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

Report on the President's Surveillance Program

Volume II

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 II" 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
II	122

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME II

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

(U) Table of Contents

This page intentionally left blank.

~~TOP SECRET//STLW//SI//ORCON//NOFORN~~
~~SPECIAL ACCESS REQUIRED~~

Report No. 09-INTEL-03
27 March 2009
(Project

Inspector General
United States
Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Review of the President's Surveillance Program (U)

~~Derived From: Multiple Sources~~
~~Declassify On: 20340511*~~

Copy ____ of ____

This page intentionally left blank.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 26, 2009

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: (U) Report on Review of the President's Surveillance Program Report No.: 09-INTEL-08 (U)

(U) We are providing this report for your information. This report fulfills the DoD Inspector General's requirement pursuant to Section 301 of Public Law 110-261, the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (the Act). This report, along with reports prepared by the Inspectors General of the Department of Justice (DoJ), the Office of the Director of National Intelligence (DNI), Central Intelligence Agency (CIA), the National Security Agency (NSA), will be summarized in a comprehensive report as required by the Act.

~~(TS//STLW//SI//OC//NF)~~ **Results.** The OSD role in the establishment and implementation of the PSP was limited, with the burden of program execution residing with the NSA. We determined that there were six OSD officials with access to the PSP. These individuals had limited involvement, and did not make any additional tasking decisions beyond those directed for NSA implementation. We are aware of no other OSD involvement in the PSP.

(U) Background. The Act requires the IGs of the DoJ, DNI, NSA, the DoD, and any other element of the intelligence community that participated in the President's Surveillance Program (PSP)[1], to complete a comprehensive review of, with respect to the oversight authority and responsibility of each such IG:

- All facts necessary to describe establishment, implementation, product and use of the product in the program
- Access to legal reviews and access to information about the Program
- Communications and participation of individuals/entities related to the Program

[1] (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 September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

~~Derived from: Multiple Sources~~
~~Declassify on: 20340511*~~

- Interaction with the Foreign Intelligence Surveillance Court and
- Any other matters identified by the IGs

~~(TS//STLW//SI//OC//NF)~~ **Scope and Methodology.** We conducted this review to examine the involvement of the Office of the Secretary of Defense (OSD), Department of Defense (DoD), in the establishment and implementation of the President's Surveillance Program (PSP). We interviewed current and former officials within OSD that had access to the PSP. We withdrew our request to interview Secretary of Defense Gates because he was provided access to the PSP after the program ended. The former Deputy Secretary of Defense Dr. Wolfowitz declined our request for an interview. We reviewed all relevant documentation within OSD and NSA related to OSD's involvement in the PSP. We also reviewed documentation at DoJ related to the PSP.

(U) The IGs of the DoJ, DoD, DNI, NSA, and CIA issued an interim report on September 10, 2008. In the interim report, the DoD IG stated that he would examine the involvement of the Office of the Secretary of Defense (OSD) in the establishment and implementation of the PSP. The NSA, as an agency within DoD performed the requirements of the PSP. As such, the NSA IG is conducting a review of NSA involvement with the PSP separate from this memorandum report.

~~(TS//STLW//SI//OC//NF)~~ **Implementation and Establishment of the PSP.** The OSD access to the PSP was limited to six individuals.[2] Those individuals are Secretary of Defense Robert Gates; former Secretary of Defense Donald Rumsfeld; former Deputy Secretary of Defense Paul Wolfowitz; Under Secretary of Defense for Intelligence (USD(I)) James Clapper[3]; former USD(I) Stephen Cambone; and Principal Deputy General Counsel Daniel Dell 'Orto.

~~(TS//STLW//SI//OC//NF)~~ The PSP was an extremely sensitive counterterrorism program focused on detecting and preventing terrorist attacks within the United States. The PSP was authorized by the President every 30 to 45 days and was initially directed against international terrorism; after March 2004, the PSP focused specifically against al-Qaeda and its affiliates. The Director of Central Intelligence (DCI), and later the DNI, would prepare a Threat Assessment

[redacted]

[3] ~~(TS//STLW//SI//OC//NF)~~ Secretary Gates and Under Secretary Clapper were provided access to the PSP after the PSP was transferred to Foreign Intelligence Surveillance Court supervision.

Memorandum, which validated the current threat to the United States. The Secretary of Defense would review and sign the Threat Assessment Memorandum. On three occasions, Dr. Wolfowitz, the former Deputy Secretary of Defense, signed the Threat Assessment Memoranda in the Secretary's absence. On two occasions, Dr. Cambone, the former USD(I), signed the Threat Assessment Memoranda when Secretary Rumsfeld and Dr. Wolfowitz were unavailable.

~~(TS//STLW//SI//OC//NF)~~ Once the Threat Assessment Memorandum was signed, the President would then sign a Presidential Authorization with the Threat Memorandum attached. The President would task the Secretary of Defense to employ DoD resources to execute the requirements set forth in the Presidential Authorization. The Attorney General, or his designee, would certify the Presidential Authorization for form and legality. The Secretary of Defense would then direct the actions authorized by the Presidential Authorization to the NSA for implementation. On one occasion, Dr. Wolfowitz, the former Deputy Secretary of Defense, directed the Director of NSA to implement the Presidential Authorization, in the Secretary's absence. On a separate occasion, Dr. Cambone, the former USD(I), directed the Director of NSA to implement the Presidential Authorization.

~~(TS//SI//NF)~~ **Interaction with the Foreign Intelligence Surveillance Court.** Dr. Wolfowitz also executed two declarations to the U.S. Foreign Intelligence Surveillance Court. The first, executed on [redacted] was in support of the Government's Application seeking renewal, in part, of the authority to install and use pen register and trap and trace devices, in order to obtain information [redacted] pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. sections 1801-1811, 1841-1846, as amended. The initial authority under FISA to install and use pen register and trap and trace devices for that purpose was granted by the Foreign Intelligence Surveillance Court on July 14, 2004. [redacted]

~~(TS//SI//NF)~~ Dr. Wolfowitz's second declaration was executed on [redacted] That declaration was made in response to the Foreign Intelligence Surveillance Court's [redacted] Order requiring the Government to submit a declaration from the Deputy Secretary of Defense discussing NSA' violations of the Court's July 14 Order authorizing NSA to install and use pen register and trap and trace devices in order to obtain information about [redacted]. In that declaration, Dr. Wolfowitz stated the circumstances surrounding unauthorized collection that occurred, the disposition of information collected without authorization, steps NSA took to remedy the violation, and measures NSA implemented to prevent recurrence of such violations.

(TS//STLW//SI//ORCON/NOFORN)

(U) Should you have questions on this memo, please feel free to contact [illegible], Patricia A. Dunmire at (703) 613-8879.

[illegible]

APPENDIX (U)

REPORT DISTRIBUTION LIST (U)

(U)

OFFICE OF THE SECRETARY OF DEFENSE

Secretary of Defense
Under Secretary of Defense for Intelligence
Deputy General Counsel, Intelligence

OTHER DEFENSE ORGANIZATION

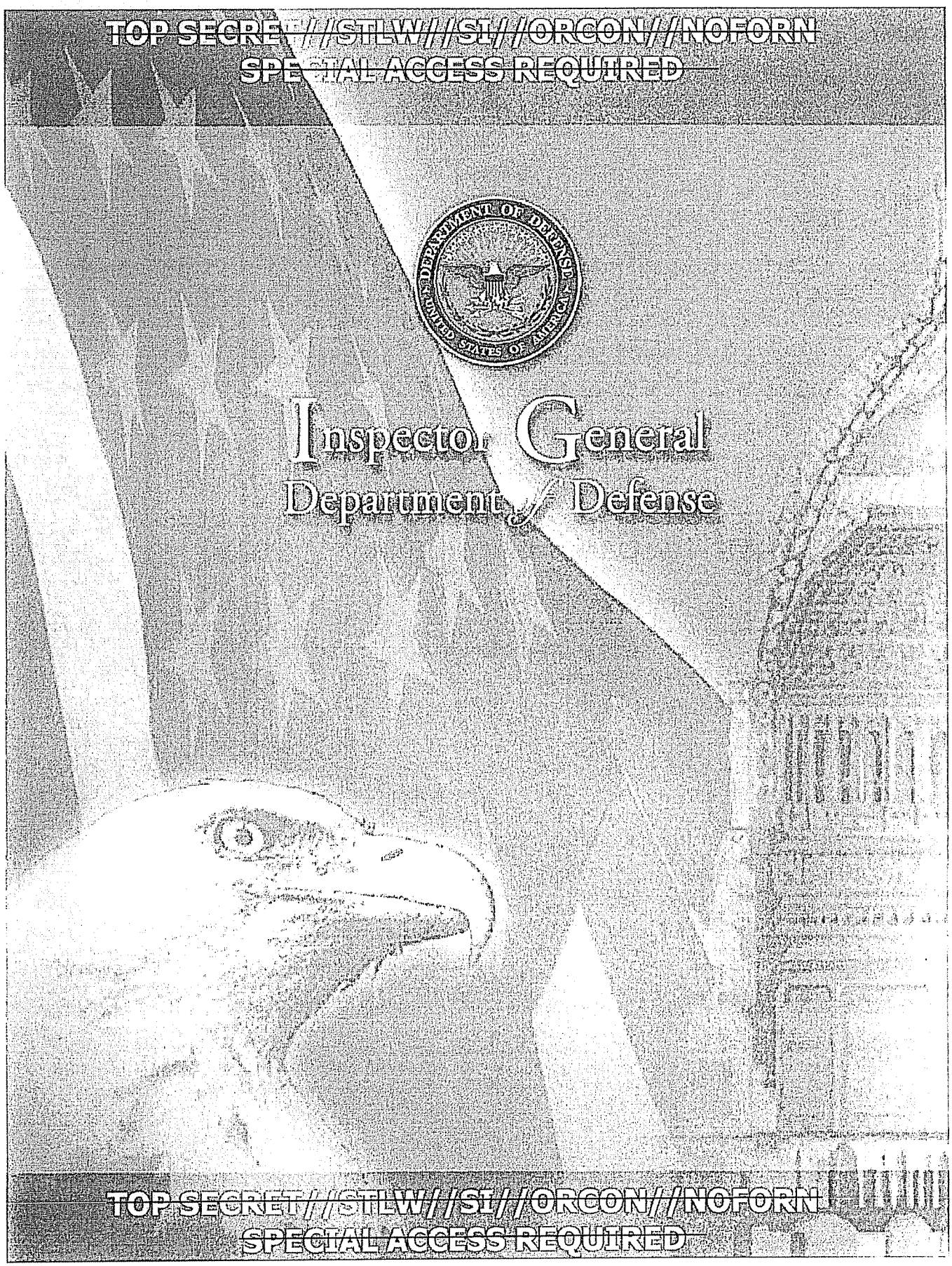
Inspector General, National Security Agency

NON-DEFENSE FEDERAL ORGANIZATIONS

Inspector General, Director of National Intelligence
Inspector General, Department of Justice
Inspector General, Central Intelligence Agency

CONGRESSIONAL COMMITTEES

Senate Judiciary Committee
Senate Select Committee on Intelligence
House Judiciary Committee
House Permanent Select Committee on Intelligence


TOP SECRET//STLW//SI//ORCON//NOFORN
SPECIAL ACCESS REQUIRED
Inspector General
Department of Defense
TOP SECRET//STLW//SI//ORCON//NOFORN
SPECIAL ACCESS REQUIRED

This page intentionally left blank.

This page intentionally left blank.

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

CENTRAL INTELLIGENCE AGENCY

Office of Inspector General

(U) FINAL REPORT

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

Report No. 2008-0016-AS

[redacted]

30 June 2009

Issue Date

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

This page intentionally left blank.

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

(U) Table of Contents

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

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

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

(U) EXECUTIVE SUMMARY

~~(S//NF)~~ Title III of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 requires the Inspectors General (IGs) of the elements of the Intelligence Community (IC) that participated in the President's Surveillance Program (PSP) to conduct a comprehensive review of the program. The results of our review of CIA participation in the PSP are presented in this report, and will be included in the comprehensive report required to be provided to the appropriate committees of Congress by 10 July 2009.

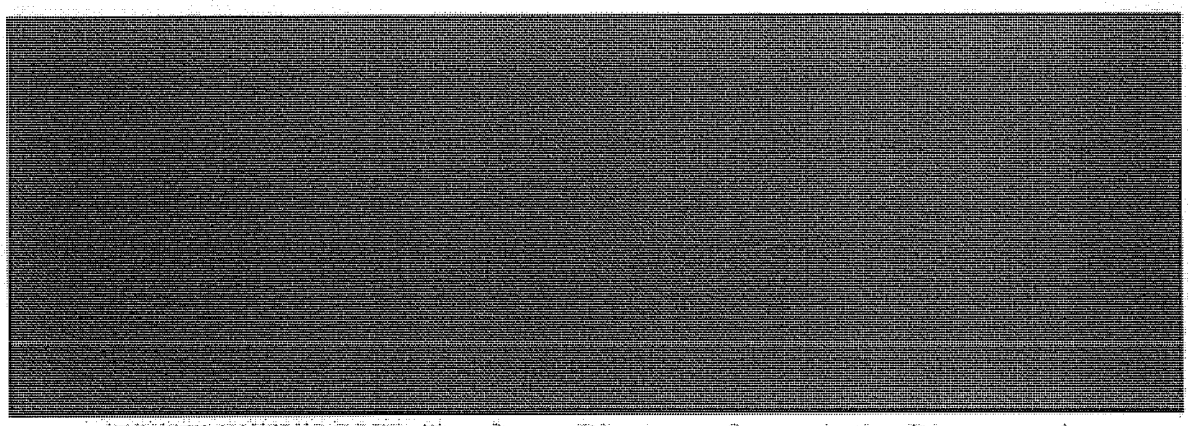
~~(TS//STLW//SI//OC/NF)~~ The CIA prepared the threat assessment memorandums that were used to support Presidential authorization and periodic reauthorizations of the PSP. The threat assessment memorandums were prepared by personnel from the CIA [redacted] Each of the memorandums focused on the current threat situation and did not provide an assessment of the PSP's utility in addressing previously reported threats. The threat assessment memorandums were signed by the Director of Central Intelligence (DCI) and forwarded to the Secretary of Defense to be co-signed. Responsibility for drafting the threat assessment memorandums was transferred to the newly-established Terrorist Threat Integration Center in May 2003 and retained by TTIC's successor organization, NCTC (the National Counterterrorism Center). The DCI continued to sign the threat assessment memorandums through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence.

~~(TS//STLW//SI//OC/NF)~~ CIA analysts and targeters, as PSP consumers, tasked the program and utilized the product from the program in their analyses. [redacted]

1

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

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



~~(TS//STLW//SI//OC/NF)~~ Two former Directors, a former Acting Director, and other senior CIA officials we interviewed told us that the PSP addressed a gap in intelligence collection. [redacted] However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC and CIA officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat. Current and former CIA officials emphasized the increased timeliness, flexibility, and access provided by the PSP as compared to the process for obtaining a warrant under FISA.

~~(TS//STLW//SI//OC/NF)~~ The CIA did not implement procedures to 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 told us that PSP reporting was used in conjunction with reporting from other intelligence sources and was rarely the sole basis for a counterterrorism success. [redacted] CIA officers, even those read into the program, would have been unaware of the full extent of PSP reporting. Consequently, 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 therefore, we were unable to independently draw any conclusion on the overall usefulness of the program to CIA.

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

~~(S//NF)~~ 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. [redacted] officials told us that CIA analysts and targeting officers who were read in had too many competing priorities and too many other available information sources and analytic tools—many of which were more easily accessed and timely—to fully utilize the PSP. CIA officers also told us that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. Many CIA officers noted that there was insufficient training and legal guidance concerning the program's capabilities and the use of PSP-derived information. 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.

~~(TS//STLW//SI//OC/NF)~~ There is no indication that personnel from the CIA Office of General Counsel or other CIA components were involved in preparing the legal memorandums supporting the PSP that were produced by the Department of Justice, Office of Legal Counsel (OLC). CIA OGC personnel had very limited access to these memorandums.

~~(S//NF)~~ Senior CIA officials participated in meetings with a *New York Times* editor and reporter and senior Administration officials concerning an article the newspaper was preparing concerning the PSP.

[redacted]
Assistant Inspector General for Audit

This page intentionally left blank.

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

(U) BACKGROUND

(U) Origin and Scope of the Review

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008, which was signed into law on 10 July 2008, requires the IGs of the elements of the Intelligence Community that participated in the PSP to conduct a comprehensive review of the program.[1] The review required to be conducted under the Act is to 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.

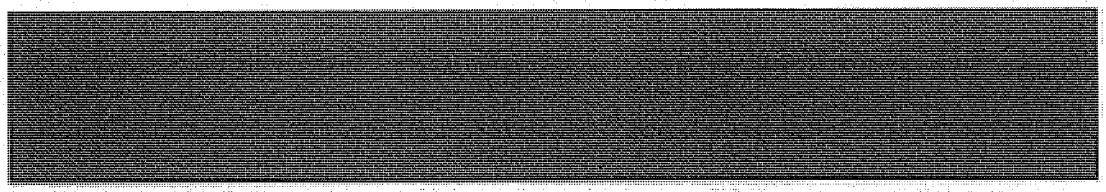
~~(TS//STLW//SI//OC/NF)~~ The interim report required under the Act was submitted to the committees of Congress prescribed in the Act on 10 September 2008. That report described the scope of the work to be conducted by each of the participating IGs, which include the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and the CIA. Our review of CIA participation in the PSP examined CIA's :

- Role in preparing the threat assessments and legal certifications supporting periodic reauthorization of the PSP.
- Role in identifying targets for the PSP.

---

[1] ~~(S//NF)~~ 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). The classified name for the President's Surveillance Program is "STELLARWIND."

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



The results of our review of CIA participation in the PSP are presented in this report, and will be included in the comprehensive final report required to be provided to the appropriate committees of Congress by 10 July 2009.

(U) The President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ According to former Director of the NSA and former Director of the CIA (DCIA) Michael V. Hayden, initial discussions concerning the activities that would become the PSP occurred less than two weeks after the 11 September 2001 terrorist attacks in a meeting between DCI George J. Tenet and Vice President Richard B. Cheney. Although Hayden did not attend the meeting, he was told by Tenet that Cheney asked if the Intelligence Community was doing everything possible to prevent another terrorist attack. In response, Tenet described

Cheney then asked if there was more that NSA could do. This led to discussions between Cheney, Hayden, Cheney's legal counsel David S. Addington, and senior NSA officials. It was determined that the NSA had the capability to collect additional wire communications that could enhance the IC's counterterrorism efforts, but that new authority was needed to employ the capability. The determination led to the authorization of the PSP by President George W. Bush on 4 October 2001.

~~(TS//STLW//SI//OC/NF)~~ The PSP was intended to help prevent additional terrorist attacks against the US Homeland. Although the authorized collection activities changed over the life of the program, in general, the program authorized the NSA to acquire content and/or metadata concerning telephone and e-mail communications for which there were reasonable grounds to believe that at least one of the participants in the communication was located outside the US and that a party to

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

the communication was affiliated with a group engaged in international terrorism. The collection activities conducted under the PSP were brought under Foreign Intelligence Surveillance Court oversight in stages between July 2004 and January 2007.[2]

~~(TS//STLW//SI//OC/NF)~~ Under the PSP, the NSA collected three sets of data. The first set included the content of individually targeted telephone and e-mail communications. The second set consisted of telephone dialing information—the date, time, and duration of calls; the telephone number of the caller; and the number receiving the call—collected in bulk [redacted] The third data set consisted of e-mail transactional data—[redacted] collected in bulk [redacted]

(U) REVIEW RESULTS

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

[redacted]

[2] (U) The Foreign Intelligence Surveillance Act of 1978 established the Foreign Intelligence Surveillance Court to oversee requests for surveillance warrants by federal agencies against suspected foreign intelligence agents inside the US.

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

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

[redacted]

~~(TS//STLW//SI//OC/NF)~~ [redacted] CIA personnel prepared the threat assessment memorandums that were used to support the initial Presidential authorization and subsequent reauthorizations of the PSP. [redacted]

~~(TS//STLW//SI//OC/NF)~~ CIA Prepared the Threat Assessment Memorandums Supporting Authorization of the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ The CIA initially prepared the threat assessment memorandums that were used to support Presidential authorization and periodic reauthorizations of the PSP. The memorandums documented the current threat to the US homeland and to US 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 DCI Tenet on 4 October 2001.[3] Subsequent threat assessment memorandums were prepared every 30 to 60 days to correspond with the President's reauthorizations of the PSP.

~~(TS//STLW//SI//OC/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 [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. Initially, the [redacted] analysts who prepared the threat assessments were not read into the PSP and did not know how the threat assessments would be used. [redacted] analysts drew upon all sources of intelligence in preparing their threat assessments. Each of the memorandums focused on the current threat situation and did not provide an assessment of the PSP's utility in addressing previously reported threats.

---

[3] ~~(S//NF)~~ The title of the threat assessment memorandums was changed to *The Global War Against Terrorism* in June 2002.

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

~~(TS//STLW//SI//OC/NF)~~ After [redacted] completed its portion of the memorandums, the DCI's Chief of Staff 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 US. Moseman recalled that the paragraph was provided to him initially by either White House Counsel Alberto R. Gonzales or Addington. The paragraph recommended that the President authorize the Secretary of Defense to employ within the US the capabilities of the Department of Defense, including but not limited to NSA's signals intelligence capabilities, to collect foreign intelligence by electronic surveillance. The paragraph also described the types of communication and data that would be collected and the circumstances under which they could be collected.[4] The draft threat assessment memorandums were then reviewed by Office of General Counsel attorneys assigned to [redacted] and Acting General Counsel (Senior Deputy General Counsel) John A. Rizzo. Rizzo told us that the draft memorandums were generally sufficient, but that 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 tha[redacted] provide additional available threat information or make revisions to the draft memorandums.

~~(TS//STLW//SI//OC/NF)~~ The threat assessment memorandums were then signed by DCI Tenet and forwarded to the Secretary of Defense to be co-signed. Tenet signed most of the threat memorandums prepared during his tenure as DCI. On the few occasions when he was unavailable, the Deputy Director of Central Intelligence (DDCI), John E. McLaughlin, signed the memorandums on behalf of Tenet. McLaughlin also signed the memorandums in the capacity of Acting DCI in August and September 2004. In November 2004, Porter J. Goss became DCI and assumed responsibility for signing the memorandums. There were no occasions when the DCI or Acting DCI withheld his signature from the threat assessment memorandum. After they were signed by the Secretary of Defense, the memorandums were reviewed by the Attorney General and delivered to the White House to be attached to the PSP reauthorization memorandums signed by the President.

~~(TS//STLW//SI//OC/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

---

[4] (U) Exhibit B presents the conclusion and recommendation paragraph included in the threat assessment memorandum dated 10 January 2005. Similar language was included in each of the memorandums.

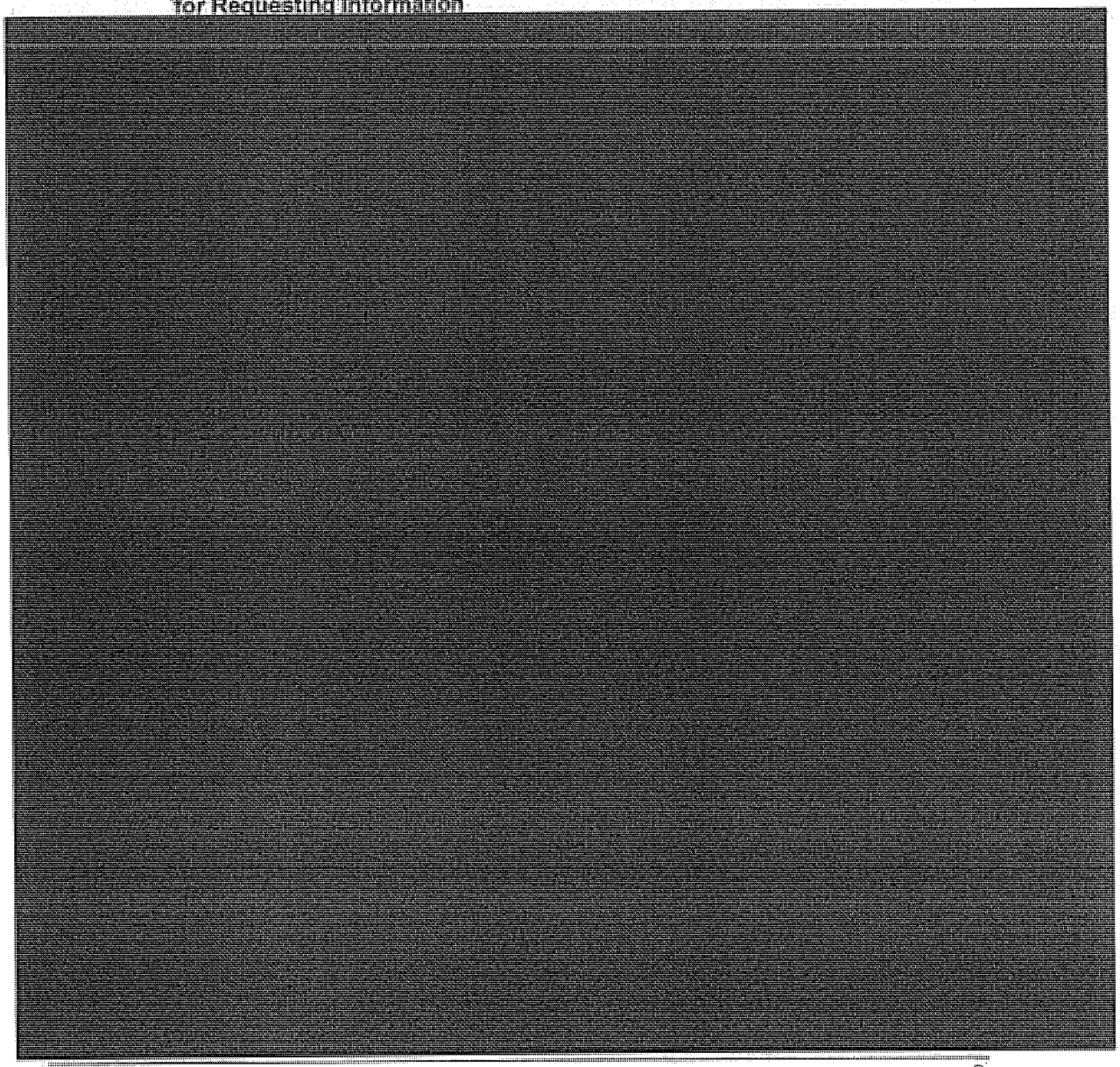
~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

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

through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence.[5]

(U//~~FOUO~~) CIA Tasked and Received Reporting From the President's Surveillance Program

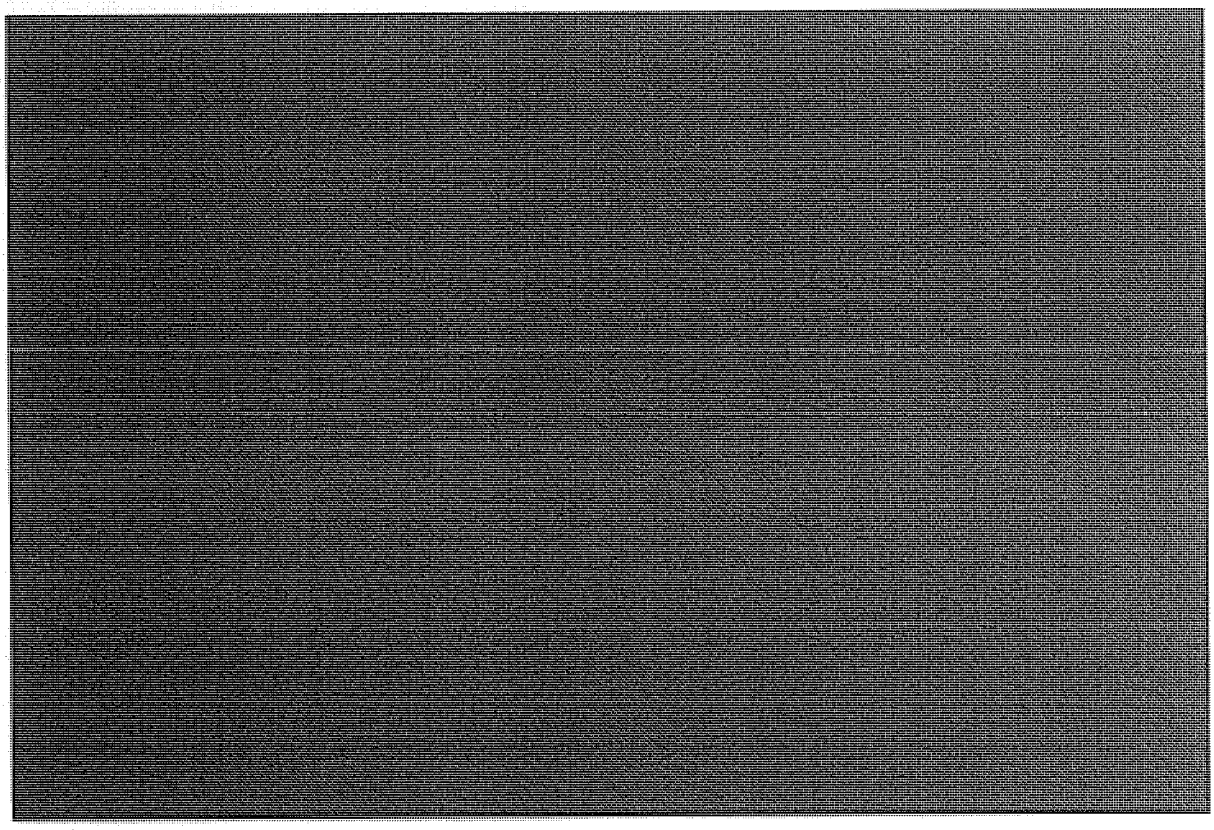
(U//~~FOUO~~) Procedures and Standards for Requesting Information



