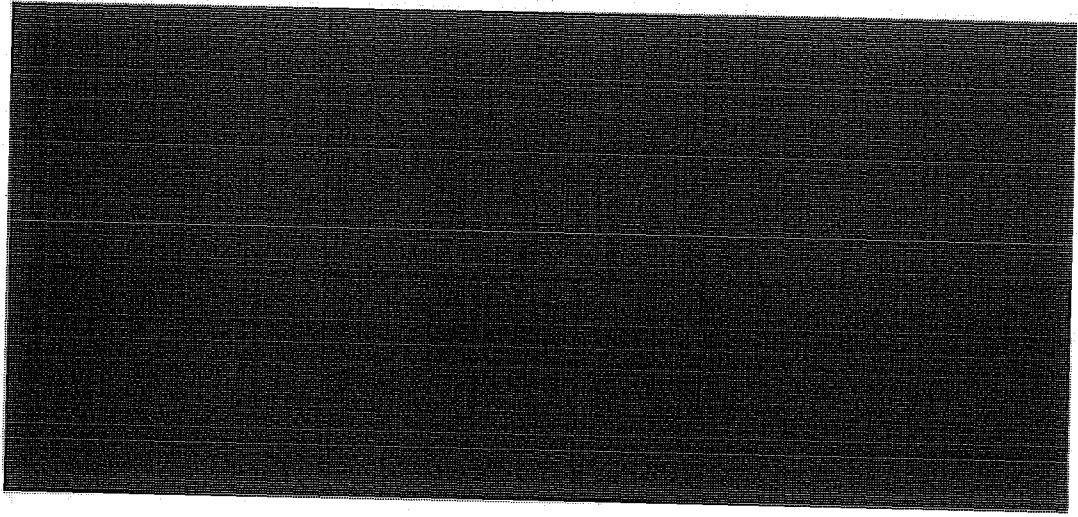
~~(TS//SI//NF)~~ Content collection and analysis under the PSP was conducted in the same manner as collection and analysis conducted previously by the NSA under E.O. 12333 authority. NSA management applied standard minimization and specially designed procedures to task domestic selectors such as telephone 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 that [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.



~~(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.