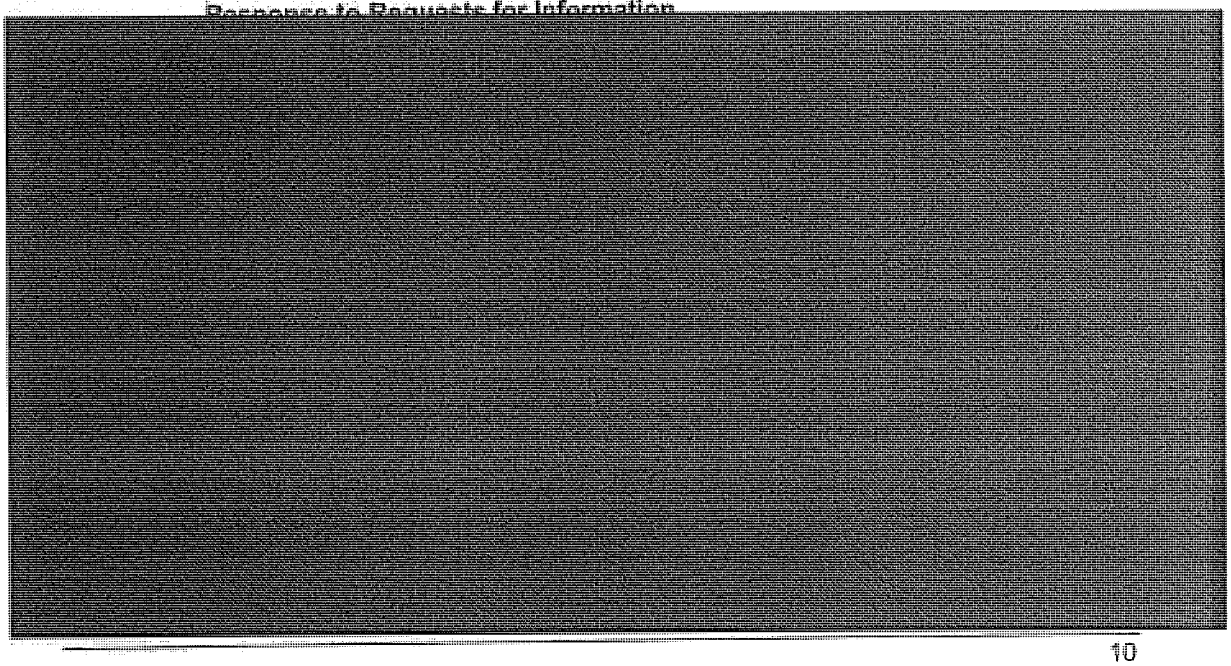
9

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

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



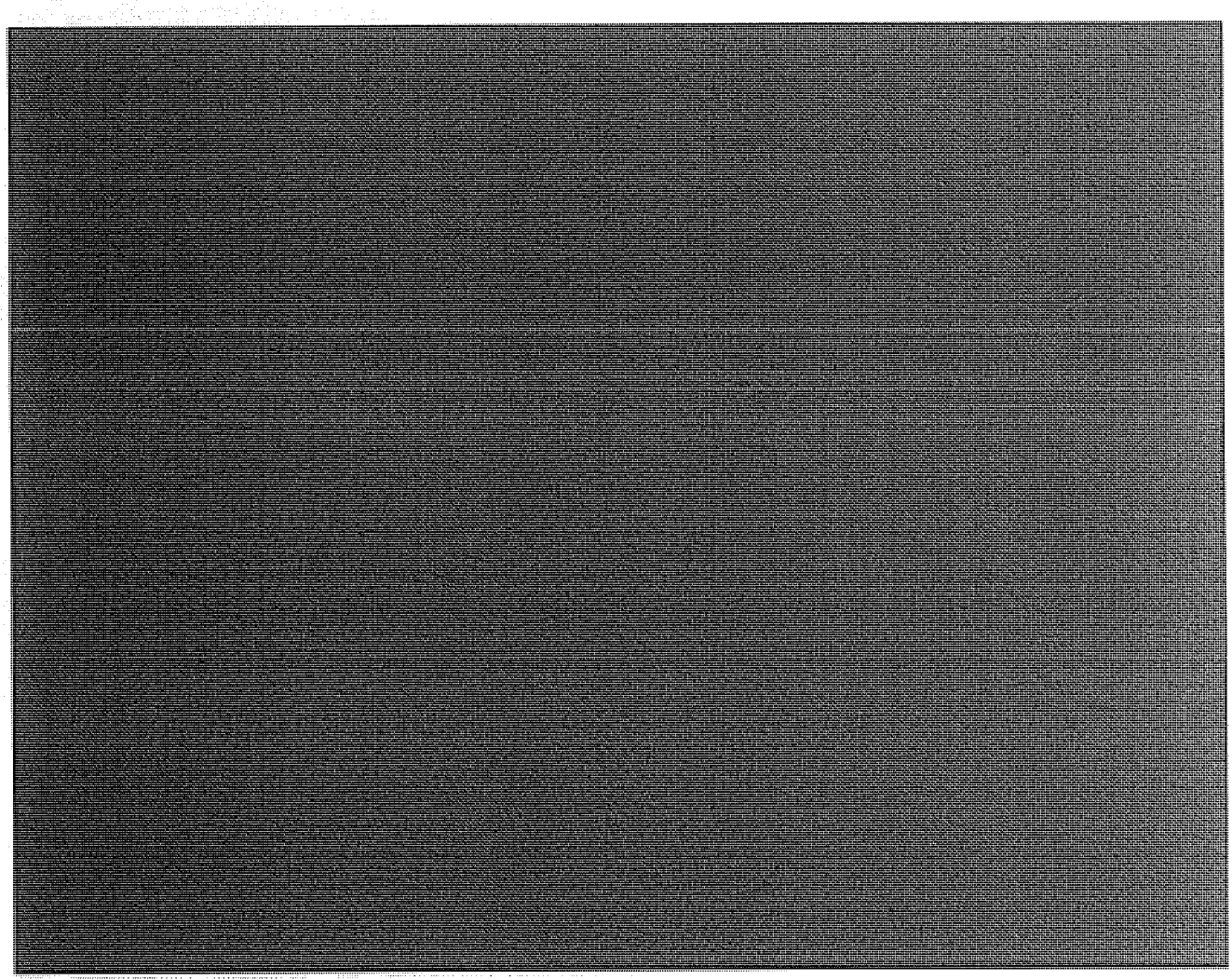
(U//FOUO) Reporting Provided in
Response to Requests for Information



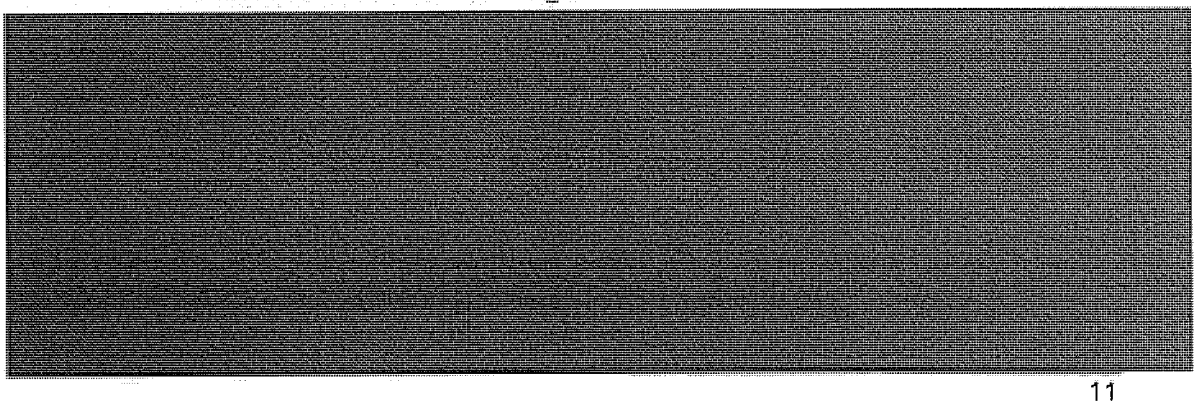
10

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

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



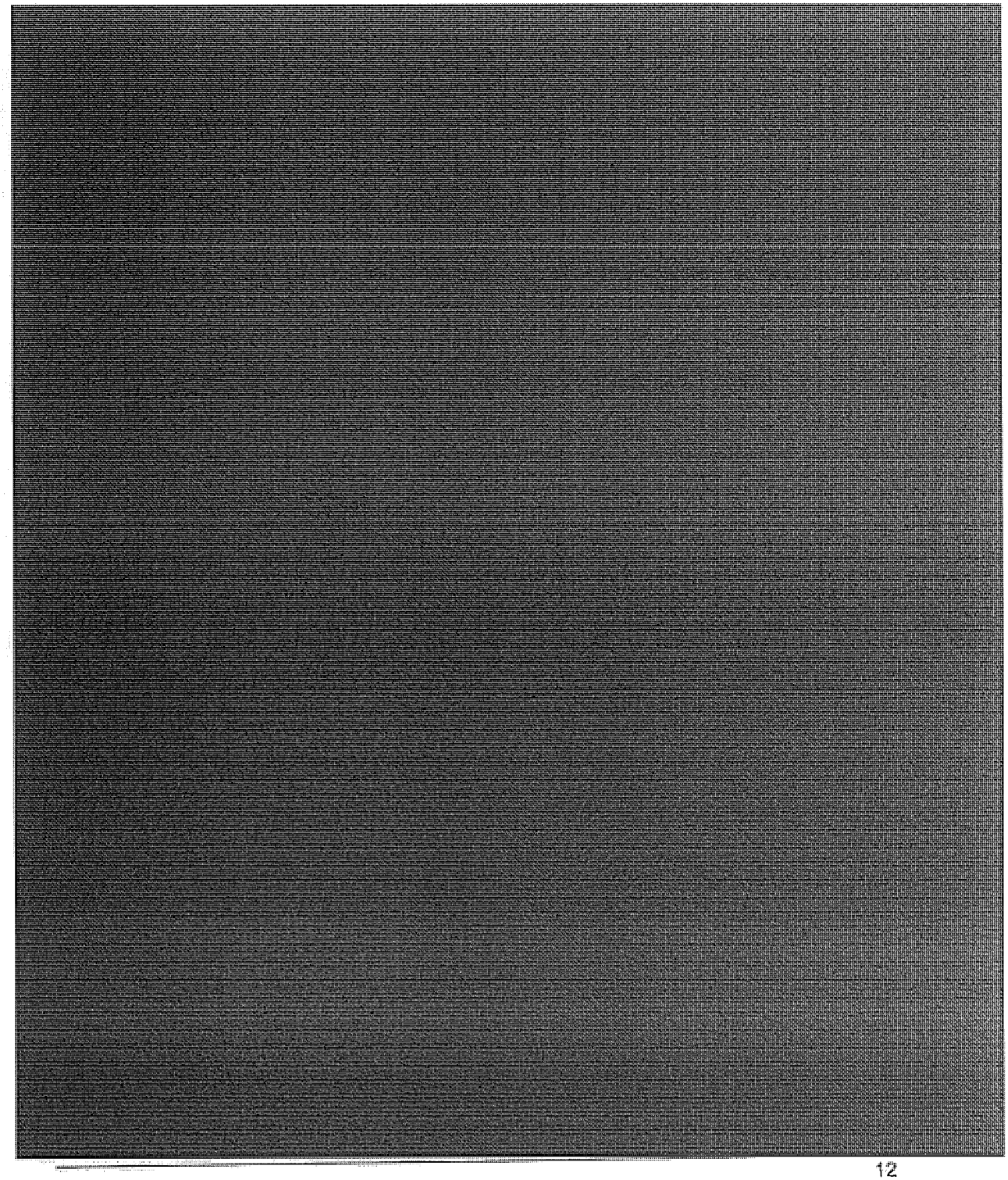
(U//~~FOUO~~) Primary CIA Users of the President's Surveillance Program



11

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

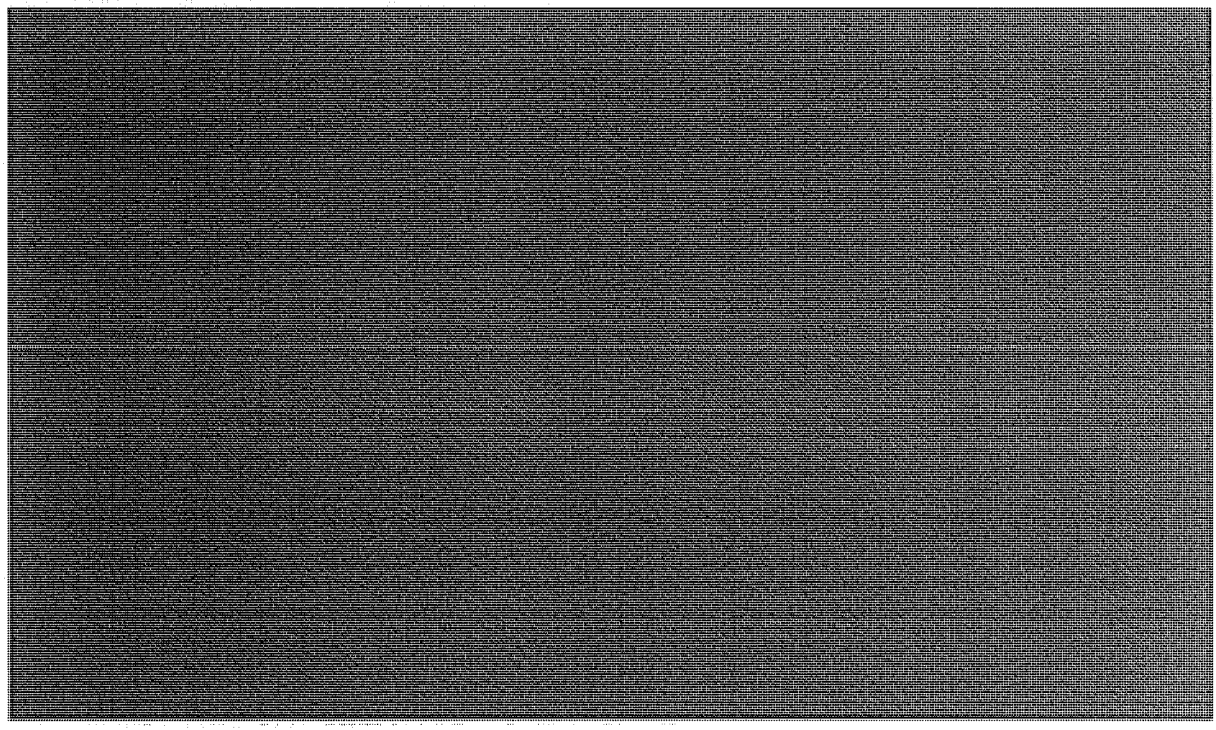
~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~



12

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

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



(U//~~FOUO~~) Senior CIA Officials Believe That the President's Surveillance Program Filled an Intelligence Gap

~~(TS//STLW//SI//OC/NF)~~ Former Directors Hayden and Goss, former Acting Director McLaughlin, and other senior CIA officials we interviewed told us that the PSP addressed a gap in intelligence collection. Following the terrorist attacks on 11 September 2001, there was concern that additional acts of terrorism would be perpetrated by terrorist cells already inside the US. [redacted] However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC and CIA officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat.

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

[redacted]

~~(TS//STLW//SI/OC/NF)~~ Other senior CIA officials told us that the PSP provided CIA access to information that was previously unavailable. [redacted]

14

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

(U//~~FOUO~~) The CIA Did Not Assess the Effectiveness of the President's Surveillance Program

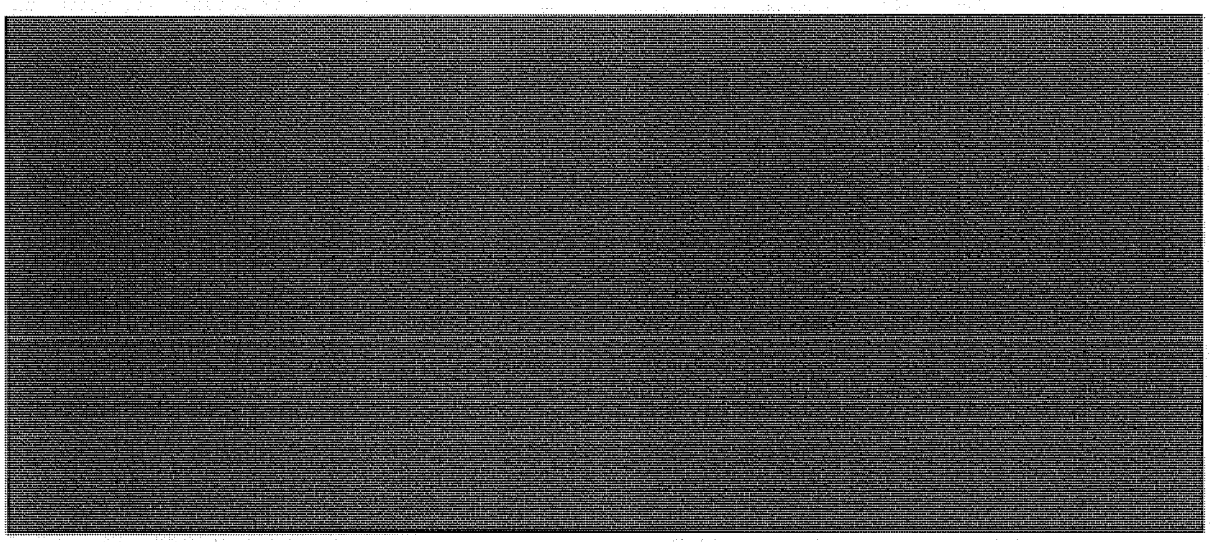
~~(TS//STLW//SI//OC/NF)~~ The CIA did not implement procedures to assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials, including DCIA Hayden, told us that PSP reporting 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 Senate Select Committee on Intelligence (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.

[redacted]

15

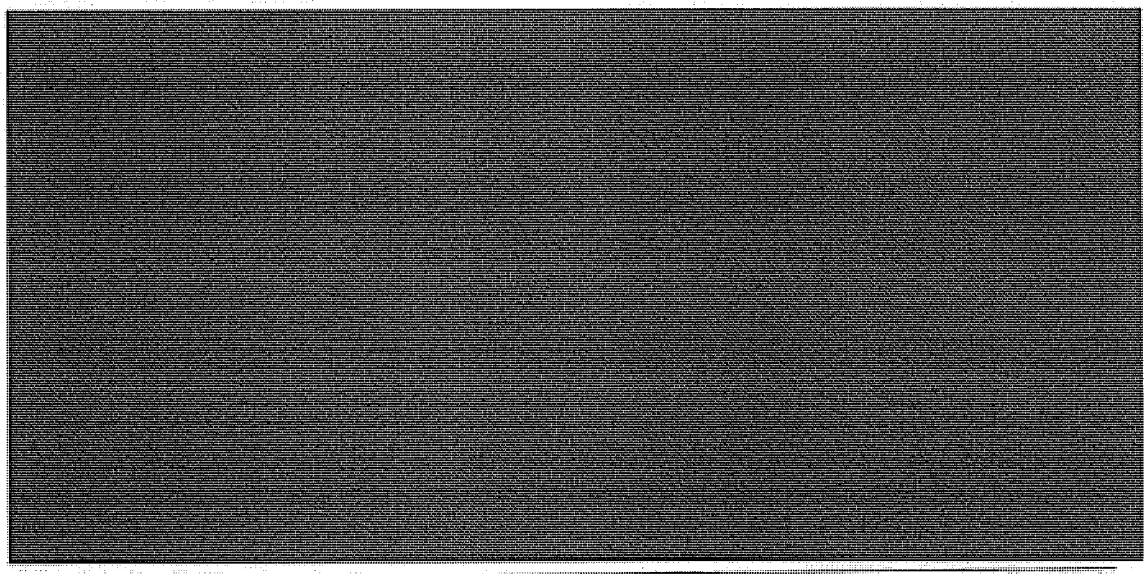
~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

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



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

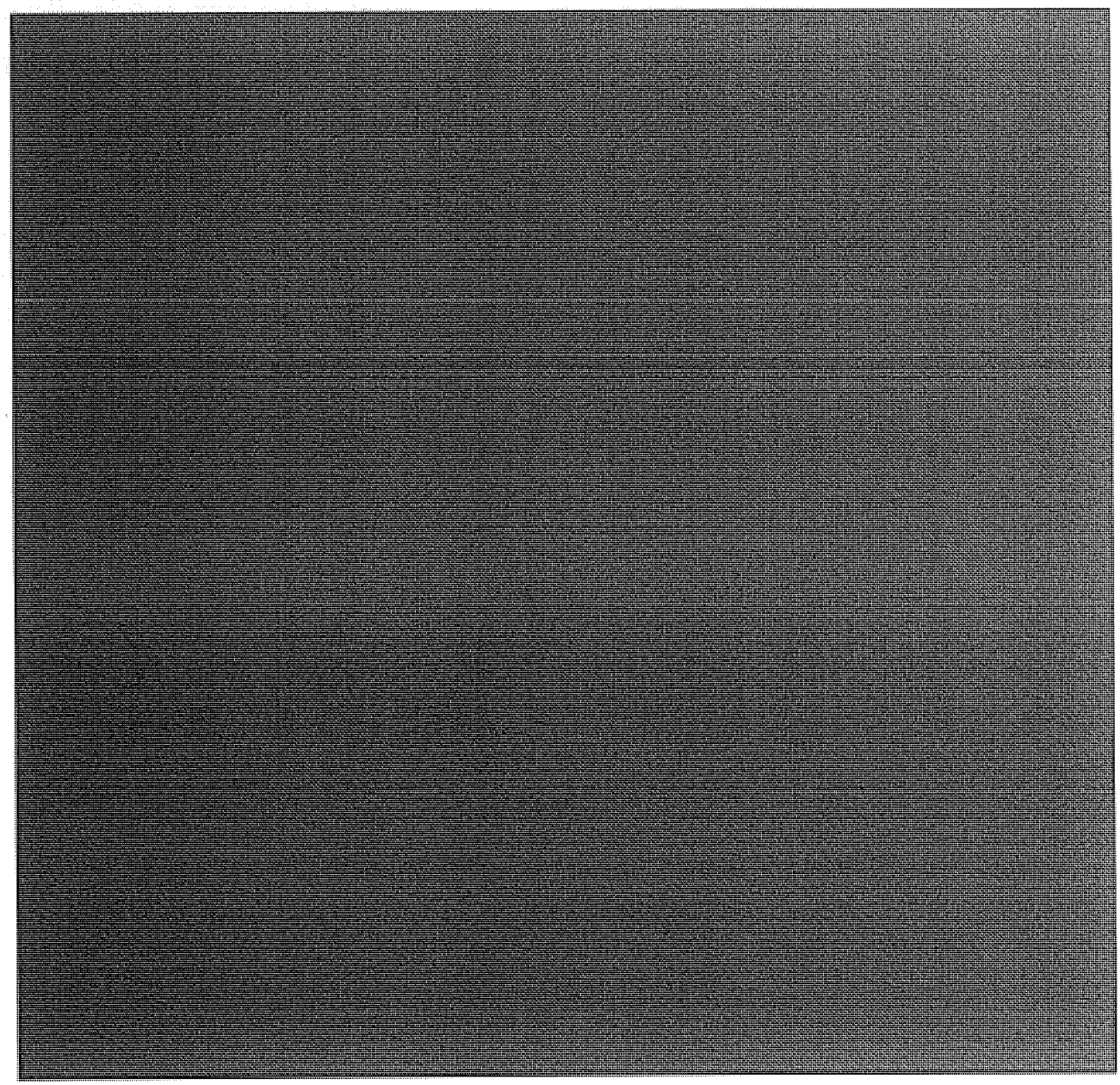
~~(S//NF)~~ Despite the fact that CIA officials we interviewed did not provide much specific information on PSP-derived counterterrorism successes, some key counterterrorism operations supported by the PSP were cited in briefings presented by CIA officials. In March 2004, the CIA provided a series of three briefings at the White House to senior Administration officials and Congressional leaders. These briefings included operational details concerning the PSP as well as examples of program successes. In May 2006, the Deputy Director, [redacted] briefed SSCI members and staff on the usefulness to [redacted] of the PSP.



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

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

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



~~(S//NF)~~ Several Factors Hindered CIA Utilization of the President's Surveillance Program

~~(S//NF)~~ 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

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

CIA personnel who were read into the PSP were senior CIA managers. [redacted]

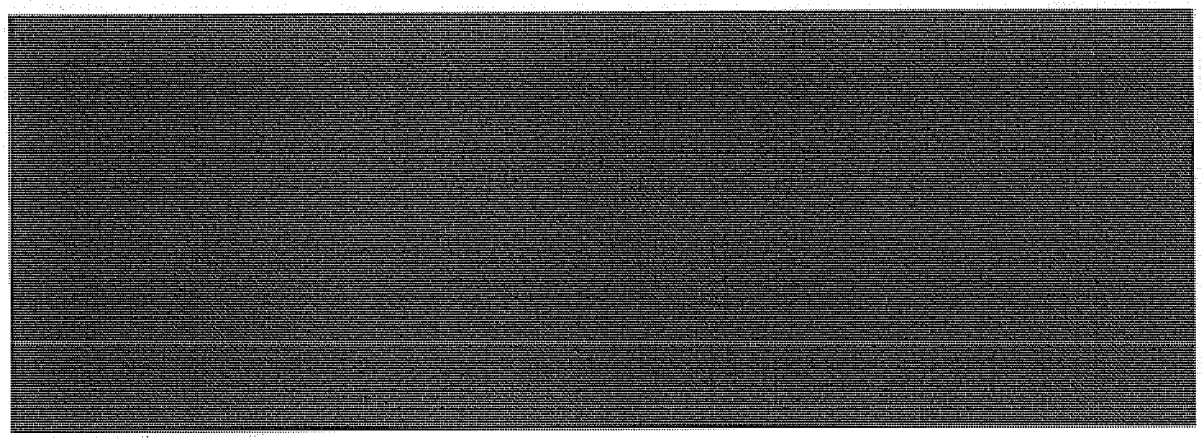
~~(S//NF)~~ [redacted] officials also told us that working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that 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 also told us 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. [redacted]

~~(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]

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

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



(U) CIA Had Limited Access to Legal Reviews of the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ There is no indication that personnel from the CIA Office of General Counsel or other CIA components were involved in preparing the legal memorandums supporting the PSP that were produced by the Department of Justice, Office of Legal Counsel (OLC). At the time of the initial authorization of the PSP (4 October 2001), Robert M. McNamara, Jr. was the CIA General Counsel. There is no record that McNamara was ever read into PSP, and he retired from the CIA on 15 November 2001. Acting General Counsel John Rizzo was read into the program on 21 December 2001, but, at that time, he was not provided access to the OLC legal opinions. Rizzo told us that by working through Addington, with whom Rizzo was acquainted, he eventually was allowed to read the OLC legal memorandums at Addington's office in July 2004.

~~(TS//STLW//SI//OC/NF)~~ Scott W. Muller became the CIA General Counsel on 24 October 2002. Although NSA records do not indicate that Muller was read into PSP, during our interview with Muller, he acknowledged having been read into the program and having read the OLC legal memorandums supporting the program. After Jack L. Goldsmith became the Assistant Attorney General for the Office of Legal Counsel in October 2003, the OLC undertook a reassessment of the legal rationale for the PSP. Muller recounted discussions with Deputy Attorney General James B. Comey around March 2004 concerning the legal basis for certain aspects of the program. Muller told us that he shared Comey's concern

Several of the senior CIA managers we interviewed said that, although they were concerned that the PSP operate within legal authorities, they believed that it was important to continue CIA

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

participation in the program because CIA analysts and targeters had told them that the program was a useful counterterrorism tool.

~~(S//NF)~~ CIA Officials Sought to Delay Exposure of the President's Surveillance Program by the *New York Times*

~~(S//NF)~~ In October 2004, James Risen, a reporter for *The New York Times*, contacted the CIA Office of Public Affairs seeking an interview with DCI Goss concerning an article the newspaper was planning on the PSP. Senior officials from the CIA, NSA, Office of the Vice President, and the Office of the Secretary of Defense met to discuss a response. On 20 October 2004, DDCI McLaughlin and DCI Chief of Staff Moseman met with the Washington, DC editor of *The New York Times*, Philip Taubman, and Risen. According to a memorandum for the record prepared by Moseman, McLaughlin did not provide any details regarding the PSP or comment on the legal basis for the program, but he stressed that publication of the article would expose, and potentially compromise, effective counterterrorism tools.

~~(S//NF)~~ [redacted] Ultimately, based on assurances from Hayden that he would advise them of inquiries from other news organizations concerning the PSP, Taubman and Risen agreed to hold the article and publish it only when it became apparent that other news organizations were preparing their own stories on the PSP. On 16 December 2005, *The New York Times* published its first article on the PSP: "Bush Lets U.S. Spy on Callers Without Courts." On 17 December 2005, President Bush publicly confirmed in a radio address the existence of the disclosed portion of the PSP.

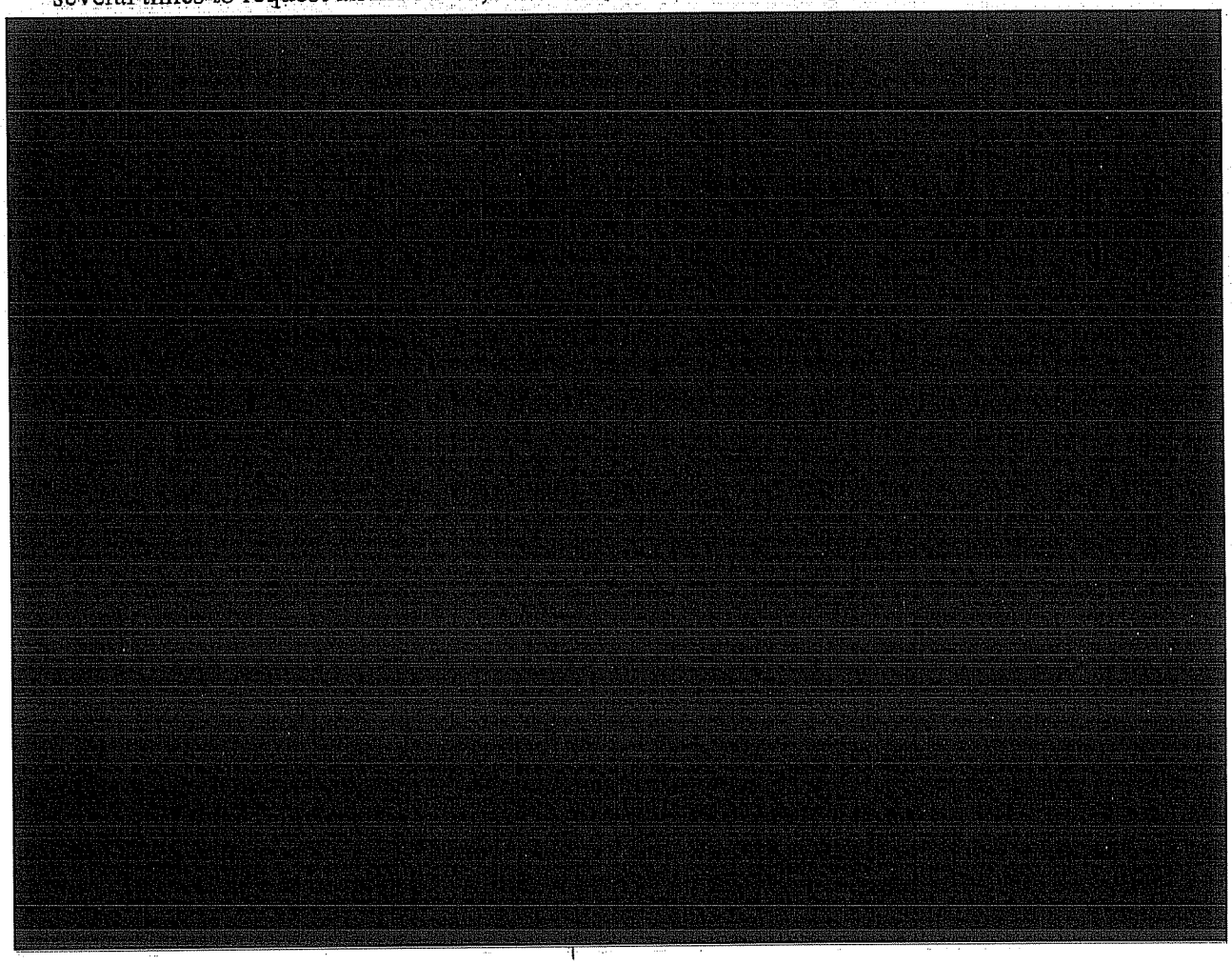
This page intentionally left blank.

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

Exhibit A

(U) Methodology

(U//~~FOUO~~) During our review, we conducted 50 interviews of current and former CIA personnel who had been involved with the President's Surveillance Program (PSP). Among the senior CIA officials we interviewed were former Director of the National Security Agency (NSA) and former Director of the CIA (DCIA) Michael V. Hayden, former Director of Central Intelligence (DCI) and former DCIA Porter J. Goss, and former Acting DCI John E. McLaughlin. We contacted former DCI George J. Tenet for an interview. Tenet suggested that we first interview his former Chief of Staff, John H. Moseman, and then contact him if we still had a need to interview him. Following our interview with Moseman, we contacted Tenet's office several times to request an interview, but he did not return our telephone calls.



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

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

[redacted]

(U//~~FOUO~~) Management comments were received from Michael V. Hayden; Scott W. Muller; John H. Moseman; the Director, [redacted] and the Chief [redacted] Their comments were considered in preparation of the final report.

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

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

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

Exhibit B

(U) Threat Assessment Memorandum Concluding Paragraph

[Excerpt from the *Global War Against Terrorism* memorandum dated 10 January 2005.]

~~(TS//STLW//SI//OC/NF)~~ Based on the information available to me from all sources, including the information in this document, it is my estimate that those involved in global terrorism possess both the capability and the intention to undertake further terrorists attacks within the United States, that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the United States Government. Accordingly, I recommend that, in accordance with the Constitution, you authorize the Secretary of Defense, for the purpose of detection and prevention of terrorist acts within the United States, to employ within the United States 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, if such electronic surveillance is 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, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe such communication originated or terminated outside the United States and a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group, provided that such group is al Qa'ida, is a group affiliated with al Qa'ida, or is another group that you determine for this purpose is in armed conflict with the United States and poses a threat of hostile action within the United States;

(b) acquire, with respect to a telephony communication, 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, (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; or

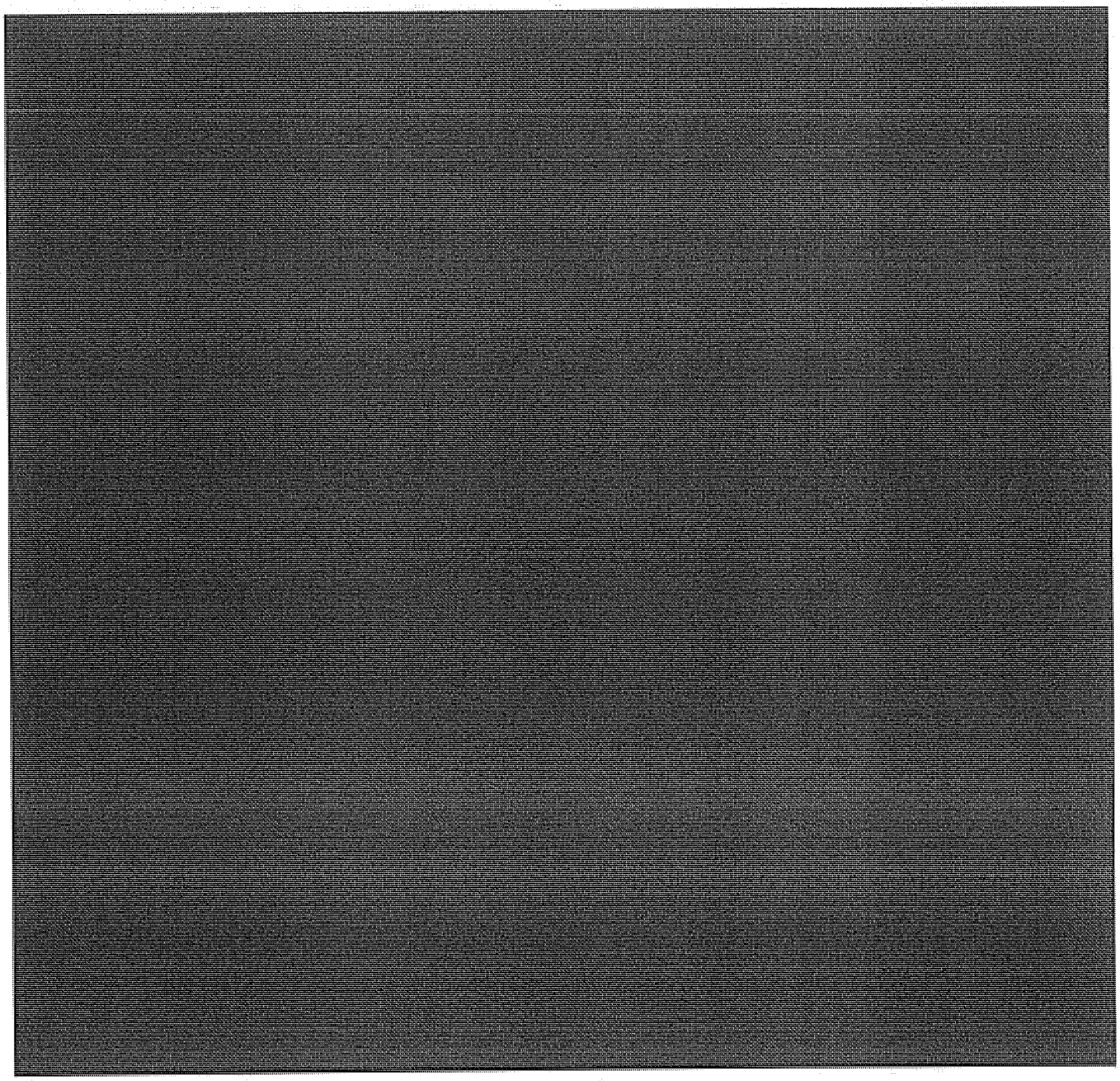
(c) collect, with respect to a non-telephony communication, header/ router/ addressing-type information, but not the contents of the communication, when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group, provided that such group is al Qa'ida, is a group affiliated with al Qa'ida, or is another group that you determine for this purpose is in armed conflict with the United States and poses a threat of hostile action within the United States.

This page intentionally left blank.

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

Exhibit C

(U) Example of a Link Diagram From August 2002



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

This page intentionally left blank.

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

Exhibit D

(U) Review Team

(U//~~FOUO~~) This report was prepared by the Operations Division, Audit Staff, Office of Inspector General.

[redacted] Division Chief
[redacted] Project Manager
[redacted] Auditor
[redacted] Auditor
[redacted] Auditor

~~This Exhibit is UNCLASSIFIED//FOUO~~

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

This page intentionally left blank.

~~TOP SECRET//STLW//COMINT//ORCON/NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

[redacted]

INSPECTOR GENERAL REPORT

(U) Review of the President's Surveillance Program

ST-09-0002
29 June 2009

~~Derived From: STLW Classification Guide~~
~~Dated: 22 January 2009~~
~~Declassify On: MR~~

~~TOP SECRET//STLW//COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//COMINT//ORCON//NOFORN~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts inspections, audits, and investigations. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations; to provide intelligence oversight; to protect against fraud, waste, and mismanagement of resources; and to ensure that NSA/CSS activities are conducted in compliance with the Constitution, laws, executive orders, regulations, and directives. The OIG also serves as ombudsman, assisting all NSA/CSS employees and affiliates, civilian and military.

(U) INSPECTIONS

(U) The inspection function conducts management and program evaluations in the form of organizational and functional reviews, undertaken either as part of the OIG's annual plan or by management request. The inspection team's findings are designed to yield accurate and up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with laws and regulations; the recommendations for corrections or improvements are subject to followup. The inspection office also partners with the Inspectors General of the Service Cryptologic Elements to conduct joint inspections of the consolidated cryptologic facilities.

(U) AUDITS

(U) The internal audit function is designed to provide an independent assessment of programs and organizations. Performance audits evaluate the economy and efficiency of an entity or program, as well as whether program objectives are being met and operations are in compliance with regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) THE OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations and Special Inquiries may be undertaken as a result or irregularities that surface during an inspection or audit; or at the initiative of the Inspector General.

~~TOP SECRET//STLW//COMINT//ORCON//NOFORN~~

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

29 June 2009
IG-11051-09

TO: DISTRIBUTION

SUBJECT: (U) Review of President's Surveillance Program (ST-09-0002) — INFORMATION MEMORANDUM

1. (U//~~FOUO~~) This report summarizes our review of the President's Surveillance Program, as mandated by the Foreign Intelligence Surveillance Act Amendments Act of 2008.

2. (U//~~FOUO~~) For additional information, please contact my office on 301-688-6666. We appreciate the courtesy and cooperation extended to our staff throughout the review.

George Ellard

GEORGE ELLARD
Inspector General

DISTRIBUTION:

SID
OGC

(U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(TS//SI//NF)~~ For over a decade before the terrorist attacks on 11 September 2001, NSA used its SIGINT authorities to provide information in response to Intelligence Community requirements on terrorism targets. In late September 2001, when the Vice President asked the Director of Central Intelligence what more NSA could do with additional authority, NSA's Director identified impediments to enhancing SIGINT collection under existing authorities. He said that in most instances NSA could not collect communications on a wire in the United States without a court order. As a result, NSA's ability to quickly collect and report on a large volume of communications from foreign countries to the United States was impeded by the time-consuming court order approval process. Attempting to obtain court orders for [redacted] foreign telephone numbers and Internet addresses was impractical for collecting terrorist communications with speed and agility.

~~(TS//STLW//SI//OC/NF)~~ Counsel to the Vice President drafted the 4 October 2001 Authorization that established the President's Surveillance Program (PSP), under which NSA could routinely collect on a wire, for counterterrorism purposes, foreign communications originating or terminating in the United States. Under the PSP, NSA did not target communications with both ends in the United States, although some of these communications were incidentally collected.

~~(TS//STLW//SI//OC/NF)~~ The PSP gave NSA a capability to exploit a key vulnerability in terrorist communications.

[redacted]

According to senior NSA leaders, the value of the program was that this SIGINT coverage provided confidence that someone was looking at the seam between foreign and domestic intelligence domains to detect and prevent attacks in the United States.

~~(TS//STLW//SI//OC/NF)~~ NSA's Director said that SIGINT reporting on an extremist linked (b)(1), (b)(3) "probably saved more lives" than any other PSP information and is, therefore, the most important SIGINT success of the PSP. NSA analysis (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ Knowledge of the Program was strictly limited at the express direction of the White House, and NSA's Director needed White House approval to inform members of Congress about Program activity. Between 25 October 2001 and 17 January 2007, General Michael V. Hayden and Lieutenant General Keith B. Alexander conducted PSP briefings for members of Congress and staff.

~~(TS//STLW//SI//OC/NF)~~ NSA activity conducted under the PSP was authorized by Foreign Intelligence Surveillance Court (FISC) orders by 17 January 2007, when NSA stopped operating under PSP authority. The NSA Office of the Inspector General (OIG) detected no intentional misuse of Program authority.

(U) HIGHLIGHTS

- **(U) PSP establishment, implementation, and product**

~~(TS//STLW//SI//OC/NF)~~ NSA began PSP operations on 6 October 2001. Although the Director of NSA was "comfortable" exercising the new authority and believed that it was lawful, he realized that it would be controversial. Under the PSP, NSA issued over (b)(3) reports. This included (b)(3) reports based on collected metadata, which was defined in the Authorization as "header/router/addressing-type information including telecommunications dialing-type data, but not the contents of the communication." It also included (b)(3) reports based on domestic content collection, which includes words spoken in a telephone conversation or sent in an e-mail (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ NSA's PSP products, all of which were sent to CIA and FBI, were intended for intelligence purposes to develop investigative leads and were not to be used for judicial purposes.

[redacted] and NSA had no mechanism to track and assess the effectiveness of PSP reporting.

- **(U) Access to legal reviews and program information**

~~(C//NF)~~ NSA's General Counsel and Inspector General were not permitted to read the 2001 DoJ, Office of Legal Counsel opinion on the PSP, but they were given access to draft 2004 Office of Legal Counsel opinions. Knowledge of the PSP was strictly controlled by the White House. Between 4 October 2001 and 17 January 2007, [redacted] people were cleared for access to PSP information.

- [redacted]

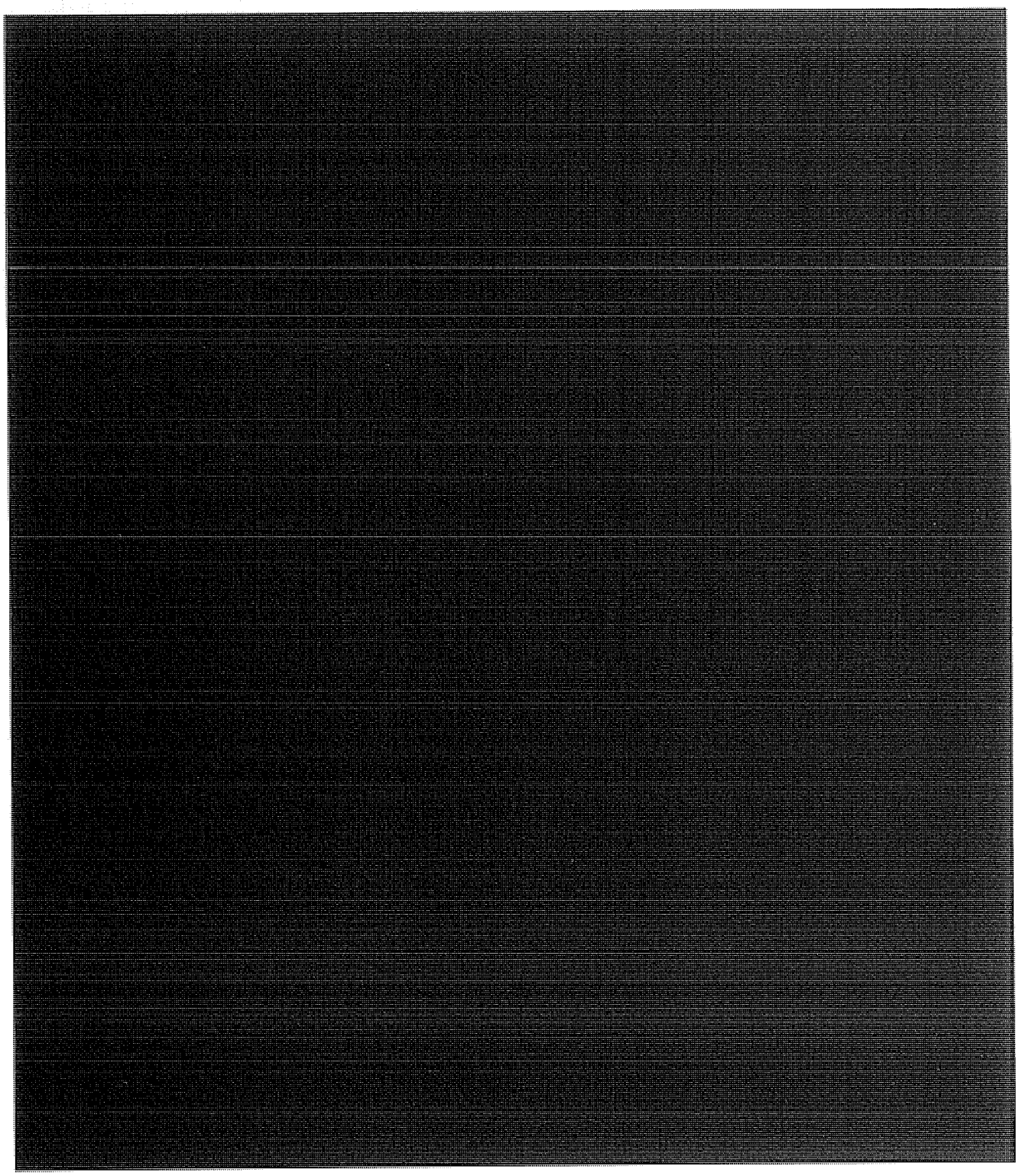
- **(U) NSA-FISC interaction and transition to court orders**

~~(TS//STLW//SI//OC/NF)~~ NSA's PSP-related interaction with the FISC was primarily briefings to presiding judges, beginning in January 2002. Interaction increased when NSA and the DoJ began to transition PSP activities to FISC orders. After parts of the program had been publicly revealed in December 2005, all members of the FISC were briefed. NSA's PSP authorized collection of bulk Internet metadata, telephony business records, and the content of communications transitioned to FISC orders on 14 July 2004, 24 May 2006, and 10 January 2007, respectively.

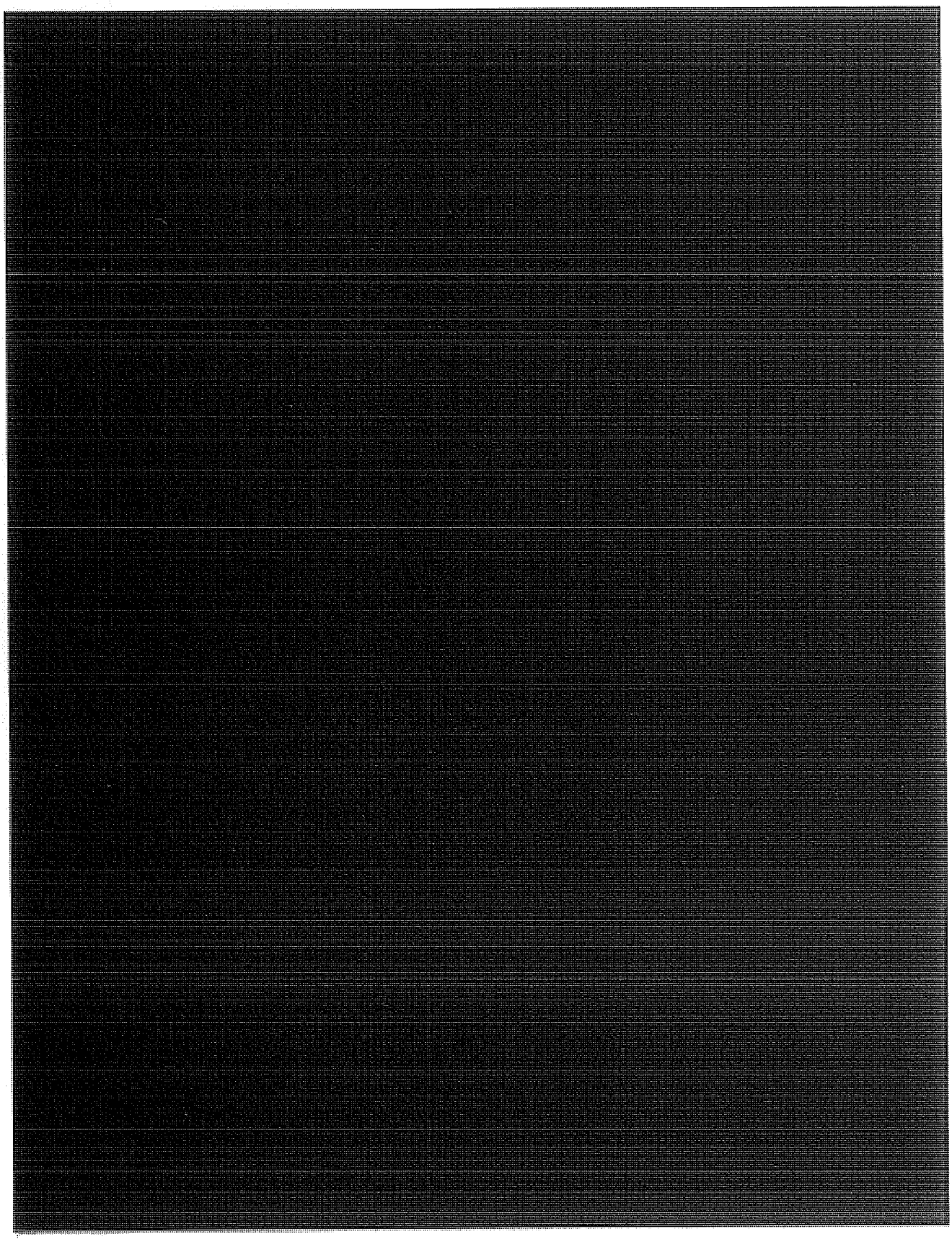
- **(U) Program oversight at NSA**

~~(C//NF)~~ NSA's Office of General Counsel and Signals Intelligence Directorate provided oversight of NSA PSP activities from October 2001 to January 2007. NSA OIG oversight began after the IG was cleared for PSP information in August 2002.

This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

[redacted]

~~(S//NF)~~ For years before the 11 September 2001 terrorist attacks in the United States, NSA had been using its authorities to focus the United States Signals Intelligence (SIGINT) System on foreign intelligence targets, including terrorism, in response to Intelligence Community requirements. After the attacks, NSA adjusted SIGINT collection, in accordance with its authorities, to counter the terrorist threat within the United States. In late September, the Vice President asked the Director of Central Intelligence (DCI) if NSA could do more to prevent another attack. NSA's Director responded by describing impediments to SIGINT collection of terrorist-related communications to the Vice President. Counsel to the Vice President used the information about impediments to draft the Presidential Authorization that established the PSP.

(U) SIGINT Efforts against Terrorists before 11 September 2001

~~(C//NF)~~ For over a decade before terrorists attacked the United States in September 2001, NSA was applying SIGINT assets against terrorist targets in response to Intelligence Community requirements. The Signals Intelligence Directorate (SID) Counterterrorism (CT) Product Line led these efforts in accordance with SIGINT authorities, which defined what NSA could and could not do against SIGINT targets.

(U) Authorized SIGINT activity in September 2001

(U) 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. NSA and other Intelligence Community agencies were required by E.O. 12333 to conduct intelligence activities in accordance with U.S. law and other E.O. 12333 provisions.

(U) Both DoD regulation and NSA/Central Security Service (CSS) policy implemented NSA's authorities under E.O. 12333 and specified procedures governing activities that affect U. S. persons (DoD Regulation 5240.1-R, December

1982, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* and NSA/CSS Policy 1-23, 11 March 2004, *Procedures Governing NSA/CSS Activities that Affect U. S. Persons).*

~~(S//SI//NF)~~ The policy of the U.S. SIGINT System is to collect, retain, and disseminate only foreign communications, which, in September 2001, were defined in NSA's legal compliance procedures (described below) as communications having at least one communicant outside the United States or entirely among foreign powers or between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA could not collect communications from a wire in the United States without a court order unless they originated and terminated outside the United States.

~~(S//SI//NF)~~ In 2001, NSA's authority to collect foreign communications included the Director of NSA's authority to approve targeting communications with one communicant in the United States, if technical devices (such as [redacted]) could be employed to limit acquisition of communications to those in which the target is a non-U.S. person located outside the United States, [redacted] or [redacted]

~~(S//SI//NF)~~ NSA's Director 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 safeguards to protect U.S. persons' Constitutional rights

(U) The Fourth Amendment to the U.S. Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government.[1] United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and Minimization*

---

[1] ~~(C//NF)~~ USSID SP0018 defines a U.S. person as a citizen of the United States, an alien lawfully admitted for permanent residence in the United States, unincorporated groups or associations a substantial number of the members of which constitute either of the first two groups, or corporations incorporated in the United States, including U.S. flag non-governmental aircraft or vessels, but not including those entities openly acknowledged by a foreign government to be directed and controlled by them.

Procedures, 27 July 1993, prescribes policies and minimization procedures and assigns responsibilities to ensure that United States SIGINT System missions and activities are conducted in a manner that safeguards U.S. persons' Constitutional rights. (See Appendix G.)

~~(S//SI//NF)~~ During the course of normal operations, NSA personnel sometimes inadvertently encounter information to, from, or about U.S. persons. When that happens, they must apply standard minimization procedures approved by the Attorney General in accordance with E.O. 12333 and defined in *USSID SP0018*. These procedures implement the constitutional principle of reasonableness by giving different categories of individuals and entities different levels of protection. They ensure that U.S. person information is minimized during collection, processing, dissemination, and retention of SIGINT by, for example, strictly controlling collection with a high risk of encountering U.S. person information and focusing all reporting solely on the activities of foreign entities and persons and their agents.

(U) NSA Director Used Existing Authorities to Enhance SIGINT Collection after Terrorist Attacks

[redacted]

[redacted]

[redacted]

[redacted]

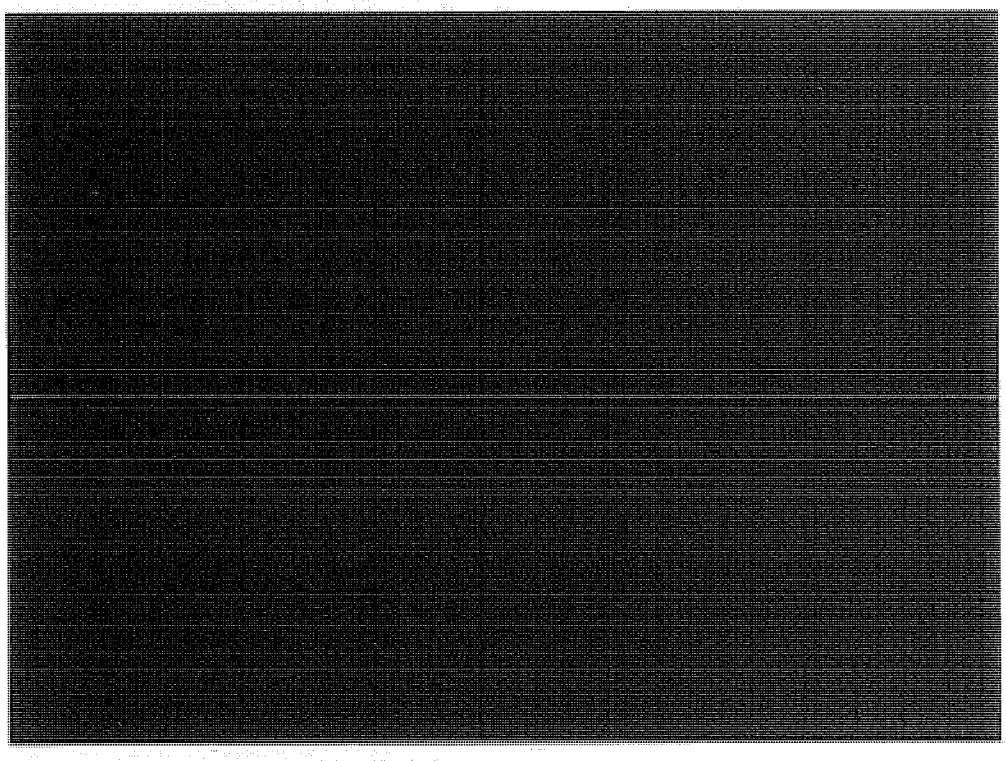
~~(S//NF)~~ In Oval Office Meeting, DCI Explained NSA Director's Decision to Expand Operations under Existing SIGINT Authorities

(U//~~FOUO~~) General Hayden recalled that in late September 2001, he told Mr. Tenet about NSA actions under E.O. 12333 to counter the terrorist threat. Mr. Tenet shared that information with the White House in an Oval Office meeting.

(U//~~FOUO~~) We did not interview Mr. Tenet or White House personnel during this review. We asked the White House to provide documentation of meetings at which General Hayden or NSA employees discussed the PSP or the Terrorist Surveillance Program with the President, Vice President, or White House personnel, but we did not receive a response before this report was published. Therefore, information about the sequence of events leading up to the establishment of the PSP comes from interviews of NSA personnel.

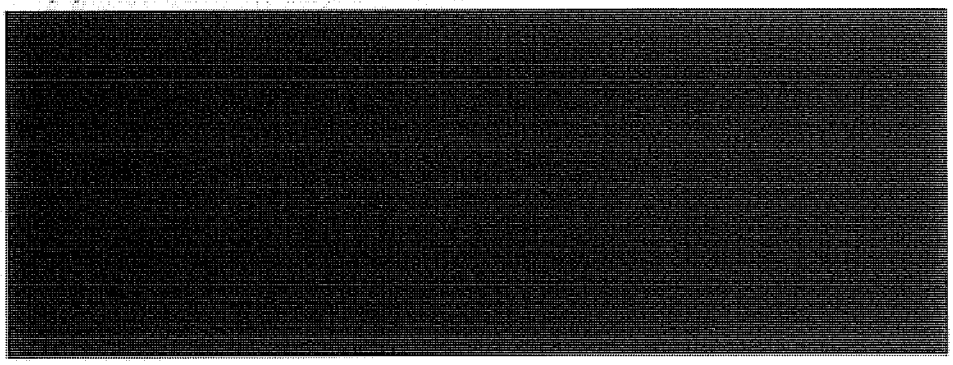
(U) Vice President Asked What Other Authorities NSA Needed

[redacted]



~~(S//NF)~~ NSA Options to Improve SIGINT Collection Could Not Fill Intelligence Gaps on Terrorist Targets

(U) FISA Amendments Considered



~~(S//NF)~~ General Hayden said that, in his professional judgment, NSA could not get the needed collection using the FISA. The process for obtaining court orders was slow, and it involved extensive coordination and separate legal and policy reviews by several agencies. Although an emergency authorization provision permitted 72 hours of surveillance without 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 the FISA and be acceptable to the FISC.

[redacted]

~~(S//SI//NF)~~ Under its authorities, NSA had no other options for the timely collection of communications of suspected terrorists when one end of those communications was in the United States and the communications could only be collected from a wire or cable in the United States.

(U//~~FOUO~~) NSA Director Described to the Vice President the Impediments to Improved SIGINT Collection against Terrorist Targets

[redacted]

[4] ~~(TS//SI//NF)~~ According to NSA OGC, DoJ has since agreed with NSA that simply processing communications metadata in this manner does not constitute electronic surveillance under the FISA.

(U//~~FOUO~~) After two additional meetings, the Vice President asked General Hayden to work with his Counsel, David Addington. Because early discussions about expanding NSA authority were not documented, we do not have records of attendees or specific topics discussed at General Hayden's meetings with White House representatives.

III. (U) THE PRESIDENTIAL AUTHORIZATIONS

[redacted]

~~(TS//STLW//SI//OC/NF)~~ Between 4 October 2001 and 8 December 2006, President George W. Bush signed 43 Authorizations, two modifications, and one document described as [redacted] The authorizations were based on the President's determination that after the 11 September 2001 terrorist attacks in the United States, an extraordinary emergency existed for national defense purposes. The Authorization documents contained the terms under which NSA executed special Presidential authority and were titled *Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States.* They were addressed to the Secretary of Defense.

(U) SIGINT Activity Permitted under the PSP

[redacted]

[redacted]

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

~~(TS//STLW//SI//OC/NF)~~ The authorizations changed over time, first eliminating the possibility that the Authority could be interpreted to permit collection of communications with both ends in the United States and adding an additional qualification that metadata could be collected for communications related to international terrorism or activities in preparation for international terrorism.[7] (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ Starting in March 2004, the authorizations underwent several adjustments related to DoJ's Office of Legal Counsel's review of the Authority. (b)(1), (b)(3) When these two clarifications were added to the 11 March 2004 and subsequent authorizations, an accompanying statement added that these clarifications had been previously understood and implemented by NSA and that they applied to past and future activities. Al-Qa'ida (also spelled al-Qaeda) was specified as a target for content collection, (b)(1), (b)(3) and NSA's authority to acquire (b)(1), (b)(3) Finally, as a result of a subsequent change, NSA's authority to collect (b)(1), (b)(3) but only fo(b)(1), (b)(3)with (b)(1), (b)(3) thus (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ The definition of "terrorist groups" within the authorities was also refined, and, for a limited

---

[6]~~(TS//SI//NF)~~ Metadata, as defined by the Authorization, is "header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication."
[7](U) See Appendix B for information about the types of collection permitted.

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

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

[redacted]

(U) NSA Discussions about the Lawfulness of the Authorization

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

Operations—concluded that the Program was legally defensible.

(U) Director of NSA

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

(U) General Hayden

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

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

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

(U) General Alexander

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

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

(U) NSA Office of General Counsel

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

(U) General Counsel

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

(U) Associate General Counsel for Operations

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

(U) Deputy General Counsel

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

(U) Discussions on Legality

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

[redacted]

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

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

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

---

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

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

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

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

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

This page intentionally left blank.

[redacted]

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

(U) NSA Begins PSP Operations

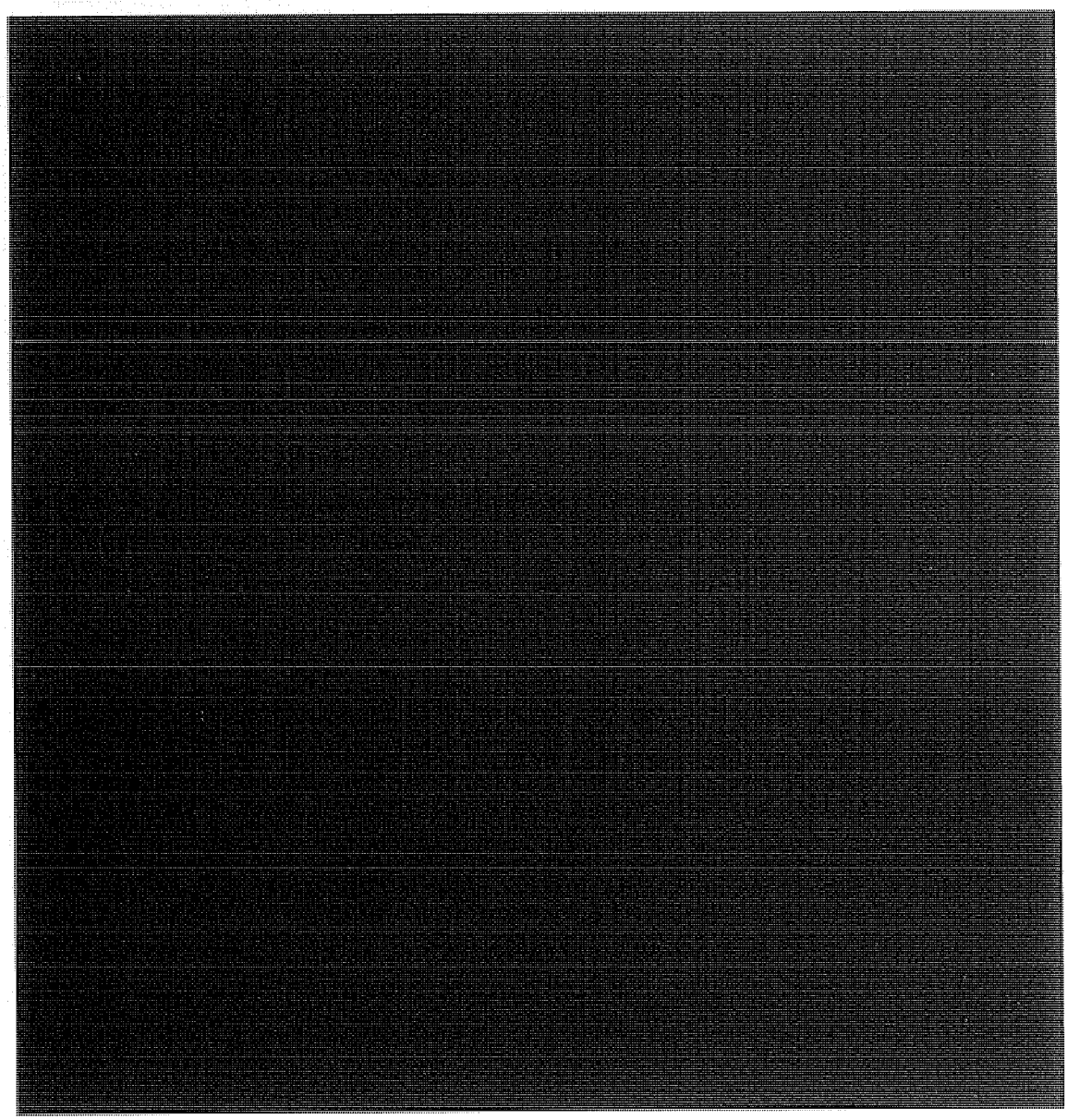
~~(S//NF)~~ On 4 October 2001, General Hayden received the initial Authorization and informed the SIGINT Director and other key personnel.

[redacted]

[redacted]

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

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



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

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

(U) FISA Authority Still not an Option in 2002

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

[redacted]

[redacted]

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

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

[redacted]

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

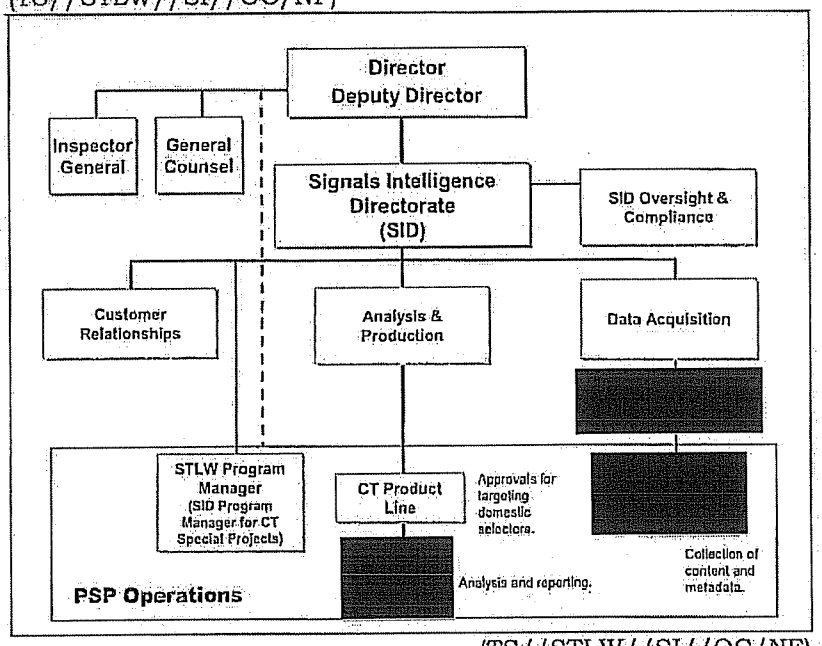
[redacted]

(U) NSA Structure for PSP Operations

[redacted]

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

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



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

(U) Chain of Command

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

[redacted]

[redacted]

[redacted]

(U) Coordination with FBI

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

[redacted]

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

[redacted]

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

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

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

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

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

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

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

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

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

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

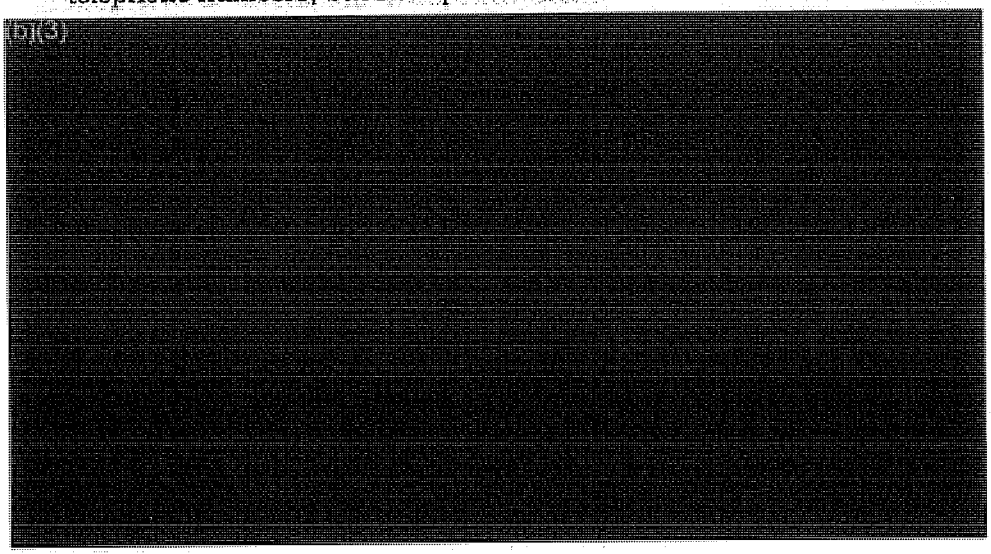
- ~~(TS//SI//NF)~~ Monitoring—Statistics on content tasking and reports were maintained and reviewed by SID, Oversight and Compliance by 2003. A CT Product Line employee stated: "... [N]owhere else did NSA have to report on selectors and how many selectors were rolled off [detasked] and why."

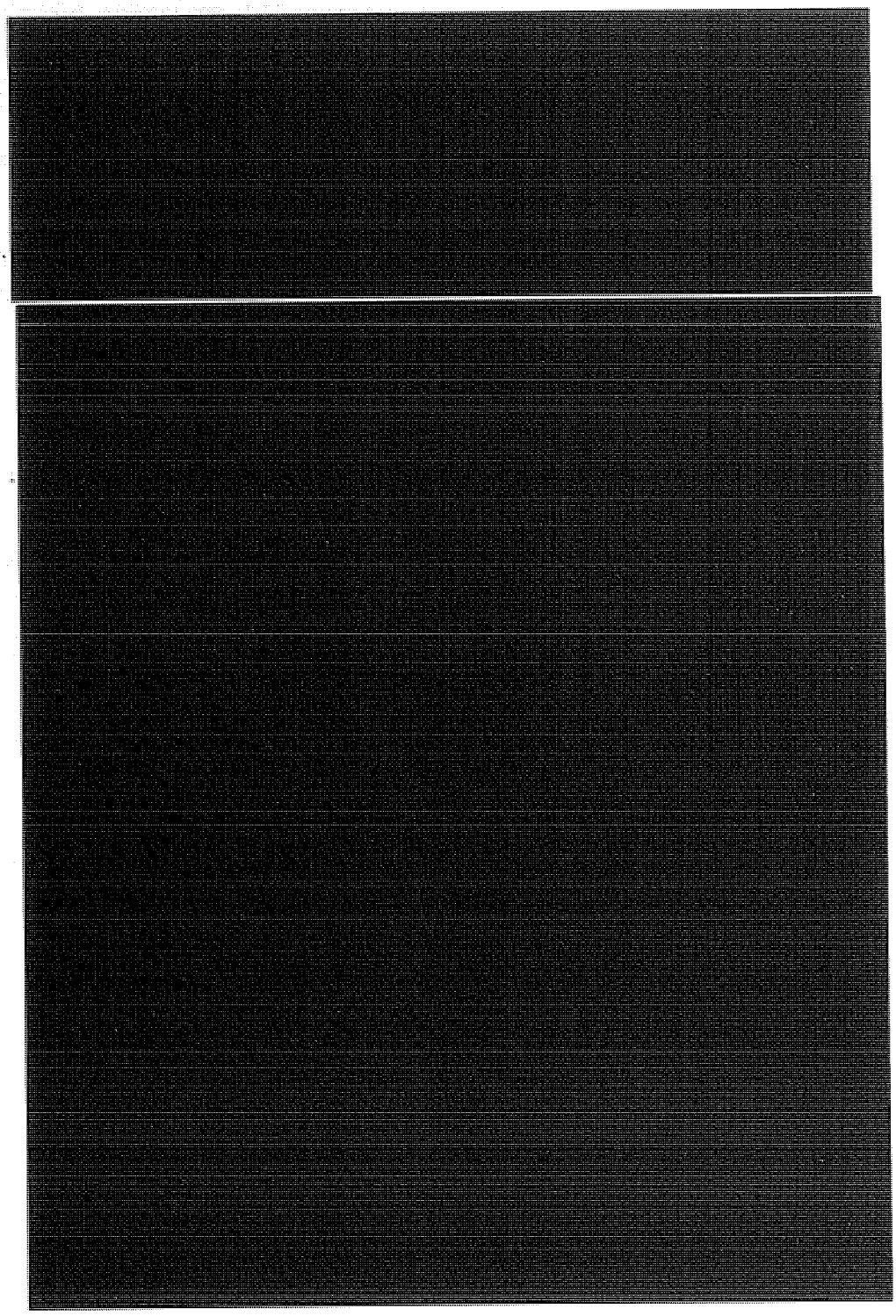
- (U//~~FOUO~~) OGC involvement—Personnel working under PSP authority noted that they had a continuous dialogue with the OGC on what was permissible under the Authorization. The Associate General Counsel for Operations confirmed that the OGC "was involved with the operations people day in and day out."

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

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

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





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

(b)(3)

[redacted]

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

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

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

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

---

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

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

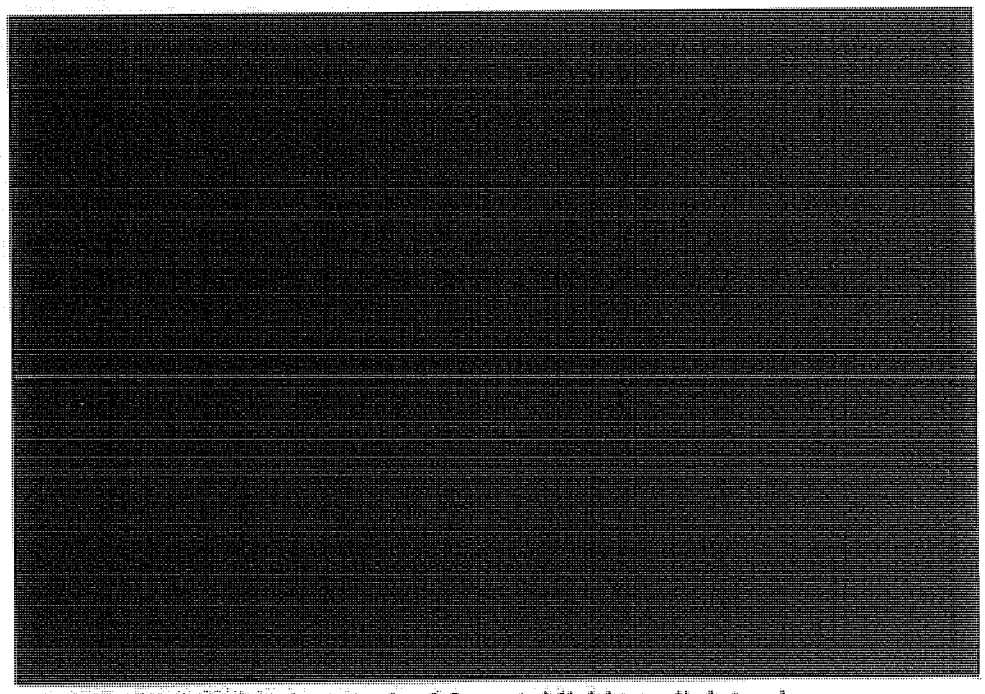
the purpose of detection and prevention of terrorist acts within the United States.

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

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

(U) Approvals for Metadata Analysis

[redacted]



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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

[redacted]

[redacted]

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

[redacted]

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

[redacted]

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

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

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

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

[redacted]

- Information associated with or obtained through FBI investigations.

(U) Process to Task Selectors

[redacted]

[redacted]

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

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

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

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

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

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

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

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

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

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

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

[redacted]

---

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

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

[redacted]

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

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

[redacted] b1, b3, b7E

~~(TS//STLW//SI//OC/NF)~~ NSA retained documentation of the analysis, supporting customer request or lead information, and a description of the link to terrorism for tippers based on PSP collection. Documentation of analysis was not retained unless a tipper was written. Counterterrorism personnel updated information in a computer tracking system to reflect the disposition of all metadata analysis requests. From October 2001 through January 2007, NSA issued [redacted] tippers to FBI and CIA: b1, b3, b7E

- [redacted] tippers were based on Internet metadata analysis.
- [redacted] tippers were based on telephony metadata analysis when telephone numbers had only direct contact (one degree of separation) with a known terrorist as defined by the Authorization. b1, b3, b7E

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

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

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

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

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

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

(U) Use of SIGINT Product

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

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

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

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

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

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

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

~~(TS//STLW//SI//OC/NF)~~ Current NSA Director General Alexander cited SIGINT reporting on [redacted] as the most important SIGINT success of the PSP. NSA analysis of PSP metadata and content collection placed [redacted], General Alexander said, "probably saved more lives" than any other PSP information produced by NSA because the information [redacted] b1, b3, b6, b7C, b7E

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

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

[redacted]

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

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

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

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

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

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

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

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

---

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

(U) Case Name	(U) PSP Contribution
(b)(1), (b)(3)	

b1, b3, b6, b7C, b7D, b7E

(U) Case Name	(U) PSP Contribution
(b)(1); (b)(3)	

b1,
b3,
b6,
b7C,
b7E

(U) Case Name	(U) PSP Contribution
(b)(1), (b)(3)	

b1, b3, b6, b7C, b7E

(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

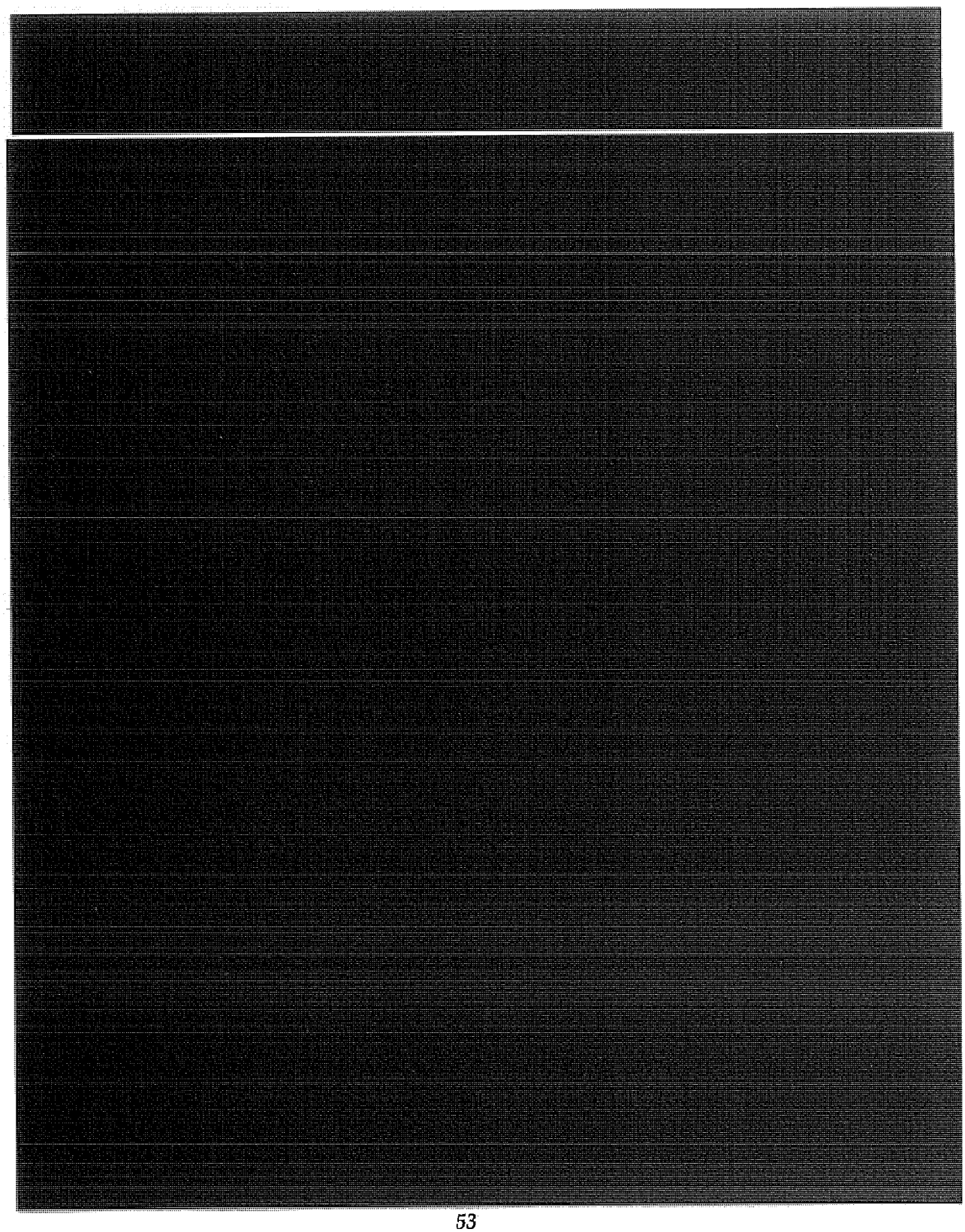
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

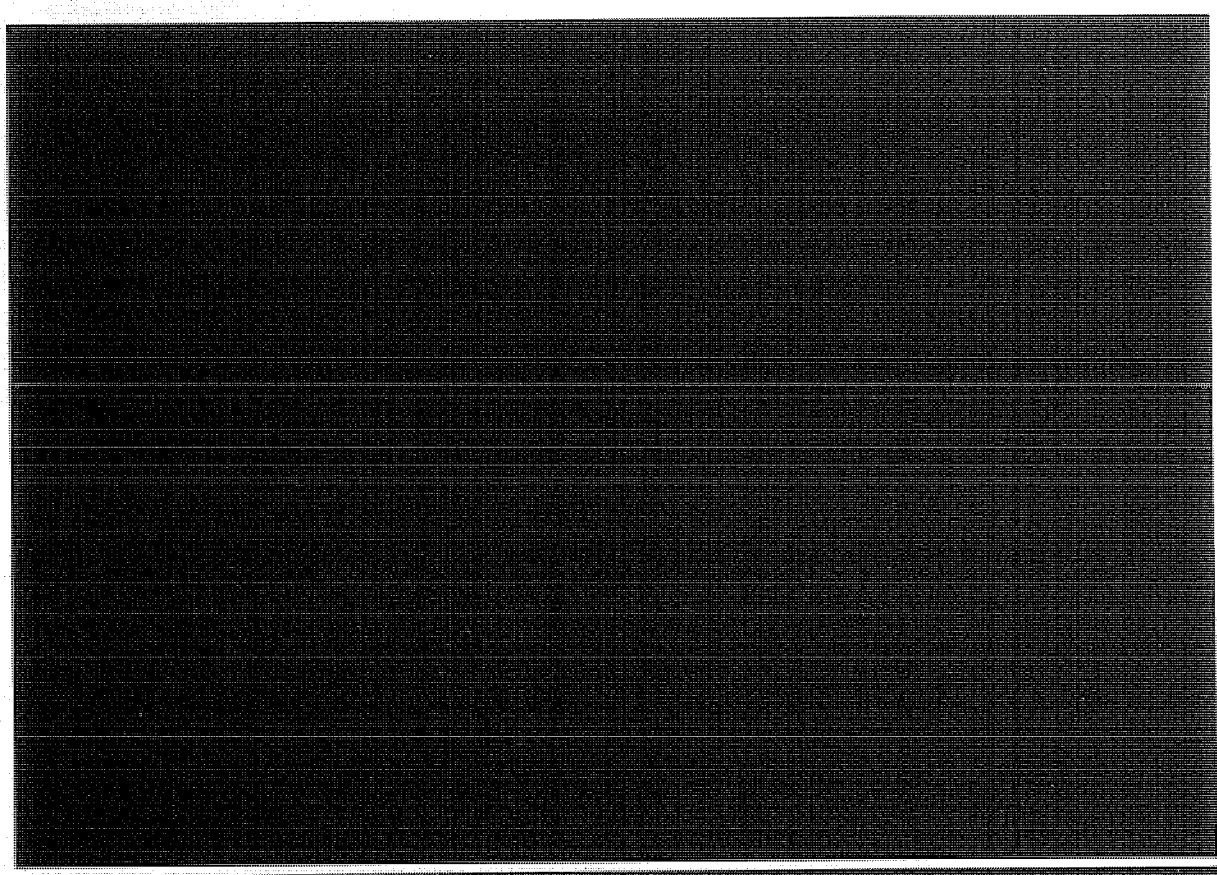
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

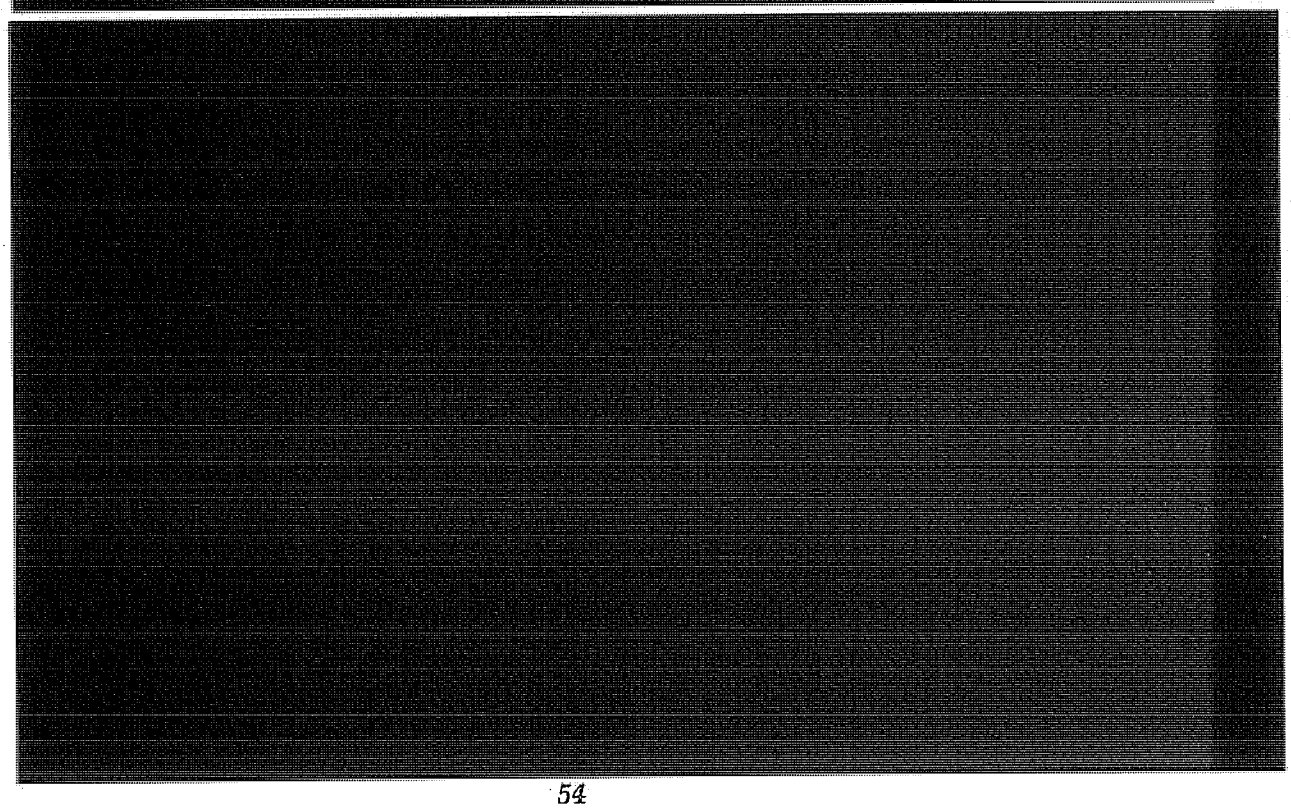
b1,
b3,
b6,
b7C,
b7E

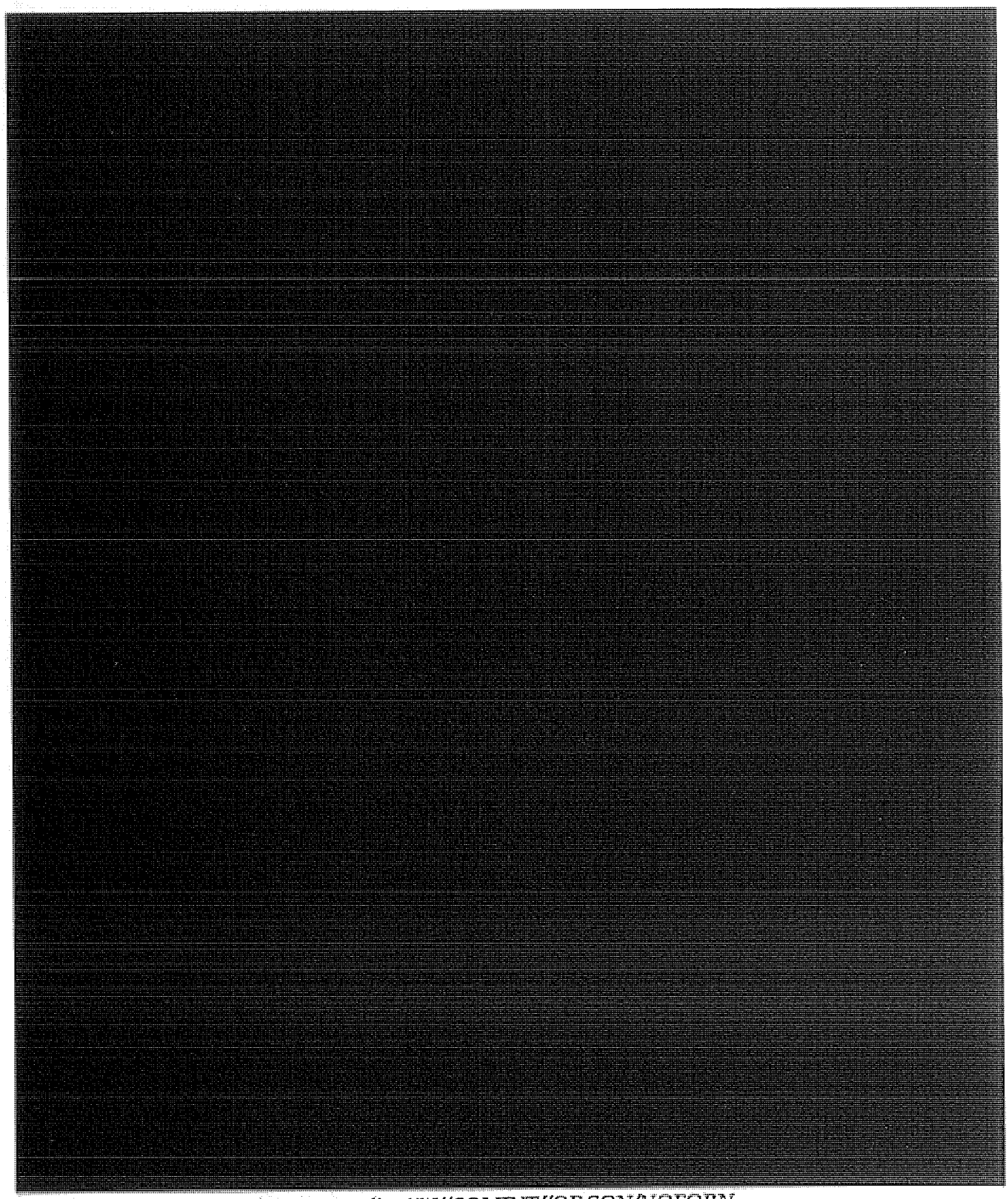
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

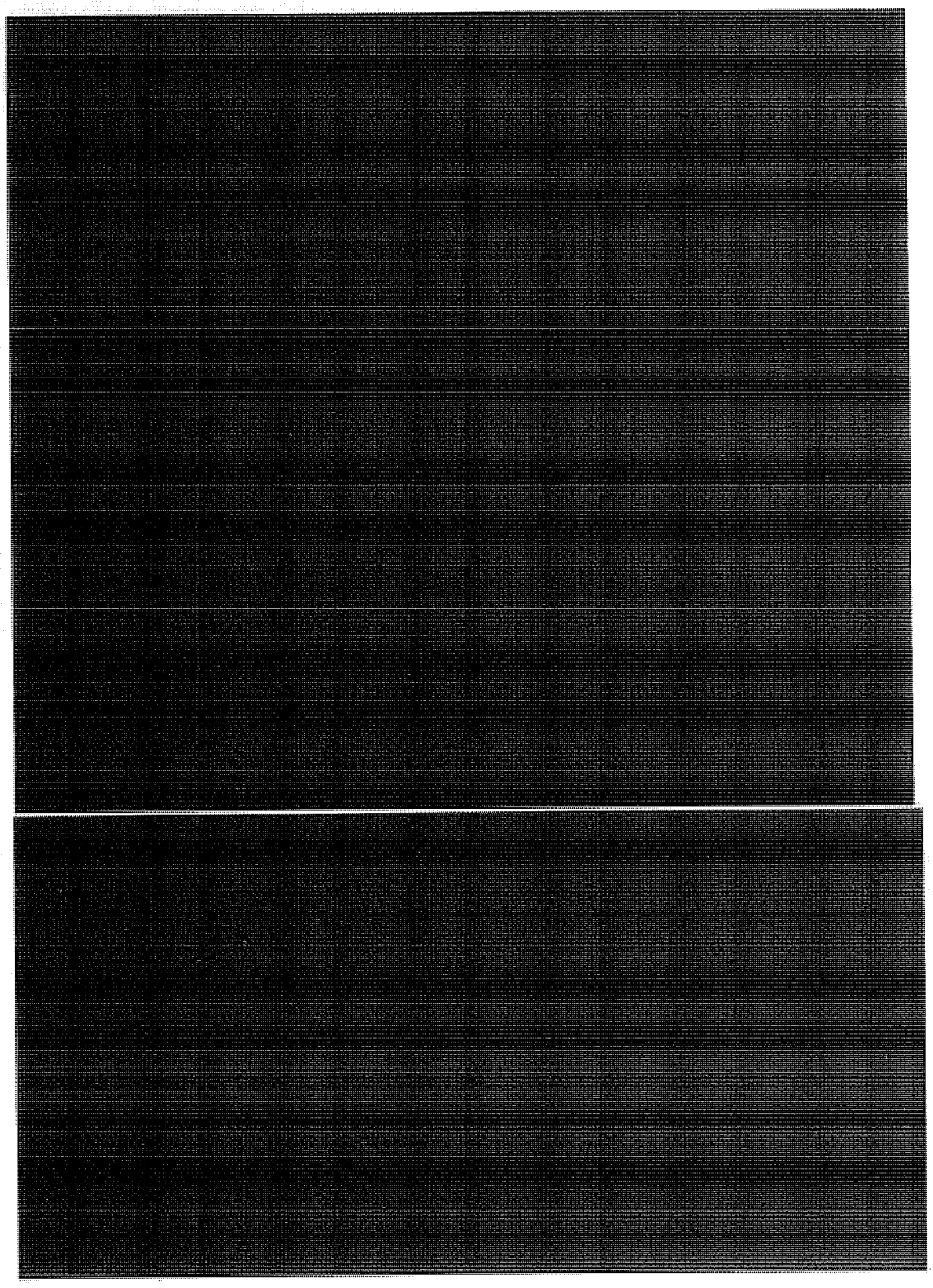
[redacted]

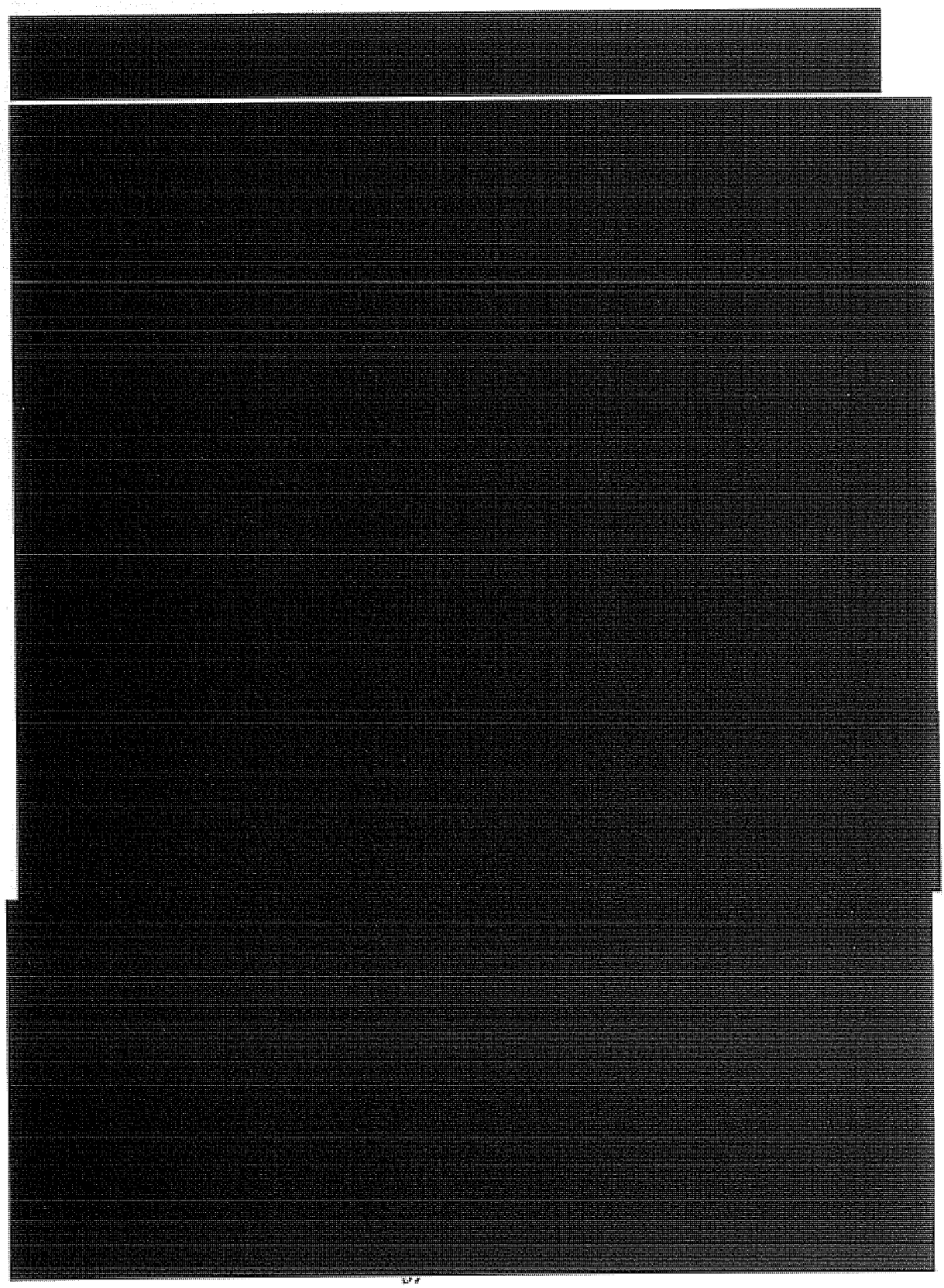




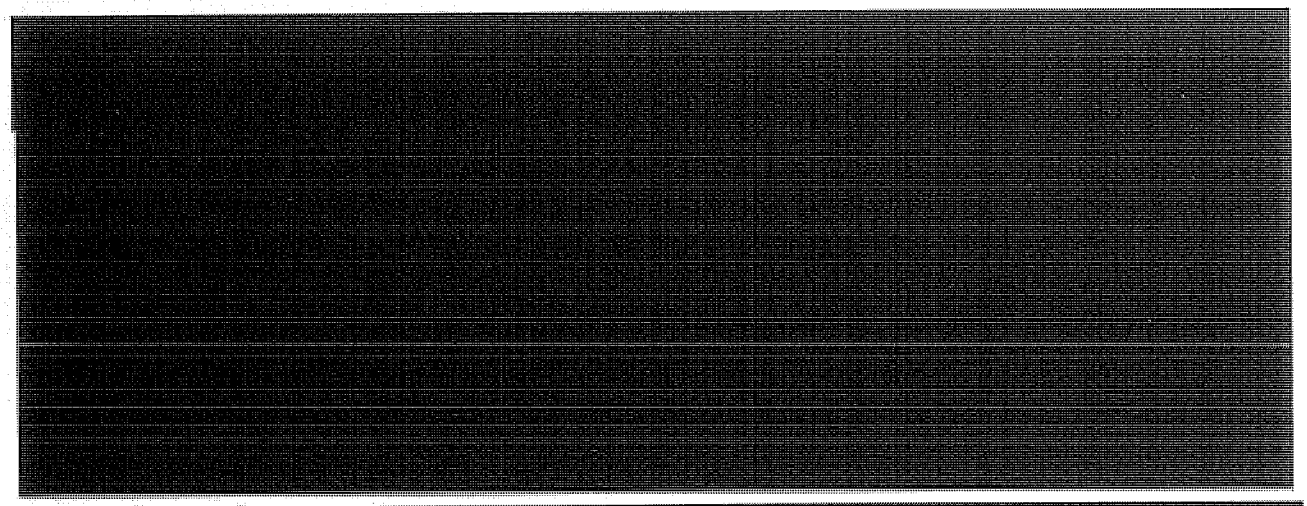


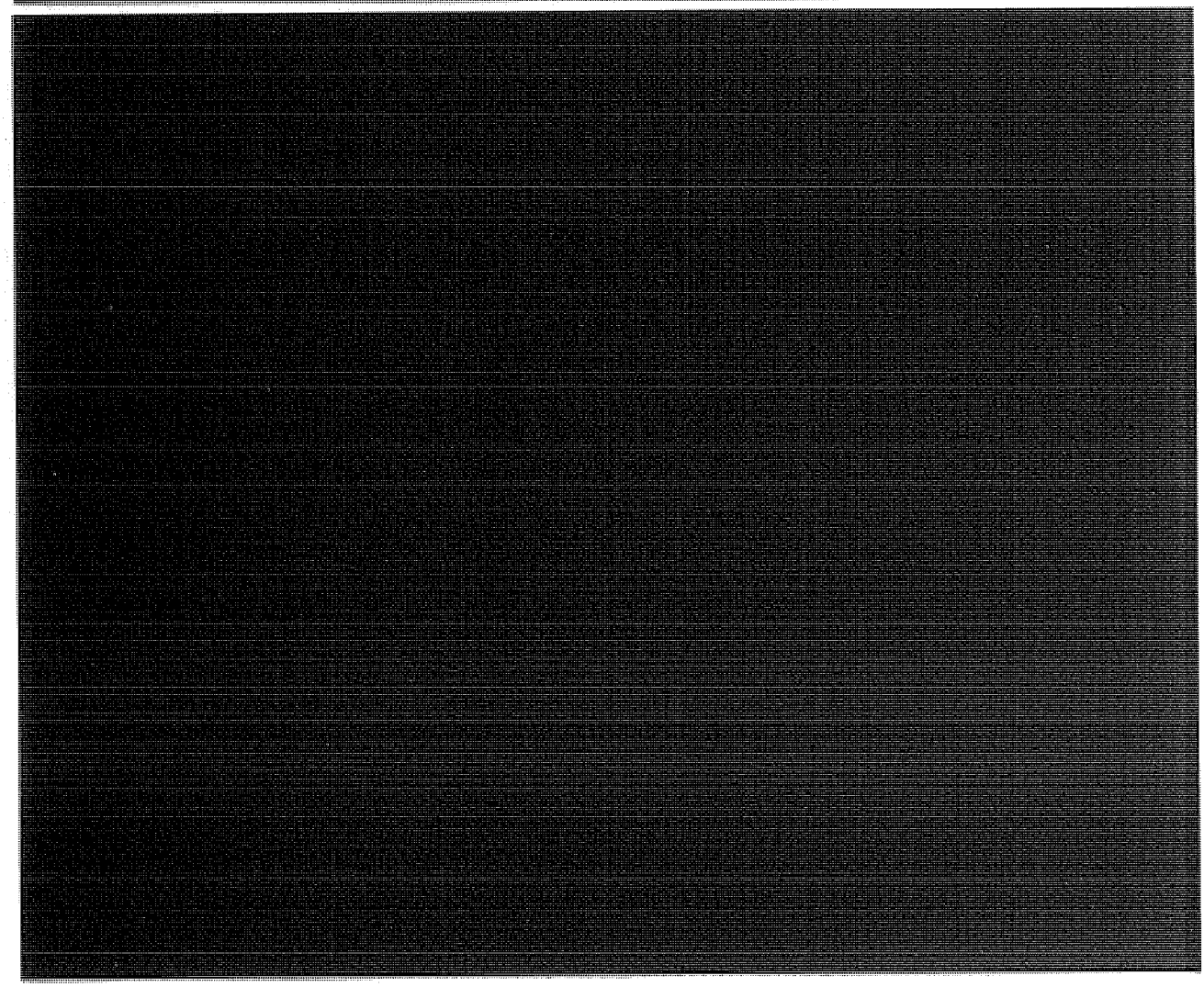


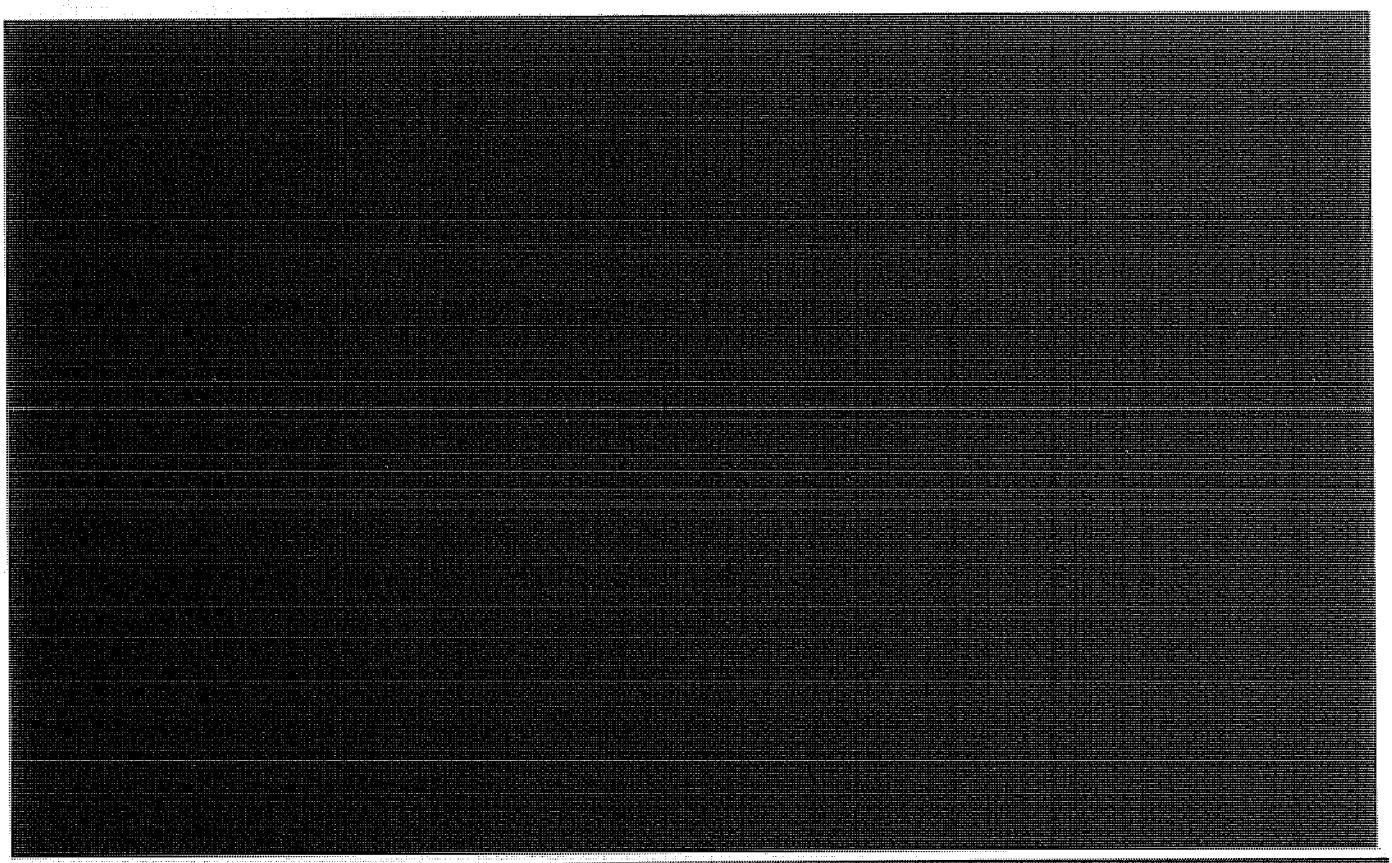


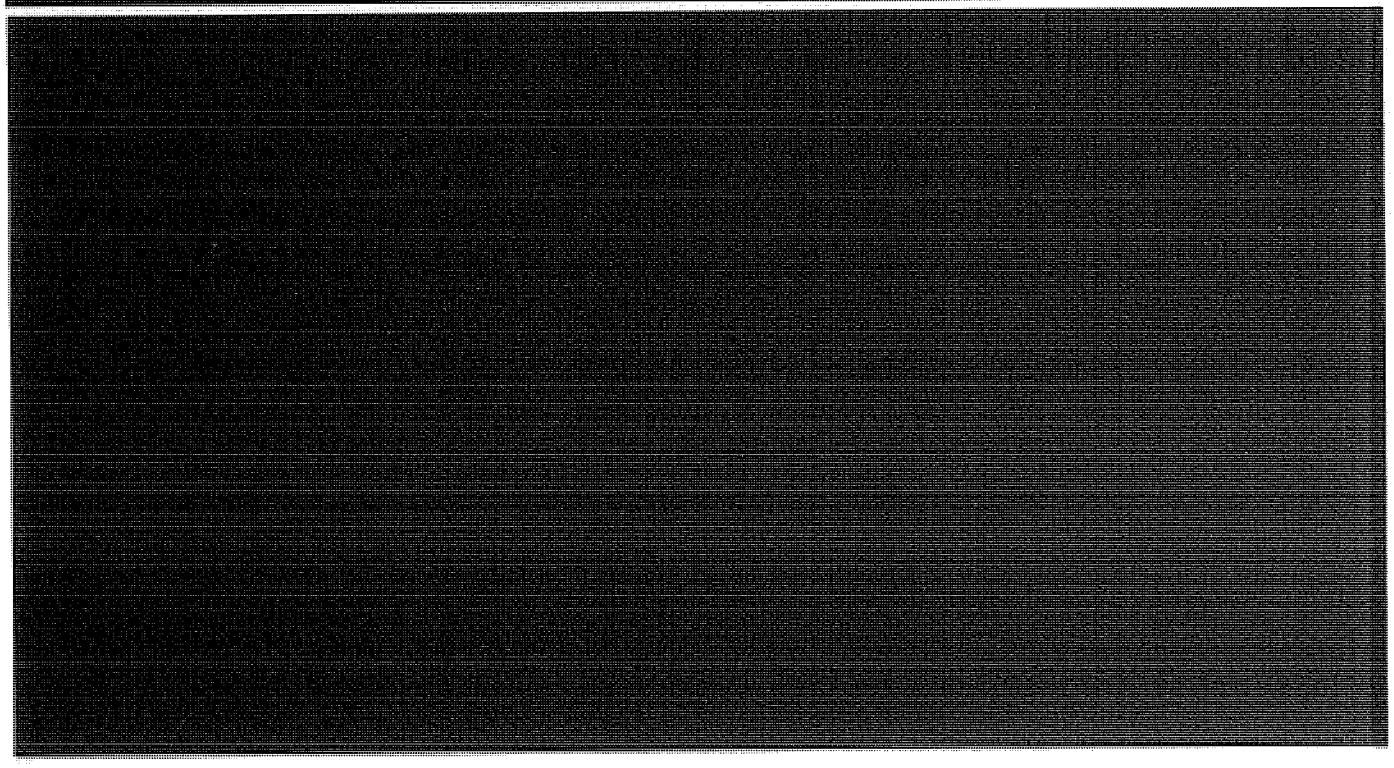


[redacted]

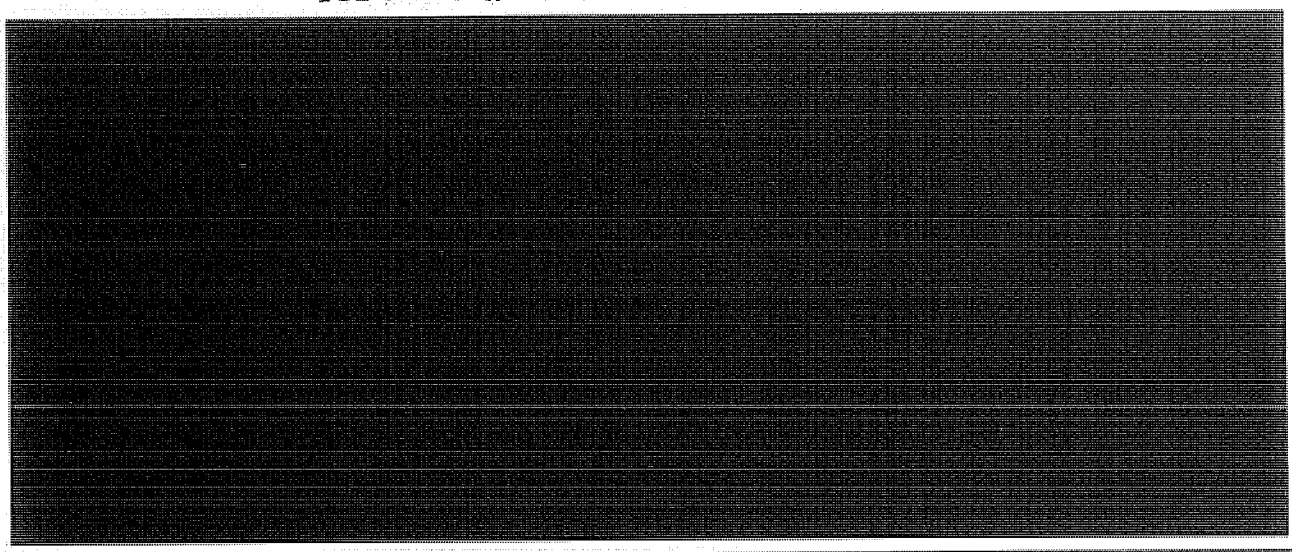




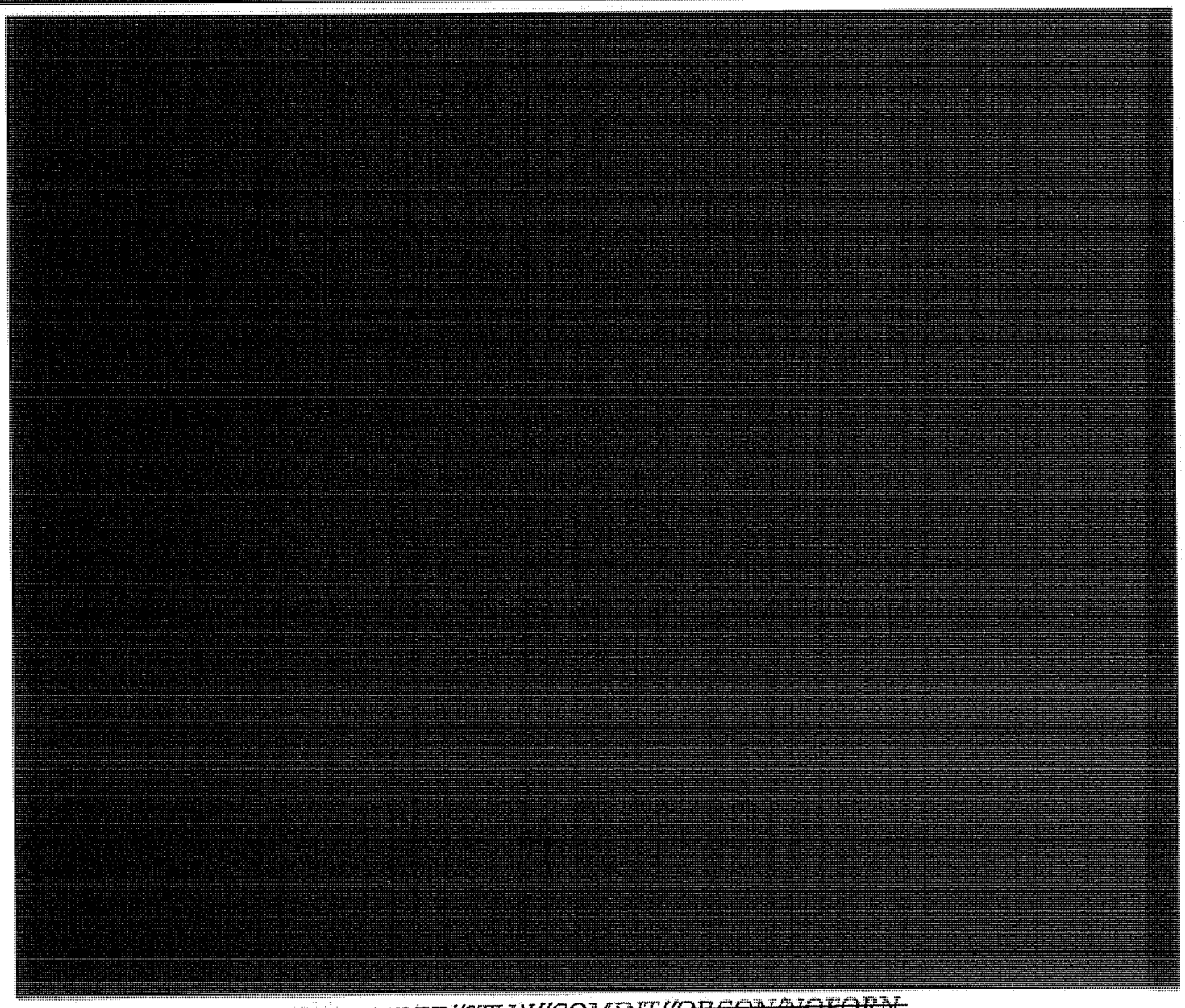


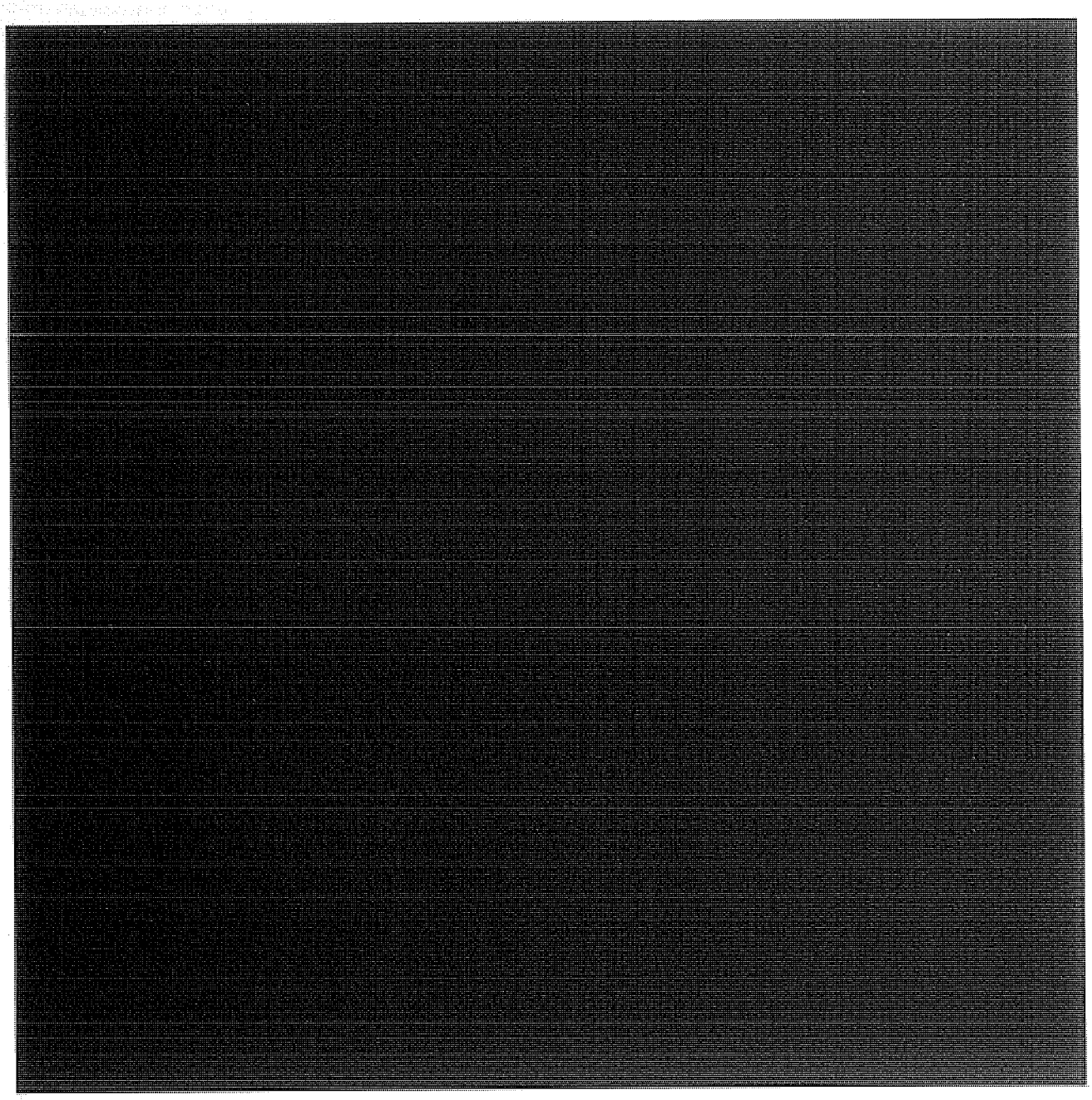


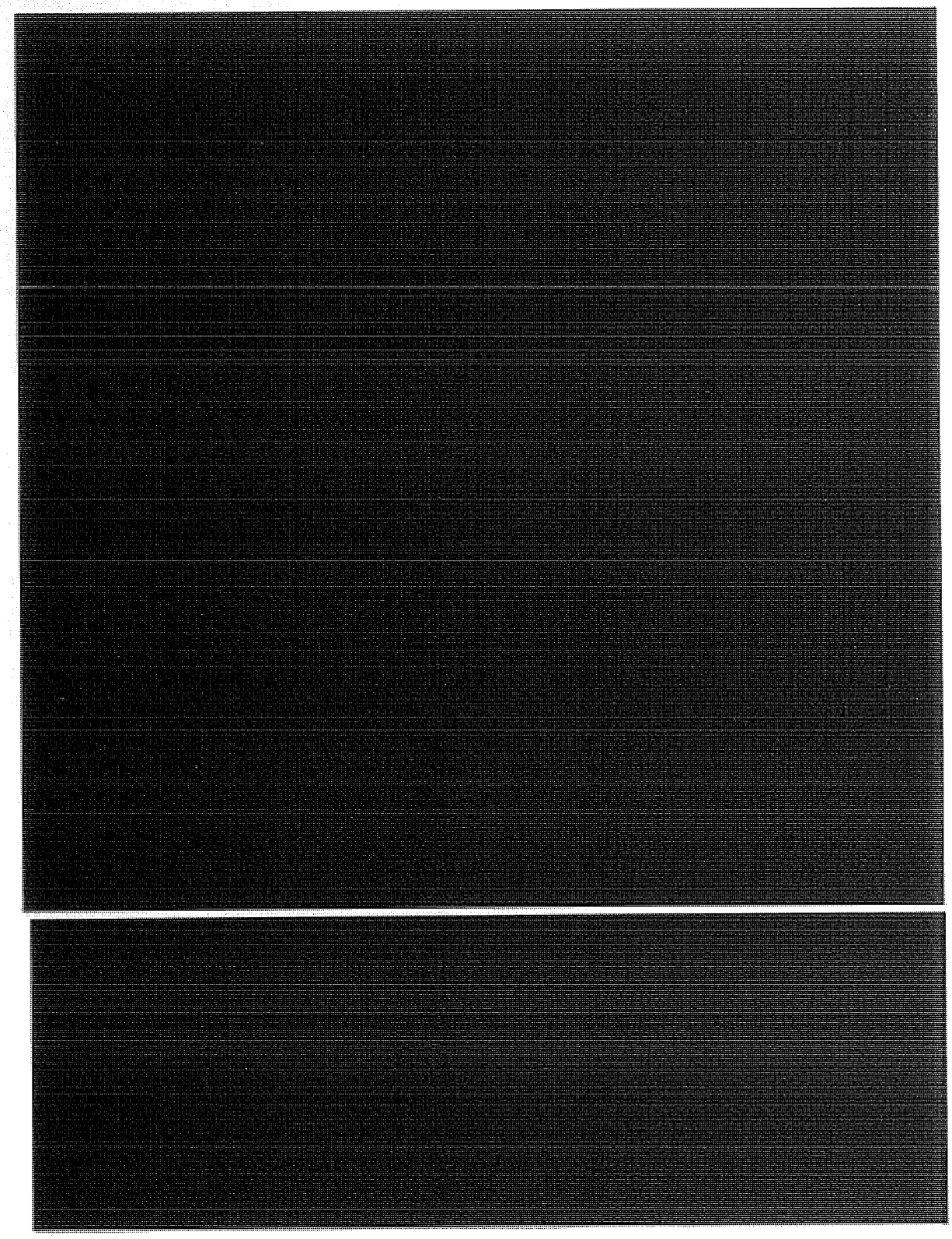
b1, b3, b7E

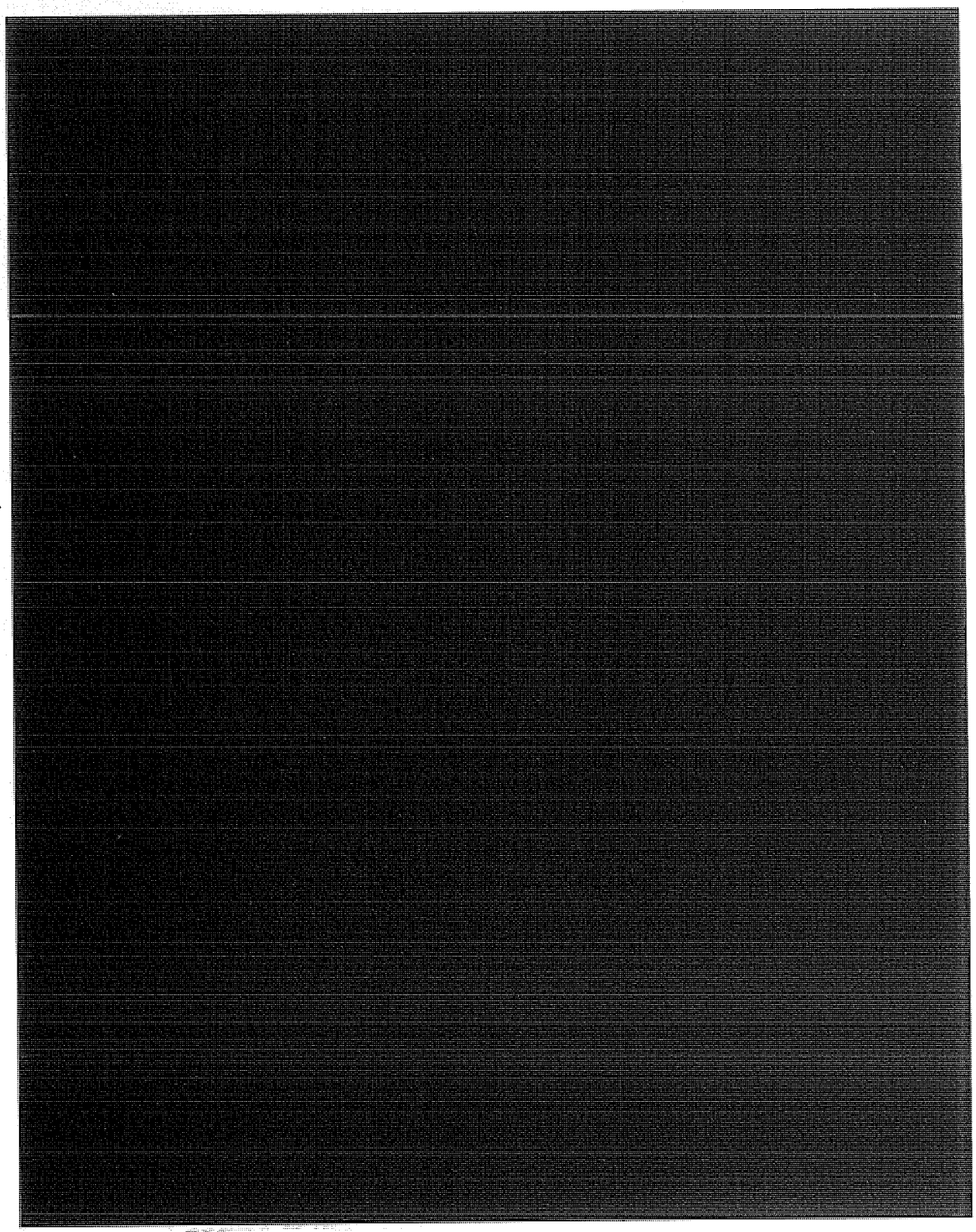


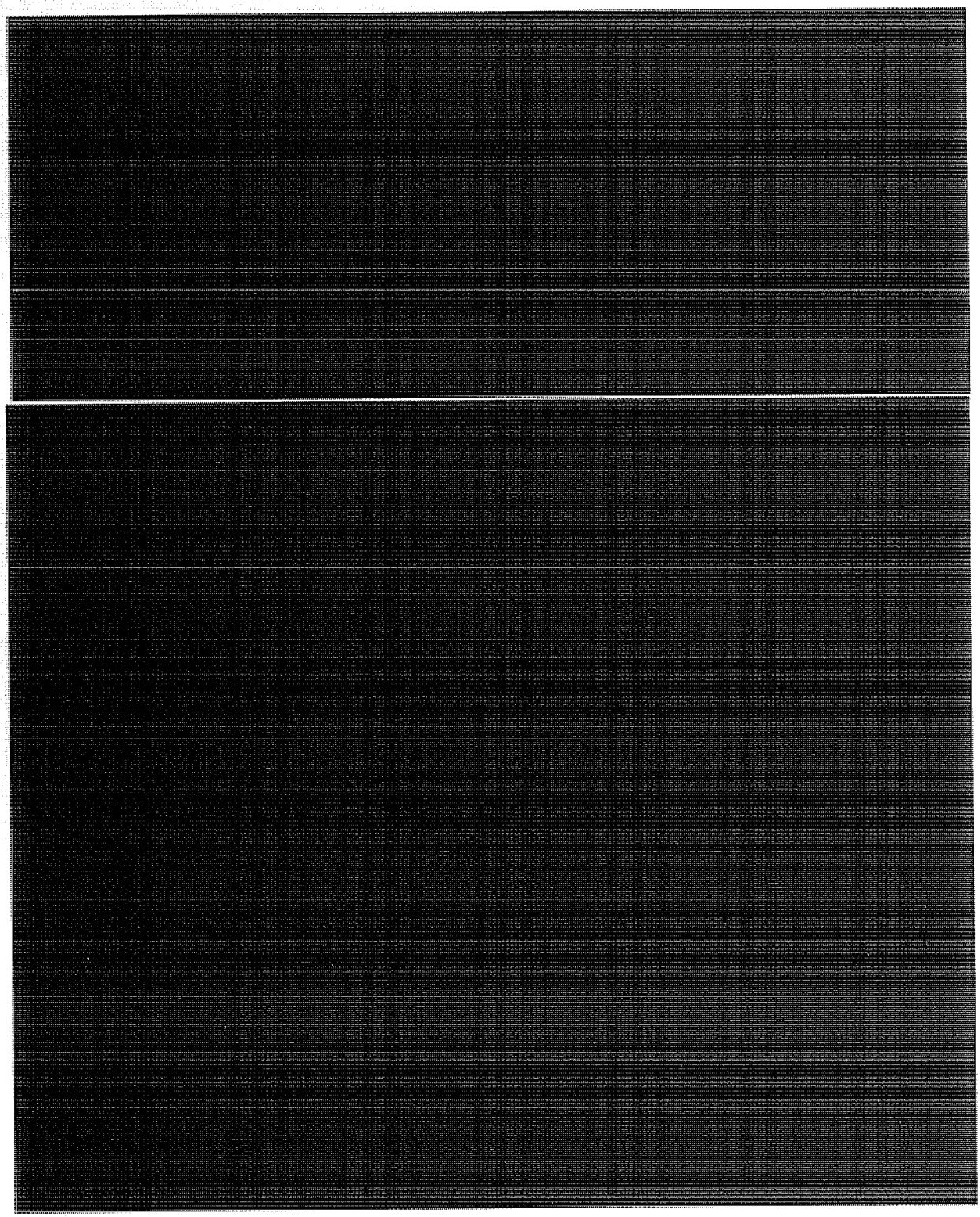
b1,
b3,
b7E

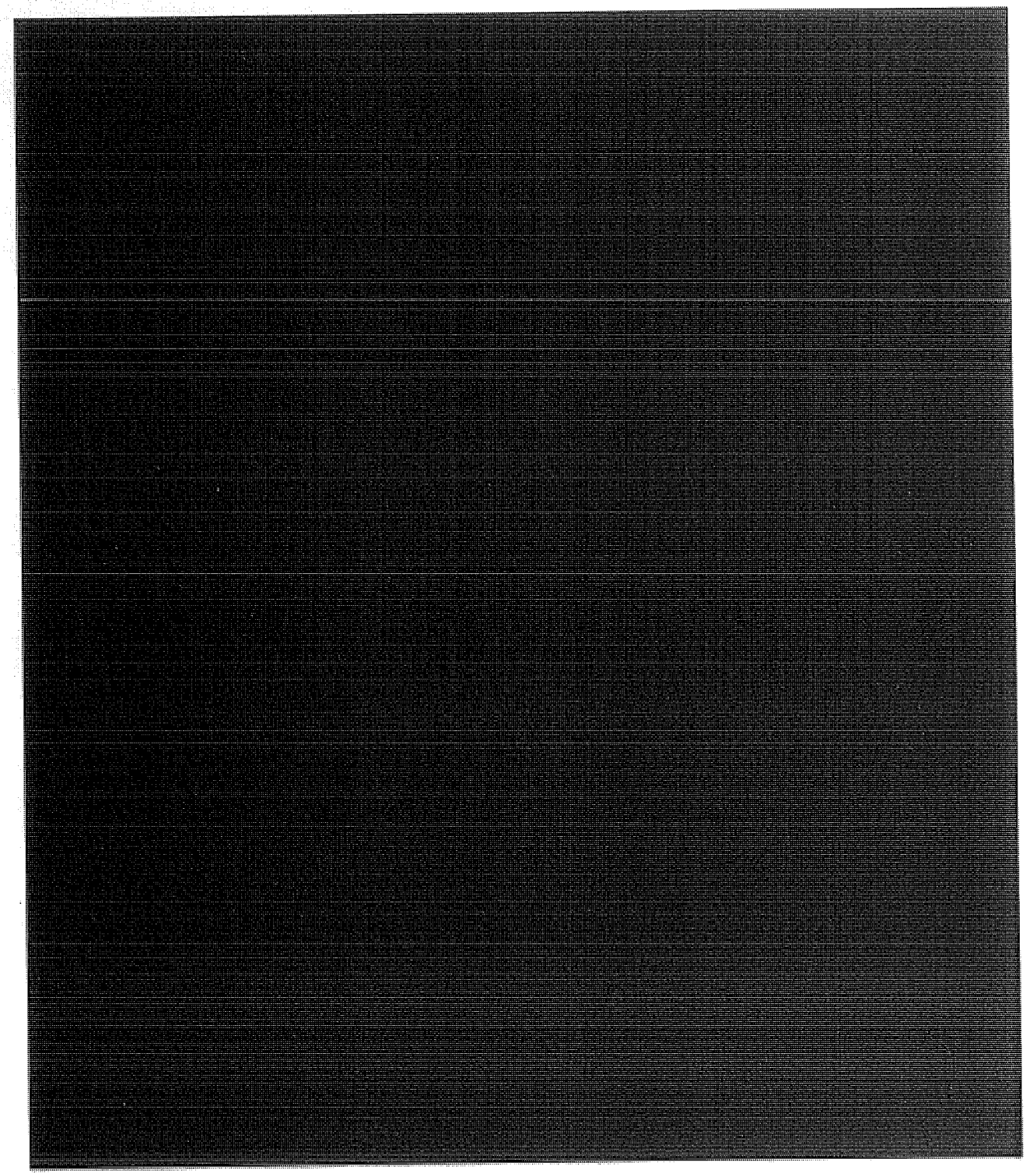










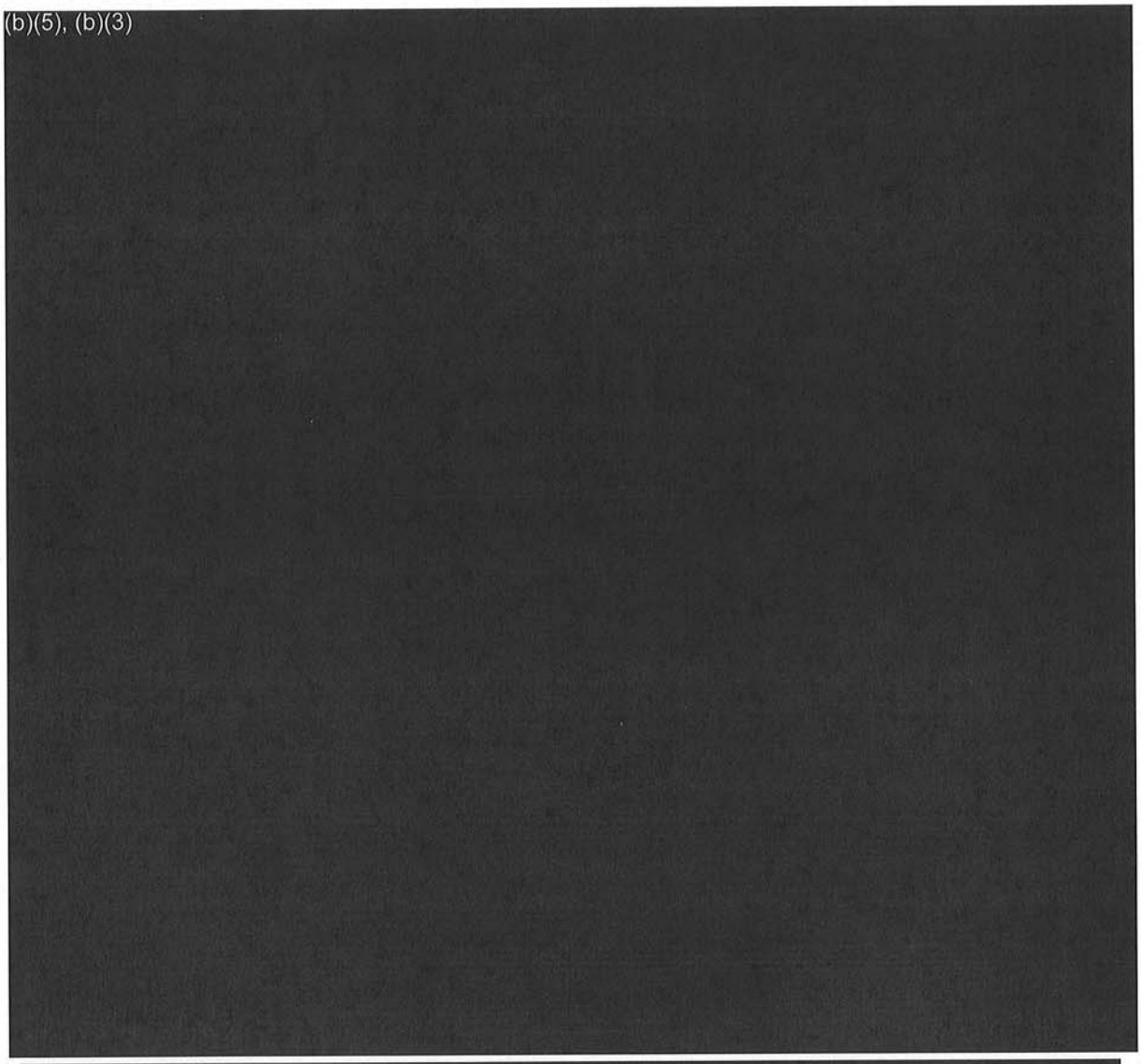


(b)(3)

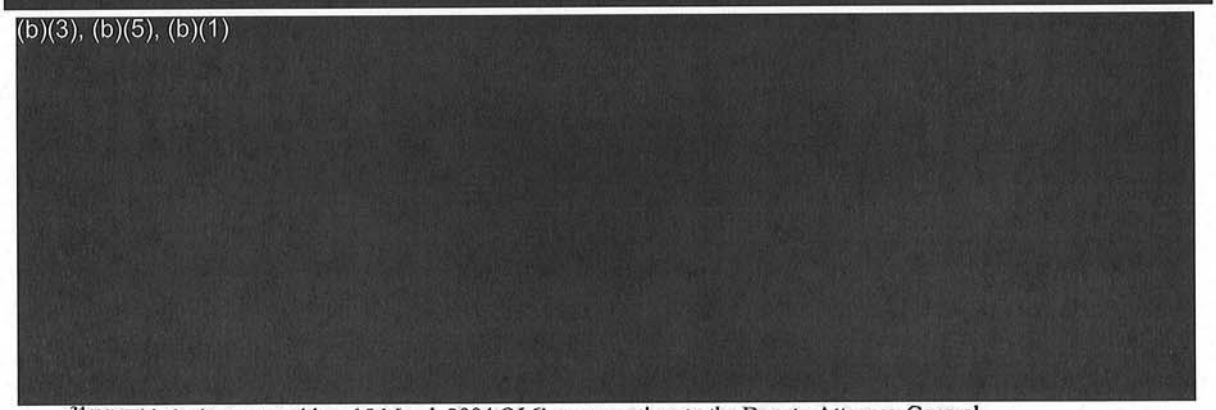
(b)(3)

(b)(3)

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



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



[24](U) This is documented in a 15 March 2004 OLC memorandum to the Deputy Attorney General.

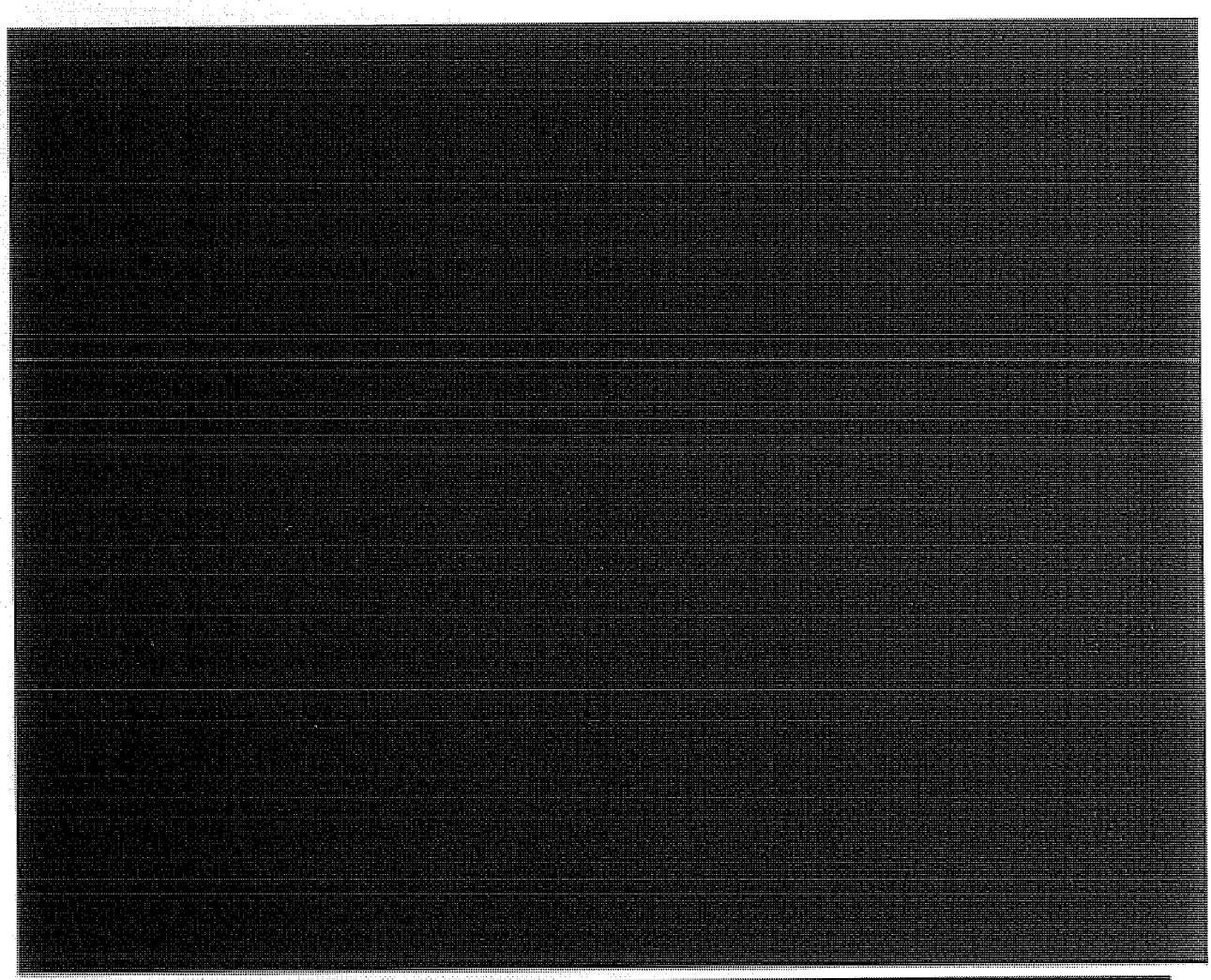
(b)(1), (b)(3)

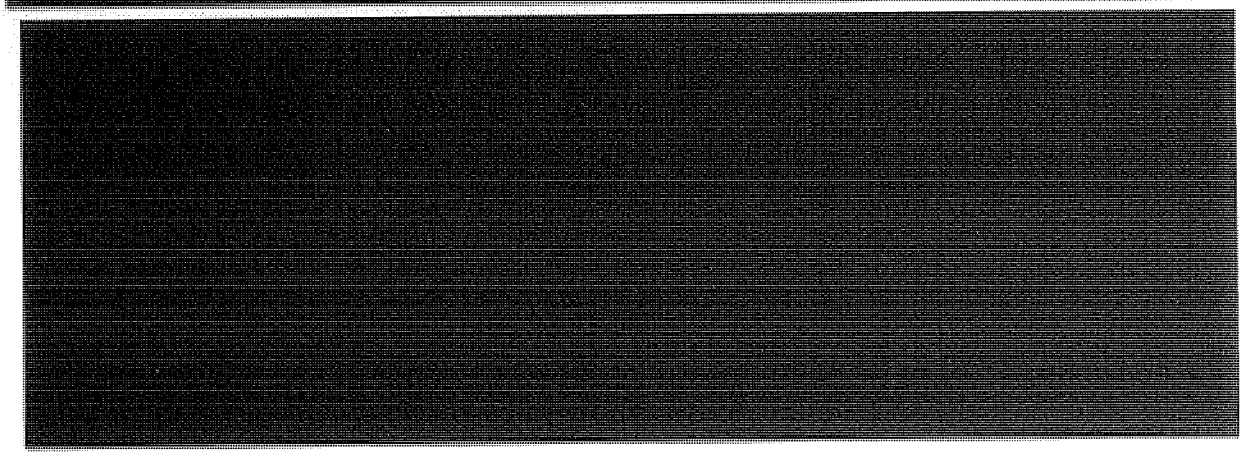
~~(TS//SI//NF)~~ On 12 March, the President directed DoJ to continue working on the legal issues, and on 15 March OLC issued a three page memorandum to the Deputy Attorney General stating that, while it had only begun to analyze the issues and was not yet prepared to issue a final opinion, it believed that (b)(1), (b)(3) types of collection authorized under the PSP were legally supportable. OLC had not yet developed a supportable argument to justify

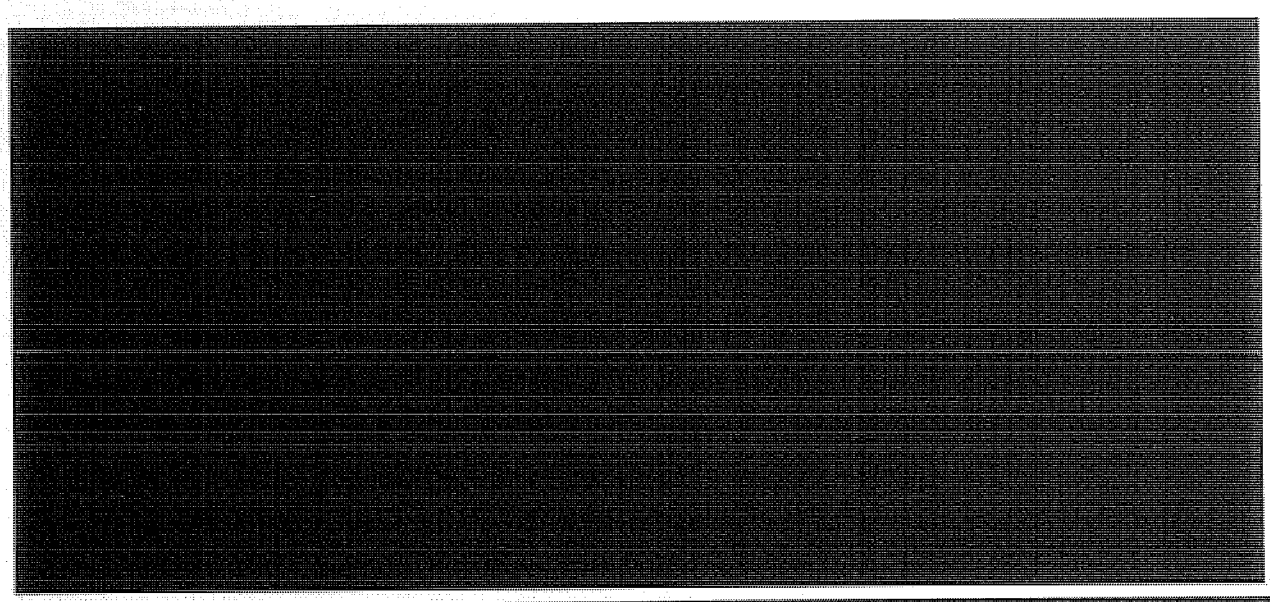
(b)(1), (b)(3), (b) (5)

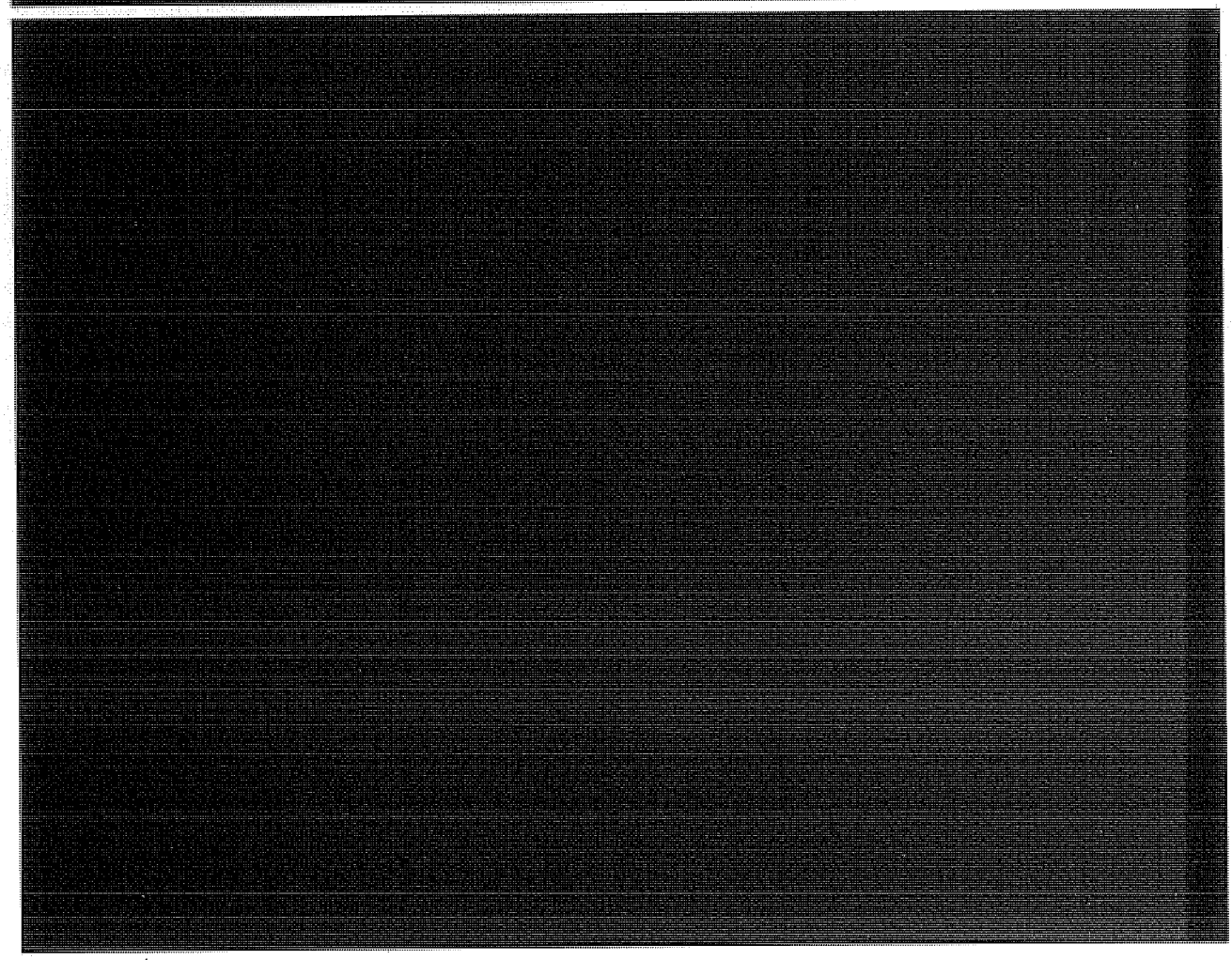
(b)(1), (b)(3)

[25] ~~(TS//SI//NF)~~ The Assistant Attorney General for OLC issued a memorandum on 6 May 2004 concluding that operation of the PSP as described in the opinion was lawful. A 16 July memorandum upheld the 6 May opinion. (b) (5)



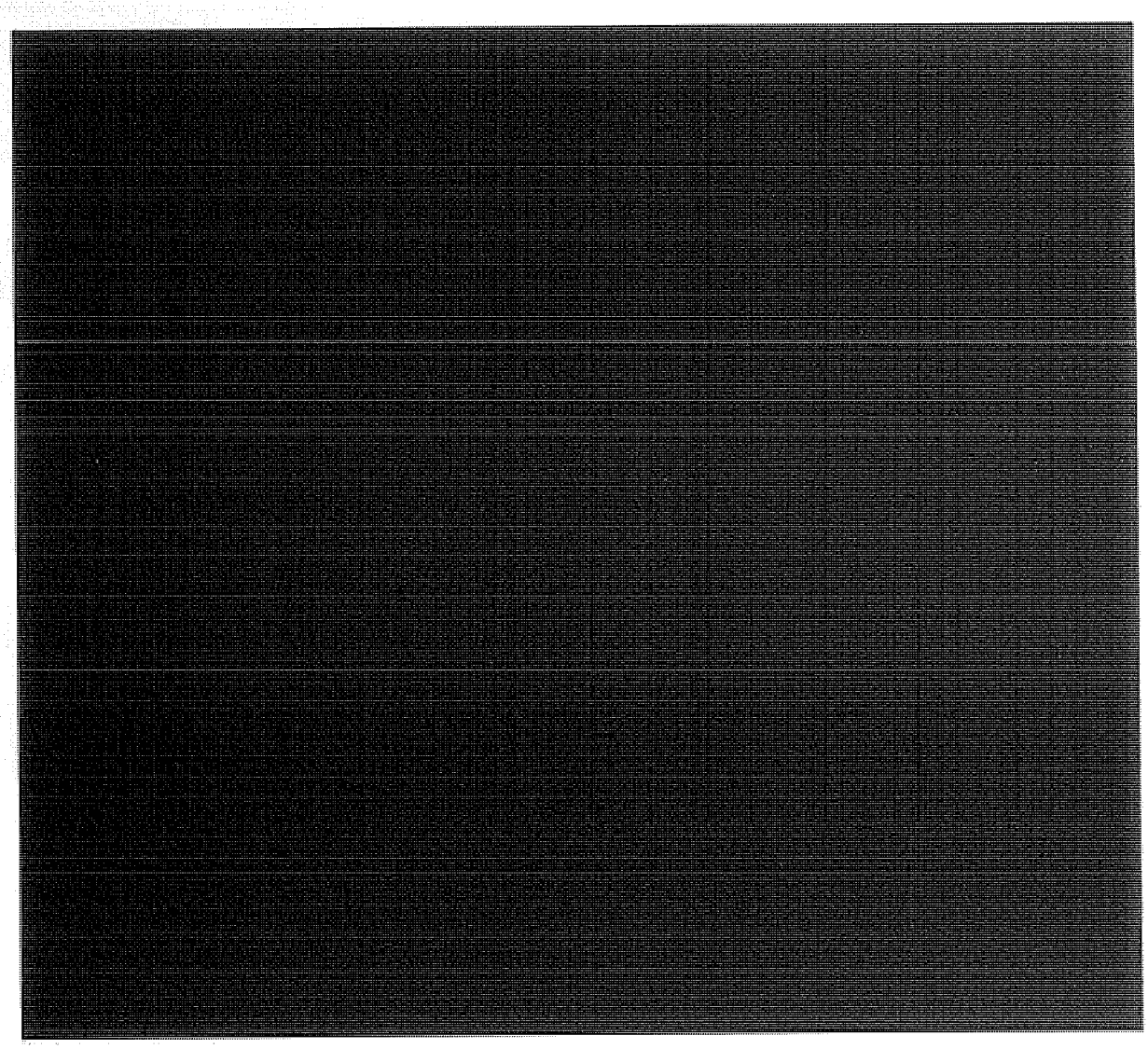




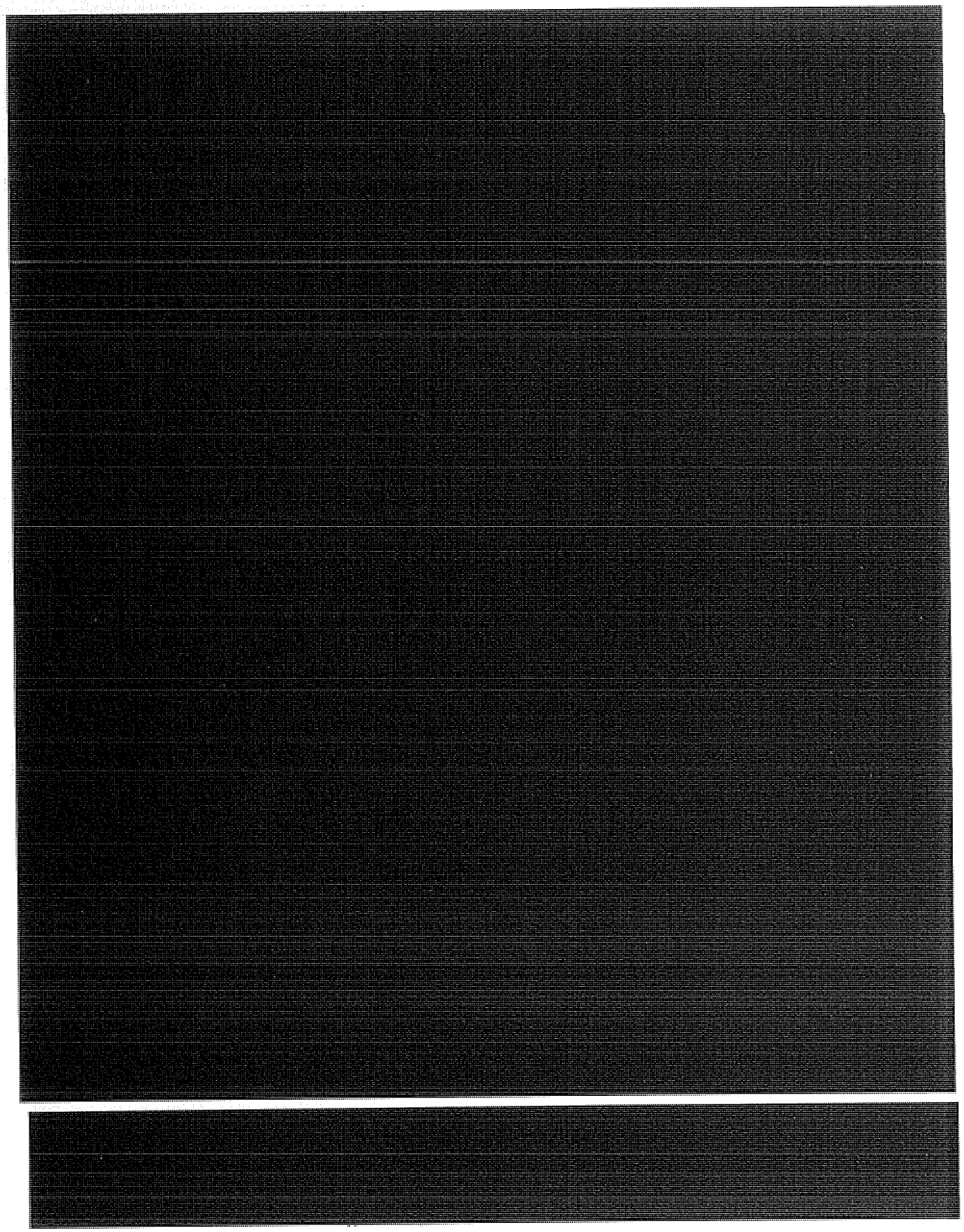


[redacted]

[27] ~~(TS//SI//NF)~~ The minimization probable cause standard states that the Agency may target for collection, communications for which there is probable cause to believe that one of the communicants is a member or agent of [redacted] and the communication is to or from a foreign country.



This page intentionally left blank.



[redacted]

(U//~~FOUO~~) The OIG issued a report for each of the 13 investigations and reviews described above. Ten reports on PSP activity resulted in 11 recommendations to management; 10 have been closed, and one remains open. Three reports on FISC-approved activity previously authorized by the PSP contained nine recommendations to management; three have been closed and six remain open.

~~(TS//STLW//SI//OC/NF)~~ Beginning in January 2007, violations that had occurred under the Authorization and violations related to PSP activity transitioned to court orders were reported quarterly to the President's Intelligence Oversight Board (through the Assistant to the Secretary of Defense for Intelligence Oversight).

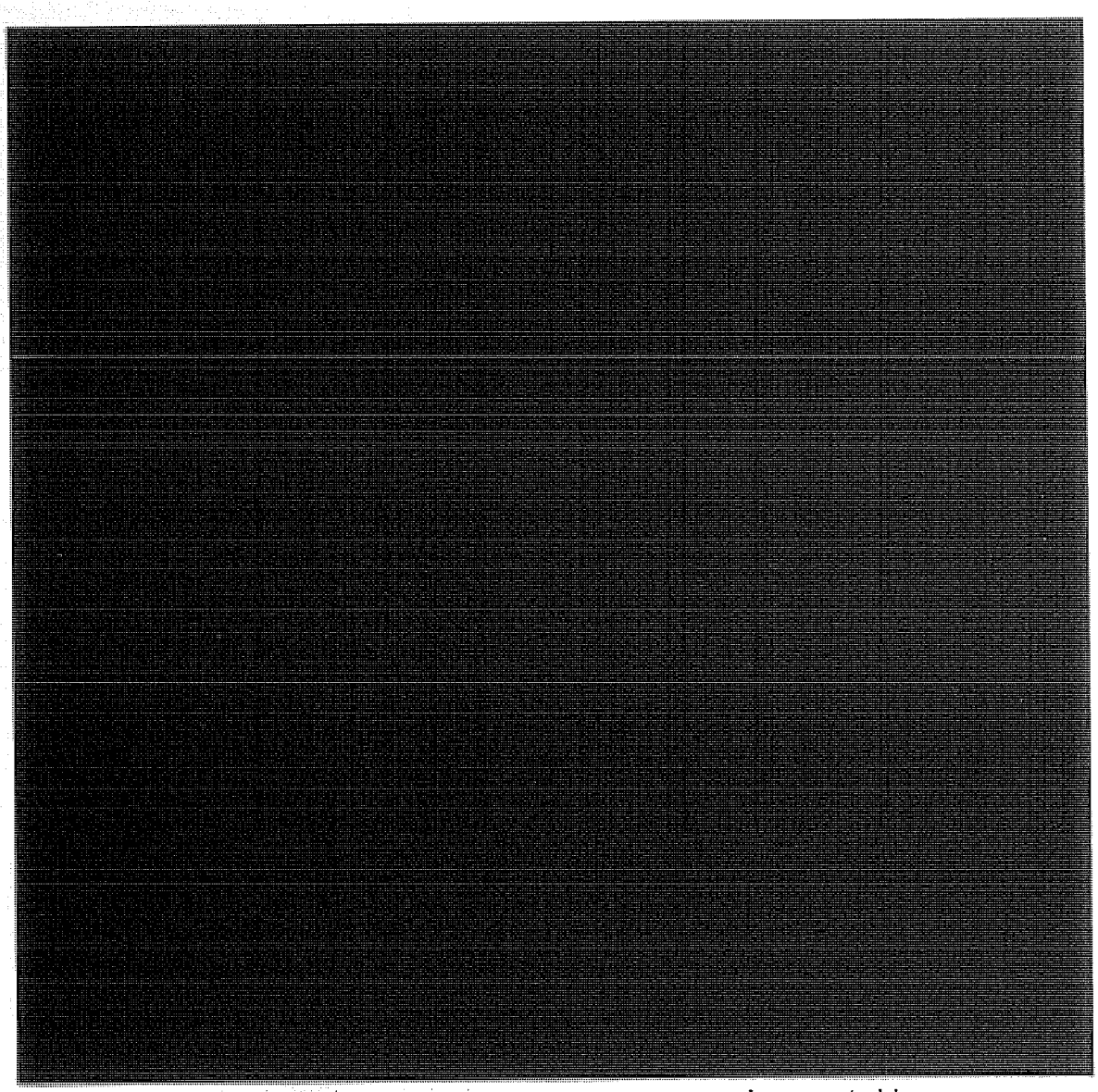
[redacted]

(U) Recently Reported Incidents

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

~~(TS//SI//NF)~~ On 15 January 2009, the Department of Justice reported to the FISC that NSA had been using an "alert list" to compare incoming business records FISA metadata against telephone numbers associated with counterterrorism targets tasked by NSA for SIGINT collection. NSA had reported to the Court that the alert list consisted of numbers for which NSA had determined that a reasonable articulable suspicion existed that the numbers were related to a terrorist organization associated [redacted] However, the majority of selectors on the alert list had not been subjected to a reasonable articulable suspicion determination. The NSA OIG has reported this incident to the President's Intelligence Oversight Board and has filed 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 Congressional oversight committees.

[redacted]



(U//~~FOUO~~) Other IG Program concerns were documented in the 2003-2008 reports. Presidential Notifications are listed and described in Appendix F. The 2008 report described the adequacy of Program decompartmentation plans.

(U) ACRONYMS AND ABBREVIATIONS

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

Bps	Bits per Second
BR	Business Records
CDR	Call Detail Records
[redacted]	
CIA	Central Intelligence Agency
COMINT	Communications Intelligence
CT	Counterterrorism
DCI	Director of Central Intelligence
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
EO	Executive Order
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GC	General Counsel
Gbps	Gigabits per Second
HPSCI	House Permanent Select Committee on Intelligence
IG	Inspector General
LAN	Local Area Network
[redacted]	[redacted]
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
O&C	Oversight and Compliance
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIPR	Office of Intelligence Policy and Review (now the Office of Intelligence, National Security Division)
OLC	Office of Legal Counsel

PM	Program Manager
PR/TT	Pen Register/Trap & Trace
PSP	President's Surveillance Program
RFI	Request for Information
SID	Signals Intelligence Directorate
SIGINT	Signals Intelligence
SSCI	Senate Select Committee on Intelligence
[redacted]	
TS/SCI	Top Secret/Sensitive Compartmented Information

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

(U) GLOSSARY OF TERMS

(U) COMINT	(U) Communications Intelligence – technical and intelligence information derived from foreign communications by someone other than the intended recipients
(U) E.O. 12333	(U) Executive Order 12333 - *United States Intelligence Activities* - provides goals, duties, and responsibilities with respect to the national intelligence effort. It mandates that certain activities of U.S. intelligence components are to be governed by procedures issued by agency heads and approved by the Attorney General.
(U) FISA	(U) The Foreign Intelligence Surveillance Act of 1978, as amended, governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information.
(U) [redacted]	~~(S//SI//NF)~~ Analytic tool for contact chaining used by analysts to do target discovery by quickly and easily navigating global communications metadata
~~(TS//SI//NF)~~ METADATA	~~(TS//SI//NF)~~ Header, router, and addressing-type information, including telecommunications dialing-type data, but not the contents of the communication
(U) [redacted]	[redacted]
(U) [redacted]	~~(S//NF)~~ NSA's primary storage, search, and retrieval mechanism for SIGINT text
(U) SANITIZATION	(U) The process of disguising COMINT to protect sensitive intelligence sources, methods, capabilities, and analytical procedures in order to disseminate the information outside COMINT channels.

(U) SIGNALS INTELLIGENCE	(U) A category of intelligence comprising individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation intelligence (FISINT), however transmitted.
(U) TEAR LINE REPORTS	(U) Reports used to disseminate SIGINT-derived information and sanitized information in the same record. The sanitized tear line conveys the same facts as the COMINT-controlled information, while hiding COMINT as the source.
(U) TELEPHONY	(U) The technology associated with the electronic transmission of voice, fax, and other information between parties using systems historically associated with the telephone
(U) TIPPERS	[redacted]

APPENDIX A

(U) About the Review

This page intentionally left blank.

(U) About the Review

(U) Objectives

(U) The Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, which was signed into law on 10 July 2008, requires that the Inspectors General of Intelligence Community elements that participated in the President's Surveillance Program (PSP) conduct a comprehensive review of the Program. The NSA Office of the Inspector General (OIG) reviewed NSA's participation in the PSP. The specific review objectives were to examine:

- (U) The establishment and evolution of the PSP as it affected NSA
- (U) NSA implementation of the PSP, including preparation and dissemination of product under the PSP
- (U) NSA access to legal reviews of the PSP and access to information about the Program
- (U) NSA communications with and representations made to private sector entities and private sector participation
- (U) NSA interaction with the Foreign Intelligence Surveillance Court (FISC) and transition of PSP-authorized collection to court orders
- (U) Oversight of PSP activities at NSA.

(U) Scope and Methodology

(U) This review was conducted in accordance with generally accepted government auditing standards, as set forth by the Comptroller General of the United States and implemented by the audit manuals of the DoD and NSA/CSS Inspectors General.

(U) The review was conducted from 10 July 2008 to 15 May 2009 in coordination with the Inspectors General of the Department of Defense, Office of the Director of National Intelligence, CIA, and DoJ.

(U//~~FOUO~~) The scope of this review was limited to NSA's participation in the PSP from 4 October 2001 to 17 January 2007. The review included NSA activities before and after the terrorist attacks of 11 September 2001 that led to the Presidential Authorization on 4 October 2001. It also included the transition of PSP-authorized activity to FISC orders.

(~~TS//NF~~) To satisfy review objectives, we interviewed [redacted] current and former NSA personnel who participated in the PSP including NSA Directors and Deputy Director, General Counsels, Deputy General Counsels, Associate General Counsels for Operations, and the Inspector General responsible for Program oversight from August 2002 until August 2006. We also interviewed former [redacted] as well as leadership [redacted] within the Signals Intelligence Directorate.

(~~TS//SI//NF~~) Interviews of the former Director of NSA, General Hayden, the former NSA Associate General Counsel for Operations, [redacted] were conducted with other IG offices involved in the joint PSP review.

(U//~~FOUO~~) We requested White House documentation of meetings at which General Hayden or NSA employees discussed the PSP or the Terrorist Surveillance Program with the President, Vice President, or White House personnel, but did not receive a response before publication of this report.

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

(U//~~FOUO~~) We reviewed NSA records dated 27 July 1993 to 10 July 2008 that pertained to review objectives. Records included NSA policies and regulations, correspondence, e-mail, briefings, notes, reports, calendars, and database reports.

(~~S//NF~~) Numbers of selectors tasked and reports issued were based on information provided by the PSP Program Management Office and were not independently verified during this review.

(U//~~FOUO~~) Information about individuals cleared for access to Program information was based on records provided by the PSP Project Security Officer and were not independently verified during this review.

(U) Prior Coverage

(U//~~FOUO~~) The OIG began oversight of the PSP and related activities in August 2002 and issued twelve reports dated 21 February 2003 through 30 June 2008 (Appendix E.) The OIG also issued 14 Presidential notifications from March 2003 to October 2006 (Appendix F). Detailed discussion of the OIG's oversight of the PSP is included in Section VIII of this report.

~~(TS//SI//NF)~~ As portions of the Program were transitioned to FISC orders for the collection of internet metadata and telephony business records, the OIG reviewed the execution and adequacy of controls in ensuring compliance with the orders. The OIG did not test the efficacy of controls for metadata collected under the authority of the PSP or court orders. Three reports summarized OIG investigations into possible misuse of the Authority or violations of FISC orders. One report summarized the OIG's oversight of the PSP, and the last report reviewed the adequacy of Program decompartmentation plans.

This page intentionally left blank.

APPENDIX B

(U) The Presidential Authorizations

This page intentionally left blank.

(U) The Presidential Authorizations

~~(TS//STLW//SI//OC/NF)~~ The Authorization documents that contained the terms under which NSA executed special Presidential authority were addressed to the Secretary of Defense and were titled "*Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States.*" The first Authorization consisted of eight paragraphs, and all but one subsequent Authorization consisted of nine. There were 43 Authorizations, two modifications, and one document described as (b)(1), (b)(3)

Description of Authorization contents by paragraph:

(U) Paragraph 1 - The President's Conclusions

~~(TS//STLW//SI//OC/NF)~~ The first paragraph referred to the 11 September 2001 terrorist attacks and the President's directions [to the Secretary of Defense] on employing U.S. Armed Forces. The first Authorization contained statements on the President's conclusions based on information about terrorist capabilities; this statement became the second paragraph in subsequent Authorizations. After the first Authorization, paragraph one included references to all previous versions of the Authorization and the dates they were signed by the President.

(U) Paragraph 2 - Terrorism Threat

~~(TS//STLW//SI//OC/NF)~~ After the first Authorization, the second paragraph stated that the President based his conclusions about terrorist capabilities on information provided by the DCI, including an attached terrorism threat assessment, a document that consisted of five or more pages and was signed by the DCI (later by the DNI) and the Secretary of Defense.

(U) Paragraph 3 - Considerations

~~(TS//STLW//SI//OC/NF)~~ The third paragraph contained the President's considerations in authorizing electronic surveillance, including the potential for deaths, injuries, and destruction from acts of terrorism, their probability, the need for action and secrecy, and intrusion into privacy, its reasonableness, and alternatives. In the first Authorization the considerations were in paragraph two.

~~(TS//STLW//SI//OC/NF)~~ Paragraph three of the first Authorization stated the President's determination that an

"extraordinary emergency" existed made electronic surveillance without a court order a compelling Government interest.[1]

~~(TS//STLW//SI//OC/NF)~~ Paragraph 4 - Authorized Electronic Surveillance

~~(TS//STLW//SI//OC/NF)~~ Paragraph four contains the President's statement of the basis for issuing the authority and the substantive description of the electronic surveillance that he authorized and directed. The President states that he is acting pursuant to Article II of the Constitution, including the executive power, his authority as Commander in Chief of the Armed Forces, his duty to preserve, protect and defend the Constitution, and the Authorization for Use of Military Force Joint Resolution (Public Law 107-40), with due regard for the Fourth Amendment. There were major and minor changes in that description, resulting in seven versions of paragraph four over approximately six years.

~~(TS//SI//NF)~~ Changes to Authorization Language on Electronic Surveillance

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

Version/Date	Description of Changes to Authorization Language
First Authorization 4 October 2001	Authorized NSA to acquire the content and associated metadata of telephony and Internet communications including wire and cable communications carried into or out of the United States for which there was probable cause to believe that one of the communicants was (b)(1), (b)(3) that one communicant was engaged in or preparing for acts of international terrorism.[2] This was the only version of the Authorization to use the term "probable cause." Version 1 also authorized the acquisition of telephony and Internet metadata for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. Paragraph four included the authority to

[1](U) The third paragraph was marked with the number three in two places until the error was corrected in the September 2003 authorization.
[2](U) This parenthetical condition is present in all descriptions of content collection.

Version/Date	Description of Changes to Authorization Language
	retain, process, analyze and disseminate intelligence from the communications acquired under the authority.
Version 2 2 November 2001 and 30 November 2001	Authorized NSA to acquire the content and associated metadata of communications for which there was "reasonable grounds to believe" that one of the communicants was (b)(1), (b)(3) that one communicant was outside the United States and was engaged in or preparing for acts of international terrorism.[3] This change to the wording on collecting content eliminated the possibility of interpreting the authority to permit collection with both ends in the United States. This version also authorized the acquisition of telephony and Internet metadata for communications with at least one communicant outside the United States, with no communicant known to be a citizen of the United States, or when there were reasonable grounds to believe that the communication related to international terrorism or activities in preparation for international terrorism. Version 2 was used in two Authorization documents.
Version 3 9 January 2002 to 14 January 2004	Eliminated (b)(1), (b)(3) but was otherwise identical to the previous version. This version of the authorizing provision was used in 19 of the documents.
Version 4 11 March 2004	Stated that the Department of Defense may obtain and retain Internet and telephony metadata (b)(1), (b)(3) on the condition that search and retrieval of that information was conducted in accordance with the Authorization. The term "acquire" was defined with respect to metadata as the act of querying stored data. (b)(1), (b)(3) The provision contained the President's statement that both

[3](U) Qualified as "based on the factual and practical considerations of everyday life on which reasonable persons act."

Version/Date	Description of Changes to Authorization Language
	these clarifications were consistent with all previous Authorizations and thus approval for acting under that definition was retroactive.
Version 5 19 March 2004	Became effective in the middle of a previously authorized period as the result of a modification. NSA's authority to collect content and associated metadata was changed to specify that the terrorist groups for which there was authority to collect were al-Qa'ida, groups affiliated with al-Qa'ida, or another group that the President determined was in armed conflict with the United States. NSA's authority to [redacted] (b)(1), (b)(3)
Version 6 2 April 2004 to 10 September 2005	Also became effective in the middle of a previously authorized period as the result of a modification. NSA's authority [redacted] (b)(1), (b)(3) al-Qa'ida, a group affiliated with al-Qa'ida, or of another group that the President determined was in armed conflict with the United States. Version 6 was used in 12 of the documents.
Version 7 26 October 2005 to 8 December 2006	Added the clarification that groups affiliated with al-Qa'ida [redacted] (b)(1), (b)(3) the provision was otherwise identical to that in version 6. Version 7 and was used in the final nine documents.

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

(U//~~FOUO~~) Paragraph 5 - Detect and Prevent

~~(TS//STLW//SI//OC/NF)~~ In paragraph five, the President stated that the surveillance was essential and appropriate to

detect and prevent future acts of terrorism in the United States.

(U//~~FOUO~~) Paragraph 6 - Minimization

~~(TS//STLW//SI//OC/NF)~~ Paragraph six directed that information concerning American citizens be minimized to the extent consistent with the mission and with the Authorization.

(U//~~FOUO~~) Paragraph 7 - Notifying Congress

~~(TS//STLW//SI//OC/NF)~~ Paragraph seven stated that notification of the Authorization outside the executive branch would be deferred, but the President stated his intent to notify Congress when consistent with national defense. When select members of Congress were briefed on the Program, information on the briefings was contained in paragraph eight.

(U) Paragraph 8 - Other Notifications

~~(TS//STLW//SI//OC/NF)~~ The initial Authorization specified that collection would cease 30 days after signature and required reporting on changes in circumstances underlying the Authorization. After the initial Authorization, paragraph eight contained a statement on restricting notifications to U.S. Government officials outside the executive branch or it named individuals, by title, who had been informed since the previous Authorization period expired.

(U) Paragraph 9 - Expiration

~~(TS//STLW//SI//OC/NF)~~ After the initial Authorization, the exact date of expiration was specified in paragraph nine.

(U//~~FOUO~~) Paragraph 10 - "The President's Ultimate Responsibility"

~~(TS//STLW//SI//OC/NF)~~ The Authorization signed in March of 2004 – the only one not signed by the Attorney General or a Deputy Attorney General– is also the only Authorization that contains a paragraph ten. This paragraph contained a legal argument about the President's ultimate responsibility to interpret the law on behalf of the executive branch and his authority for issuing the Authorization.

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

(U//~~FOUO~~) Signature of President

~~(TS//STLW//SI//OC/NF)~~ The Authorizations were signed by the President, followed by a place and date of signature. All but one authorization was signed in Washington, D.C.

(U) Other Signatures

~~(TS//STLW//SI//OC/NF)~~ Under the phrase "approved for form and legality," the Attorney General signed all but one of the Authorizations. The other authorization and the two modifications were signed by the Counsel to the President.

(U) Handwritten Note

~~(TS//STLW//SI//OC/NF)~~ The first 2 and the last 29 Authorizations, both modifications, and (b)(1), (b)(3) have a handwritten note signed by the Secretary of Defense (or Deputy Secretary of Defense) directing the NSA or the Director of NSA to execute the document.

APPENDIX C

(U) Timeline of Key Events

This page intentionally left blank.

(U) Timeline of Key Events

(U//~~FOUO~~) This timeline includes key events that occurred during NSA's implementation of the President's Surveillance Program (PSP). In addition to issuances of the Authorization, the timeline includes selected communications between NSA and Congress, the Foreign Intelligence Surveillance Court (FISC), [redacted] Because the timeline is limited to documented events and communications, it is not all-inclusive.

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

Date	Event
2001	
4-Oct-01	**1st Presidential Authorization signed**
4-Oct-01	General Hayden briefs White House (President, Vice President [VP], VP Counsel, VP Chief of Staff, White House Counsel)
[redacted]	[redacted]
25-Oct-01	NSA briefs Chair and Ranking Member of House Permanent Select Committee on Intelligence (HPSCI), Chair and Vice Chair of Senate Select Committee on Intelligence (SSCI)
2-Nov-01	**2nd Presidential Authorization signed**
[redacted]	[redacted]
14-Nov-01	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
30-Nov-01	**3rd Presidential Authorization signed**
4-Dec-01	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and Ranking Member, Senate Defense Appropriations Subcommittee
5 Dec 01	NSA briefs FBI Director Mueller
[redacted]	[redacted]
2002	
9-Jan-02	**4th Presidential Authorization signed**
[redacted]	[redacted]
11-Jan-02	NSA briefs Department of Justice, Office of Intelligence Policy and Review (DoJ, OIPR), James Baker
31-Jan-02	NSA briefs FISC Presiding Judge Lamberth
[redacted]	[redacted]
5-Mar-02	NSA briefs Chair and Ranking Member, HPSCI, and Vice Chair, SSCI
14-Mar-02	5th Presidential Authorization signed
[redacted]	[redacted]

Date	Event
10-Apr-02	NSA briefs Chair SSCI
18-Apr-02	6th Presidential Authorization signed
[redacted]	[redacted]
17-May-02	NSA briefs incumbent FISC Presiding Judge Kollar-Kotelly
22-May-02	7th Presidential Authorization signed
[redacted]	[redacted]
12-Jun-02	NSA briefs Chair, HPSCI, and Ranking Member HPSCI
24-Jun-02	8th Presidential Authorization signed
[redacted]	[redacted]
8-Jul-02	NSA briefs Chair and Ranking Member SSCI
30-Jul-02	9th Presidential Authorization signed
[redacted]	[redacted]
12-Aug-02	NSA briefs FISC Presiding Judge Kollar-Kotelly at the White House
13-Aug-02	NSA Inspector General (IG) cleared for the PSP
10-Sep-02	10th Presidential Authorization signed
11-Sep-02	NSA GC, Deputy General Counsel (GC), Associate GC for Operations, and IG meet to discuss PSP oversight
[redacted]	[redacted]
18-Sep-02	1st NSA Due Diligence Meeting
30-Sep-02	Chair HPSCI visits NSA for briefing
[redacted]	[redacted]
15-Oct-02	11th Presidential Authorization signed
[redacted]	[redacted]
18-Nov-02	12th Presidential Authorization signed
[redacted]	[redacted]
16-Dec-02	NSA IG advises General Hayden to issue "Delegation of Authority Letters" to "units that administer the project"
2003	
8-Jan-03	13th Presidential Authorization signed
[redacted]	[redacted]

Date	Event
[redacted]	[redacted]
13-Jan-03	FBI Director visits NSA for briefing
29-Jan-03	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
7-Feb-03	14th Presidential Authorization signed
[redacted]	[redacted]
4-Mar-03	General Hayden issues first Delegation of Authority letter to key Signals Intelligence (SIGINT) Directorate operational personnel
[redacted]	
17-Mar-03	15th Presidential Authorization signed
[redacted]	[redacted]
22-Apr-03	16th Presidential Authorization signed
[redacted]	[redacted]
11-Jun-03	17th Presidential Authorization signed
[redacted]	[redacted]
14-Jul-03	18th Presidential Authorization signed
[redacted]	[redacted]
17-Jul-03	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
10-Sep-03	19th Presidential Authorization signed
[redacted]	[redacted]

Date	Event
8-Oct-03	NSA-FBI-CIA conference at NSA to discuss PSP operations and customer needs
15-Oct-03	**20th Presidential Authorization signed**
[redacted]	[redacted]
1-Dec-03	NSA IG announces a review of NSA PSP operations
8-Dec-03	NSA IG asks VP Counsel for access to PSP legal opinions and is told that a request should come from General Hayden
9-Dec-03	**21st Presidential Authorization signed**
9-Dec-03	IG memo asks General Hayden to ask VP Counsel's permission for NSA IG and GC to obtain copies of, or view, PSP legal justification
[redacted]	[redacted]
2004	
6-Jan-04	NSA briefing to DoJ Mr. Philbin, Mr. Goldsmith for Mr. Goldsmith's orientation to the PSP and other NSA Signals Intelligence efforts against terrorism
8-Jan-04	NSA and FBI [redacted] meet to discuss the PSP and recent changes at NSA
14-Jan-04	**22nd Presidential Authorization signed**
[redacted]	[redacted]
9-Mar-04	General Hayden briefs Director of Central Intelligence (DCI) on value of the PSP
10-Mar-04	General Hayden briefs White House Counsel and Chief of Staff, Deputy DCI, Deputy AG, and FBI Director on value of the PSP
10-Mar-04	General Hayden briefs Speaker of the House, Senate Majority and Minority leaders, House Minority Leader, Chairman and Ranking Member, HPSCI, and Chair and Vice Chair, SSCI
10-Mar-04	General Hayden briefs Secretary of Defense, DoD Principal Deputy GC
11-Mar-04	**23rd Presidential Authorization signed**
11-Mar-04	NSA IG and Acting GC discuss new Authorization signed by President's Counsel rather than the AG
11-Mar-04	NSA briefs House Majority Leader
[redacted]	[redacted]
12-Mar-04	General Hayden briefs House Majority Leader
19-Mar-04	**Revision to 23rd Presidential Authorization signed**
[redacted]	General Hayden sends letter to Assistant AG, Office of Legal Counsel (OLC) [redacted]

Date	Event
	[redacted]
2-Apr-04	**2nd Revision to 23rd Presidential Authorization signed**
4-Apr-04	General Hayden briefs DoD Principal Deputy GC
5-May-04	**24th Presidential Authorization signed**
	[redacted]
20-May-04	NSA briefs the Minority Leader of the Senate
	[redacted]
23-Jun-04	**25th Presidential Authorization signed**
	[redacted]
14-Jul-04	Initial PR/TT Order approved by FISC
9-Aug-04	**26th Presidential Authorization signed**
	[redacted]
23-Aug-04	General Hayden briefs National Security Advisor and Homeland Security Advisor
	[redacted]
17-Sep-04	**27th Presidential Authorization signed**
	[redacted]
23-Sep-04	Presidential "further direction" of 9 August 2004 expires
23-Sep-04	NSA briefs Chair, HPSCI
	[redacted]
17-Nov-04	**28th Presidential Authorization signed**
	[redacted]
2005	
5-Jan-05	NSA briefs National Security Advisor and White House Counsel
	[redacted]
11-Jan-05	**29th Presidential Authorization signed**

Date	Event
[redacted]	[redacted]
3-Feb-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
25-Feb-05	General Hayden briefs White House Counsel and Counsel to Deputy AG
1-Mar-05	**30th Presidential Authorization signed**
2-Mar-05	NSA briefs Senate Minority Leader
[redacted]	[redacted]
19-Apr-05	**31st Presidential Authorization signed**
[redacted]	[redacted]
22-Apr-05	General Hayden briefs Director of National Intelligence (DNI)
23-May-05	Two-level PSP clearance structure discontinued
1-Jun-05	Discussions to seek FISC orders to authorize content collection begin with DoJ OLC
14-Jun-05	**32nd Presidential Authorization signed**
[redacted]	[redacted]
26-Jul-05	33rd Presidential Authorization signed
[redacted]	[redacted]
3-Aug-05	Principal Deputy DNI Hayden briefs new NSA/CSS Director General Alexander on the PSP
10-Sep-05	**34th Presidential Authorization signed**
14-Sep-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
26-Oct-05	**35th Presidential Authorization signed**
[redacted]	[redacted]
13-Dec-05	**36th Presidential Authorization signed**
16-Dec-05	New York Times says that President secretly authorized NSA eavesdropping on Americans
[redacted]	[redacted]
20-Dec-05	DoD IG receives letter, signed by 39 Congressmen, requesting a review of the PSP. DoD IG faxes the letter to the NSA IG on 10 Jan 06
21-Dec-05	NSA briefs DNI

Date	Event
2006	
3-Jan-06	NSA IG and DoD IG discuss letter from 39 Congressmen requesting DoD IG review of the PSP
9-Jan-06	NSA briefs nine FISC judges and three FISC legal advisors
11-Jan-06	NSA briefs Speaker of the House, Senate Majority Leader, Chair of HPSCI, Chair and Vice Chair, SSCI
20-Jan-06	NSA briefs Senate Minority Leader, House Minority Leader, Chair SSCI, and Ranking Member HPSCI
[redacted]	[redacted]
27-Jan-06	**37th Presidential Authorization signed**
31-Jan-06	NSA briefs FISC Judge Scullin
[redacted]	[redacted]
11-Feb-06	NSA briefs Chair SSCI
16-Feb-06	NSA briefs Speaker of the House and Chair, HPSCI
28-Feb-06	NSA briefs Chair and Ranking Member, House Appropriations Subcommittee on Defense
[redacted]	[redacted]
3-Mar-06	NSA briefs Vice Chair, SSCI
9-Mar-06	NSA briefs Chair and Vice Chair, SSCI, and Members of SSCI Terrorist Surveillance Program (TSP) Subcommittee (Roberts, Rockefeller, Hatch, DeWine, Feinstein, Levin, Bond) with SSCI Minority and Majority Staff Directors, Senior Director for Legislative Affairs, National Security Counsel, VP, AG, White House Counsel, and VP Chief of Staff
10-Mar-06	NSA briefs Mr. Bond, Member, SSCI TSP Subcommittee
13-Mar-06	NSA briefs Chair, SSCI TSP Subcommittee, Members SSCI TSP Subcommittee (Roberts, Feinstein, and Hatch), SSCI Majority and Minority Staff Directors, and SSCI Counsel at NSA
14-Mar-06	NSA briefs Mr. DeWine, Member, SSCI TSP Subcommittee at NSA
21-Mar-06	**38th Presidential Authorization signed**
21-Mar-06	NSA briefs FISC Judge Bates
[redacted]	[redacted]
27-Mar-06	NSA briefs Mr. Levin, Member, SSCI TSP Subcommittee and Minority Staff Director at NSA
29-Mar-06	NSA briefs Chairman and Ranking Member HPSCI TSP Subcommittee, TSP Subcommittee Members (Hoekstra, Harman, McHugh, Rogers, Thornberry, Wilson, Davis, Holt, Cramer, Eshoo, and Boswell), Majority General Counsel, Staff Member, and Minority General Counsel

Date	Event
7-Apr-06	NSA briefs Chairman of the HPSCI TSP Subcommittee, HPSCI TSP Subcommittee Members (Hoekstra, McHugh, Rogers, Thornberry, Wilson, and Holt), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	[redacted]
28-Apr-06	NSA briefs Ranking Member, HPSCI TSP Subcommittee, Members of HPSCI TSP Subcommittee (Harman, Wilson, and Eshoo), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	
11-May-06	NSA briefs Chair and Ranking Member House Appropriations Committee Defense Subcommittee
16-May-06	**39th Presidential Authorization signed**
17-May-06	Chair SSCI, Members, SSCI (Roberts, Hagel, Mikulski, Snowe, DeWine, Bayh, Chambliss, Lott, Bond, Levin, Feingold, Feinstein, Wyden, Warner), SSCI Staff Member, SSCI Majority Staff Director, and SSCI Counsel
17-May-06	HPSCI Chair, HPSCI Members (Hoekstra, Harman, Wilson, Eshoo, Rogers, Thornberry, Holt, Boswell, Cramer, LaHood, Everett, Gallegly, Davis, Tiahrt, Reyes, Ruppersberger, and Tierney), Majority General Counsel, Staff Director, and Minority General Counsel
[redacted]	[redacted]
24-May-06	First Business Records Order approved by the FISC
5-Jun-06	NSA briefs Ms. Feingold, SSCI Member at NSA
7-Jun-06	NSA briefs Ranking Member, Senate Defense Appropriations Subcommittee, and SSCI Staff Director
7-Jun-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
9-Jun-06	NSA briefs Chair, SSCI, SSCI Members (Mikulski, Wyden, and Hagel), SSCI Minority Staff Director, SSCI Counsel, and SSCI Staff Director
15-Jun-06	NSA briefs Chair, SSCI and SSCI Members (Roberts, Mikulski, Feingold, Bayh, Snowe, Hatch, Lott, and Bond), and Minority Staff Director
26-Jun-06	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and House Minority Leader
30-Jun-06	NSA briefs Mr. Bayh, SSCI Member at NSA
6-Jul-06	**40th Presidential Authorization signed**
[redacted]	[redacted]
10-Jul-06	NSA briefs Ms. Snowe, SSCI Member and SSCI Counsel at NSA
18-Jul-06	NSA briefs Mr. Chambliss, SSCI Member at NSA
[redacted]	
6-Sep-06	**41st Presidential Authorization signed**
[redacted]	[redacted]

Date	Event
[redacted]	[redacted]
24-Oct-06	**42nd Presidential Authorization signed**
[redacted]	[redacted]
20-Nov-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
8-Dec-06	**43rd and final Presidential Authorization signed**
[redacted]	[redacted]

2007

10-Jan-07	Content orders approved by the FISC
17-Jan-07	AG letter to Congress: Presidential program brought under the FISC
1-Feb-07	NSA briefs President's Privacy and Civil Liberties Oversight Board
1-Feb-07	Presidential Authorization expires

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

This page intentionally left blank.

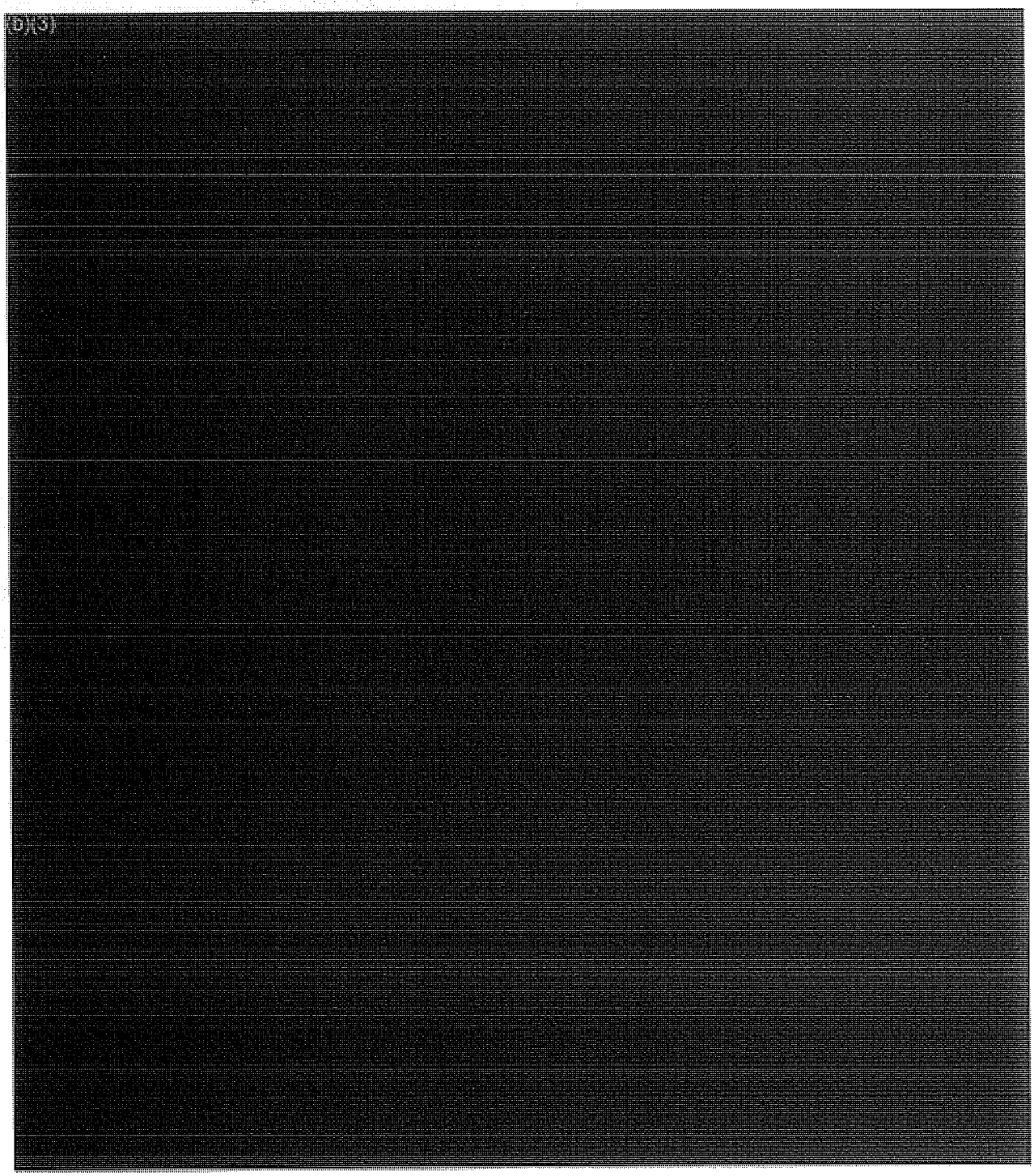
APPENDIX D

(U) Cumulative Number of Clearances for the President's Surveillance Program

This page intentionally left blank.

(U) Cumulative Number of Clearances for the President's Surveillance Program[4]

(b)(3)



This page intentionally left blank.

APPENDIX E

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

This page intentionally left blank.

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

~~(TS//SI//NF)~~ This appendix lists and describes OIG investigation and review reports of activity conducted under the PSP, also referred to as the STELLARWIND Program, and related activities such as the Pen Register Trap and Trace (PR/TT) Order and the Business Records Order. These reports are limited to activity conducted between 4 October 2001 and 17 January 2007.

(U) OIG Investigations

[redacted]

(U) Report of Investigation of Two Violations

~~(S//NF)~~ On [redacted] the OIG issued a report on what it believed to be the first two violations of Authorization, both of which were unintentional.

~~(TS//STLW//SI//OC/NF)~~ The first incident occurred on [redacted] An NSA analyst misguidedly used PSP authority to collect communications between [redacted] These communications were foreign within the meaning of the Authorization, but they were not terrorist related, [redacted]

~~(TS//STLW//SI//OC/NF)~~ The second incident occurred on [redacted] when NSA inappropriately performed contact chaining on [redacted] This query was requested by an FBI official during the investigation of [redacted]

~~(S//NF)~~ NSA OIG found that in neither incident had NSA personnel acted with intent to disregard their authority.

Both incidents occurred, at least in part, because early in the Program the terms of the Authorization were so closely held that few, if any, operational personnel working under the Authority were permitted to see the Authorization or its operative provisions. It was unreasonable to hold persons accountable for violating an order that they had not seen, when the order was too complex to be easily committed to memory. Accordingly, the OIG did not recommend disciplinary action, but did recommend that the NSA Director issue formal written delegations of authority to the Signals Intelligence Director and specified subordinates so that personnel working the Program would know the precise terms of the Authorization. Management concurred with the recommendations and made appropriate notifications.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

[redacted] ~~(TS//SI//NF)~~ ***Violations of Court Orders in [redacted] Foreign Intelligence Surveillance Court***

~~(TS//STLW//SI//OC/NF)~~ On 14 July 2004 [redacted] The Order permitted NSA to collect Internet metadata under the pen register/trap-and-trace provisions of the FISA (§§ 1841-1846). The authority to collect Internet metadata under the Order [redacted] Material acquired under the Order continued to be protected in PSP channels.

~~(TS//STLW//SI//OC/NF)~~ On [redacted] NSA OIG issued a report on an investigation of a management breakdown that had resulted in unintentional filtering violations of the FISC Order. The Order permitted NSA to collect Internet metadata from communications involving [redacted] The violations occurred because NSA [redacted] However, no violations resulted from the collection of domestic communications. An NSA collection manager discovered the violations on [redacted]. The following day, the questionable collection was stopped and reported to the OIG and the OGC. With the exception of [redacted] the OIG

found no reason to believe that any violations resulted in the collection of U.S. person information. The OIG reserved judgment on [redacted] The OIG evaluation of responsibility for the incident led directly to the replacement of the Program Manager and to changes in Program management, leadership, and chain of command.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

~~(TS//SI//NF)~~ Supplemental Report on Violations of Court Orders in [redacted]

~~(TS//STLW//SI//OC/NF)~~ A follow-up investigation of the questionable [redacted] revealed no additional violations. On [redacted] the NSA OIG issued a report detailing its examination of [redacted] that the OIG suspected might not have originated or terminated outside the United States. [redacted] All but [redacted] messages could have been associated with a foreign sender or recipient. [redacted] None of the [redacted] messages had been intentionally collected, none had been analyzed, and none had been reported outside NSA.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

(U) OIG Reviews

14 May 2004 ***(U) Need for Documentation and Development of Key Processes (ST-04-0024)***

~~(TS//SI//NF)~~ This OIG report concluded that a continuing deficiency in clear, written procedures governing the collection, processing, and dissemination of PSP material created undue risk of unintentional violations of the Authorization. The report noted that Program officials had

made progress in addressing some of these deficiencies, but found that processes had not been fully documented in the form of management directives, administrative policies, or operating manuals. The NSA OIG recommended that Program officials formally adopt rigorous, written operating procedures for the following key processes:

- Approvals for content collection by the appropriate named officials
- Reporting of violations of the Authority, similar to procedures for documenting violations of Legal Compliance and Minimization Procedures[5]
- Evaluation of dual FISA and PSP content collection
- Systematic identification and evaluation of telephone numbers and Internet identifiers for detasking.[6]

(U//~~FOUO~~) Corrective action was taken in response to the four recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 06 and HPSCI on 2 January 2008.

13 Sep 2004 ***~~(S//NF)~~ Need for Increased Attention to Security-Related Aspects of the STELLARWIND Program (ST-04-0025)***

(U//~~FOUO~~) This OIG report disclosed weaknesses in Program security. The Program was particularly vulnerable to exposure because it involved numerous organizations inside and outside NSA.

(U//~~FOUO~~) While the Program Manager placed a strong emphasis on personnel security, he did not take a proactive and strategic approach to physical and operational security. In particular, better use of the Program Security Officer would have helped to improve special security practices for handling Program material and strengthen operations security (OPSEC).

(U//~~FOUO~~) The Program Manager and the Associate Director for Security and Counterintelligence concurred with the findings and implemented corrective measures. In particular,

---

[5](U) U.S. Signals Intelligence Directive 18 or "USSID SP0018" (as of 27 July 2003).
[6](~~TS//SI//NF~~) [redacted]

the Staff Security Officer was freed from other responsibilities and took a more active and effective role in Program security. Management did not conduct a formal OPSEC survey as recommended; however, steps taken by management to implement OPSEC practices met the intent of the original recommendation.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

21 Nov 2005 ***~~(TS//SI//NF)~~ Review of the Tasking Process for STELLARWIND U.S. Content Collection (ST-04-0026)***

~~(TS//STLW//SI//OC/NF)~~ This report identified material weaknesses in the tasking and detasking process under the PSP. The process to task and detask telephone numbers for content collection under the Program was inherently fragile because it was based on e-mail exchanges and was not automated or monitored.

~~(TS//STLW//SI//OC/NF)~~ The OIG examined [redacted] telephone numbers and Internet identifiers approved for content collection on the date in November 2004 when the audit began and identified the following types of errors:

- [redacted] involved under-collection; identifiers were not put on collection quickly enough or were not put on collection until the OIG discovered the errors.
- [redacted] involved unauthorized collection caused by a typographical error.
- [redacted] involved over-collection; they were not removed from collection quickly enough.
- [redacted] record-keeping errors in the Program's tracking database

~~(TS//STLW//SI//OC/NF)~~ In the [redacted] of unauthorized collection caused by a typographical error, NSA personnel did not review the collected information before destroying it, nor did NSA issue any report based on, or otherwise disseminate, any information from the [redacted] of untimely detasking. However, without a robust and reliable collection and tracking process, NSA increased its risk of unintentionally violating the Authorization. NSA also increased the risk of missing

valuable foreign intelligence by failing to task telephone numbers and Internet identifiers in a timely manner.

(U//~~FOUO~~) NSA OIG recommended that all errors be swiftly resolved, that specific procedures be adopted to prevent recurrences, and that identifiers tasked for collection be promptly reconciled with identifiers approved for tasking, and repeated every 90 days. Management implemented the recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

31 May 2006 ***~~(TS//SI//NF)~~ Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027)***

~~(TS//STLW//SI//OC/NF)~~ This report determined that, based on a statistical sample, Program officials were adhering to the terms of the Authorization and the Director's delegation thereunder; that tasking was appropriately approved and duly recorded under the Authorization; and that tasking was justified as linked to al-Qa'ida or affiliates of al-Qa'ida. The report recommended improvements in record-keeping practices.

~~(S//NF)~~ Due to a lack of sufficient and reliable data, the NSA OIG could not reach a conclusion on the tasking approval process for two PSP-related collection programs. The OIG recommended that management responsible for the affected programs, design and implement a tasking and tracking process to allow managers to audit, assess timeliness, and validate the sequencing of tasking activities. Management agreed to install automated tracking of tasking and detasking.

~~(TS//SI//NF)~~ Although the collection architecture was designed to produce one-end-foreign communications, inadvertent collection of domestic communications occurred and was addressed. The OIG recommended changes in management reporting to improve the tracking and resolution of inadvertent collection issues.

(U//~~FOUO~~) Corrective action has been completed for one of the two recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

11 Jul 2006 ~~(TS//SI//NF)~~ ***Supplemental Report to Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027.01)***

~~(TS//STLW//SI//OC/NF)~~ After issuing the original report, the NSA OIG conducted further research to determine whether Program officials were approving content tasking requests based solely on metadata analysis. Using the statistical sample in the original audit, the OIG found no instances of metadata analysis as the sole justification for content tasking. In all cases tested, there was corroborating evidence to support the tasking decision.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

5 Sep 2006 ~~(TS//SI//NF)~~ ***Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records (ST-06-0018)***

~~(TS//STLW//SI//OC/NF)~~ On 24 May 2006, the telephony metadata portion of the PSP was transferred to FISC Order BR-06-05, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [Telecommunications Providers] *Relating to* [redacted] The Order authorized NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data regarding [redacted]

~~(TS//SI//NF)~~ On 10 July 2006, in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*, the NSA OIG issued "a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." This report was issued with the Office of the General Counsel's concurrence as mandated by the Order.

~~(TS//SI//NF)~~ The "*Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance*

Court Order: Telephony Business Records (ST-06-0018)," 5 September 2006, provided the details of the findings of the 10 July memorandum and made formal recommendations to management.

~~(TS//SI//NF)~~ Management controls governing the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order were adequate and in several aspects exceeded the terms of the Order. However, due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, the NSA OIG recommended three additional controls regarding collection procedures, reconciliation of audit logs, and segregation of duties.

~~(TS//SI//NF)~~ Collection Procedures

~~(TS//SI//NF)~~ During an OIG review of collection procedures, Program management discovered that NSA was obtaining [redacted] data that might not have been in keeping with the Order: [redacted] OGC advised that [redacted] data should have been suppressed from the incoming data flow. Immediately, management blocked the data from analysts' view. Further, working with the providers, Program management completed suppression of the suspect data on 11 October 2006 and agreed to implement additional procedures to prevent the collection of unauthorized data.

~~(TS//SI//NF)~~ Reconciliation of Audit Logs

~~(TS//SI//NF)~~ Management controls were not in place to verify that telephone numbers approved for querying were the only numbers queried. Although audit logs documented the queries of the archived metadata, the logs were not in a usable format, and Program management did not routinely use them to audit telephone numbers queried. Management concurred with the recommendation to conduct periodic reconciliations; however, action was contingent on the approval of a Program management request for two additional computer Programmers.

[redacted]

~~(C//NF)~~ Lack of Segregation of Duties

~~(C//NF)~~ The seven individuals with the authority to approve queries also had the ability to conduct queries under the Order. Standard internal control practices require that key duties and responsibilities be divided among different people to reduce the risk of error and fraud. Although Program management concurred with the finding, it could not implement the recommendation due to staffing and operational needs. As an alternative, Program management agreed to develop a process to monitor independently the queries of the seven individuals. This action plan was contingent on the development of usable audit logs recommended above.

(U//~~FOUO~~) Corrective action has been completed for one of the three recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

20 Dec 2006

~~(S//NF)~~ Summary of OIG Oversight 2001-2006 STELLARWIND Program Activities (ST-07-0011)

~~(S//NF)~~ On 20 December 2006, the OIG issued a report summarizing OIG's oversight of the STELLARWIND Program after five years of implementation.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

~~(TS//SI//NF)~~ Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using Pen Register and Trap and Trace Devices (ST-06-0020)

~~(TS//SI//NF)~~ On [redacted] the OIG reported that the management controls governing the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the FISC Order authorizing NSA to collect Internet metadata using PR/TT devices were adequate and in several aspects exceeded the terms of the Order. Due to the risk associated with the processing of electronic communications metadata involving U.S. person information, additional controls were needed for processing and monitoring queries made against PR/TT data, documenting

ST-09-0002 ~~*TOP SECRET//STLW//COMINT//ORCON/NOFORN*~~

oversight activities, and providing annual refresher training on the terms of the Order.

(U//~~FOUO~~) Corrective action has been completed for two of the six recommendations.

(U//~~FOUO~~) This report was sent to SSCI on [redacted] and HPSCI on [redacted]

5 Jul 2007 ***~~(TS//SI//NF)~~ Domestic Selector Tasking Justification Review (ST-07-0017)***

(U//~~FOUO~~) The OIG conducted this review to determine whether tasking justification statements were supported with intelligence information consistent with sources cited in the justifications. The OIG identified some justifications containing errors, but there was no pattern of errors or exaggeration of facts or intentional misstatements.

(U//~~FOUO~~) This report was sent to SSCI on 28 January 2008 and HPSCI on 28 January 2008.

30 June 2008 ***~~(TS//SI//NF)~~ Advisory Report on the Adequacy of STELLARWIND Decompartmentation Plans (ST-08-0018)***

~~(TS//SI//NF)~~ At the request of the SID Program Manager for CT Special Projects, the OIG assessed the adequacy of NSA's plans to remove data from the STELLARWIND compartment, as authorized by the Director of National Intelligence. On 30 June 2008, the OIG reported that NSA management had a solid foundation of planning for decompartmentation. In particular, the content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of successfully removing data from the STELLARWIND compartment, while complying with laws and authorities. Management was also diligent in assessing the scope and complexity of this undertaking. Although the OIG made no formal recommendations, it suggested improvements to develop more detailed plans, set firm milestones, and establish a feedback system to ensure that plans were successfully implemented.

(U//~~FOUO~~) This report was not sent to SSCI or HPSCI.

APPENDIX F

(U) Presidential Notifications

This page intentionally left blank.

(U) Presidential Notifications

~~(TS//STLW//SI//OC/NF)~~ Executive Orders 12333 and 12863 require intelligence agencies to report to the President, through the President's Intelligence Oversight Board, activities they have reason to believe may be unlawful or contrary to executive order or presidential directive. Knowing that Board members were not cleared, however, the NSA Director or Deputy Director reported the following violations of the Presidential Authorization and related authorities to the President through his Counsel, rather than through the Board. Each notification was approved if not actually drafted by OIG. Some of the notifications were not the subject of the OIG reviews or investigations discussed in Appendix E.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes violations regarding (1) the [redacted] and (2) [redacted]
[redacted]	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes a delay of about 90 days in detasking a telephone number [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes the investigation mentioned above regarding metadata collection violations that occurred under FISA Court Order *In Re* [redacted] FISA Court [redacted] The complete OIG report was issued [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes [redacted] instances in which cleared NSA analysts mistakenly accessed data [redacted] In one instance, a report based on such data went out, but it was not cancelled because the same information was available elsewhere. In the other [redacted] instances, no reports were issued. [redacted]

(U) Date	(U) Summary of Notification
	[redacted]
[redacted]	(~~TS//STLW//SI//OC/NF~~) Describes one instance of inadvertent collection of a call with both ends in the U.S. – a fact that could not have been known until it was listened to because [redacted] showed the call as having a foreign origin. [redacted]
[redacted]	(~~TS//SI//NF~~) Describes three incidents: The first involved a one-digit typo resulting in one incorrectly tasked number. The second involved a number improperly tasked for metadata analysis. The operator discovered it almost immediately and promptly removed it from tasking. The third involved [redacted] numbers that were not detasked in a timely fashion.
2 Aug 2005 [redacted]	(~~TS//SI//NF~~) Describes the evolving [redacted] a practice that may have resulted in over-collection. The notification refers to NSA's work in developing more rigorous [redacted]
[redacted]	(~~TS//STLW//SI//OC/NF~~) Describes an incident in which bulk telephony metadata was actively collected in spite [redacted] At that time NSA limited collection of bulk telephone records to [redacted] as permitted by statute. The collection resulted when [redacted] The error was not discovered for 18 months. (~~TS//STLW//SI//OC/NF~~) Although most of the metadata improperly collected was also properly acquired [redacted] pursuant to statute, the dataflow was terminated immediately upon discovery. Also, because the improperly collected metadata had been forwarded to non-STELLARWIND databases, the Agency removed non-compliant metadata from all affected databases, including those in which STELLARWIND data is normally stored.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which an [redacted] This resulted [redacted] of non-target data. The error was discovered within hours, when personnel responsible for monitoring [redacted] The error was corrected, and all inadvertently collected records were deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an instance where a [redacted] Although no reports were generated, and there was no evidence that U.S.-to-U.S. communications were collected, we could not certify that the files were all one-end foreign without reviewing [redacted] The [redacted] files were deleted, and procedures used by [redacted] were being reviewed. ~~(TS//STLW//SI//OC/NF)~~ A second incident was reported in which a typographical error resulted in contact chaining on a U.S. telephone number with no [redacted] affiliation. The telephone number was rechecked, and the error was corrected.

This page intentionally left blank.

APPENDIX G

(U) United States Signals Intelligence Directive SP0018, Legal Compliance and Minimization Procedures

This page intentionally left blank.

~~SECRET~~

AUTHORIZED REPRODUCTION NUMBER 00R0043

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES
SIGNALS INTELLIGENCE
DIRECTIVE
18

27 July 1993

INCLUDES CHANGES 1 and 2

See Letter of Promulgation for instructions on reproduction or release of this document.

~~OPR: D2~~
~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES ~~(FOUO)~~

LETTER OF PROMULGATION

(U) This USSID prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18, and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 19.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS, NSTS 963-3121 or [redacted]

J.M.McCONNELL
Vice Admiral, U.S. Navy
Director

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

USSID 18
27 July 1993

CHANGE REGISTER

No	Date	CHANGE Authority (Msg Cite/DTG, Hard Copy (HC))	ENTERED Date	By
1	28OCT97	HARDCOPY CHANGE	29OCT97	RS
2	11Dec98	P0211–0307–98, 111600Z Dec 98	11Dec98	WF
2	11Dec98	P0211–0309–98, 111640Z Dec 98 (correction to above)	11Dec98	WF

This page intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

27 July 1993

USSID 18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES (U)

SECTION 1 – PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

SECTION 2 – REFERENCES

2.1. (U) References

a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.

b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

SECTION 3 – POLICY

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS. The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

SECTION 4 – COLLECTION

4.1. ~~(S-CCO)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] will not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [redacted], or

(c) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(4) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) Technical devices (e.g. [redacted]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted] and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]:

(a) A non-U.S. PERSON located outside the UNITED STATES [redacted]

(b) [redacted]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process),

sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and abets a person engaging in such activities.

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. ~~(S-CCO)~~ [redacted]

a. [redacted]

b. [redacted]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

4.4. ~~(S-CCO)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that the DIRNSA/CHCSS is advised immediately and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [redacted]

b. If Attorney General approval is obtained, the COLLECTION may continue for the length of time specified in the approval.

c. If it is determined that [redacted] COLLECTION may continue at the discretion of the operational element.

d. If [redacted] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [redacted] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

4.5. ~~(C-CCO)~~ U.S. PERSON TARGETS Entering the UNITED STATES.

a. If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Attorney General approval described in Section 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. ~~(S-CCO)~~ Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [redacted], must be submitted through the DDO and the General Counsel to the DIRNSA/CHCSS for review.

4.7. ~~(C-CCO)~~ Direction Finding. Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for

communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5 – PROCESSING

5.1. ~~(S-CCO)~~ Use of Selection Terms During Processing.
When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located) [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the DDO or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(C-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. ~~(S-CCO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) Establish or maintain intercept, or

(b) Minimize unwanted intercept, or

(c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P02.

5.5. ~~(S-CCO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES [redacted] communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to

warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

SECTION 6 – RETENTION

6.1. ~~(S-CCO)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-CCO)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

SECTION 7 – DISSEMINATION

7.1. ~~(S-CCO)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P02.

7.2. ~~(S-CCO)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made

by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P02 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P02 should be in the form of a CRITICOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

7.3. ~~(S-CCO)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P02, the Deputy Chief, P02, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(1) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P02 within 24 hours of discovery of the error.

SECTION 8 – RESPONSIBILITIES

8.1. (U) Inspector General.
The Inspector General shall:

a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.

b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.

c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.

d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

8.2. (U) General Counsel. The General Counsel shall:

a. Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures should be sent by CRITICOMM to DDI XDI, or by NSA/CSS secure telephone 963-3121, or [redacted]

b. Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.

c. Advise the Inspector General in inspections and oversight of USSS activities.

d. Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, Inspector General or Key Components Chief, all new major requirements and internally generated USSS activities.

e. Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.

f. Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.

g. Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

8.3. (U) Deputy Director for Operations (DDO).
The DDO shall:

a. Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.

b. Apply the provisions of this USSID to all SIGINT production activities. The DDO staff focal point for USSID 18 matters is P02 (use CRITICOMM DDI XAO).

c. Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.

d. Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the General Counsel. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the General Counsel prior to acceptance or execution.

8.4. (U) All Elements of the USSS. All elements of the USSS shall:

a. Implement this directive upon receipt.

b. Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: P02.

c. Immediately inform the DDO of any tasking or instructions that appear to require actions at variance with this USSID.

d. Promptly report to the NSA Inspector General and consult with the NSA General Counsel on all activities that may raise a question of compliance with this USSID.

SECTION 9 – DEFINITIONS

9.1. ~~(S-CCO)~~ AGENT OF A FOREIGN POWER means:

a. Any person, other than a U.S. PERSON, who:

(1) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor; or

(2) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. Any person, including a U.S. PERSON, who:

(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

(2) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation therefor, for or on behalf of a FOREIGN POWER; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in those activities.

c. For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision,

absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

9.2. ~~(S)~~ COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.

9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

b. In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

9.8. ~~(S)~~ FOREIGN COMMUNICATION means a communication that has at least one COMMUNICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

9.10. (U) FOREIGN POWER means:

a. A foreign government or any component thereof, whether or not recognized by the UNITED STATES,

b. A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS,

c. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments,

d. A group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor,

e. A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or

f. An entity that is directed and controlled by a foreign government or governments.

9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. Appear to be intended:

(1) to intimidate or coerce a civilian population,

(2) to influence the policy of a government by intimidation or coercion, or

(3) to affect the conduct of a government by assassination or kidnapping, and

c. Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

9.14. ~~(C)~~ SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [redacted] telephone number, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

9.15. ~~(C)~~ SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the UNITED STATES exercises sovereignty.

9.18. ~~(C)~~ UNITED STATES PERSON:

a. A citizen of the UNITED STATES,

b. An alien lawfully admitted for permanent residence in the UNITED STATES,

c. Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or

d. CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

e. The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(4) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

(5) CORPORATIONS have the nationality of the nation-state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

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

No. OP 2008-0009

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

OFFICE OF THE INSPECTOR GENERAL

~~(S//NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

July 2, 2009

ROSLYN A. MAZER
INSPECTOR GENERAL

Copy No.

This page intentionally left blank.

(U) TABLE OF CONTENTS

This page intentionally left blank.

~~(S/NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

I. (U) EXECUTIVE SUMMARY

~~(TS//STLW//SI//OC/NF)~~ The Office of Inspector General (OIG), Office of the Director of National Intelligence (ODNI), was one of five Intelligence Community Inspectors General that conducted a review of their agency's participation in the President's Surveillance Program (hereafter "the Program"), a top secret National Security Agency (NSA) electronic surveillance activity undertaken at the direction of the President. The Program became operational on October 4, 2001, three weeks after the deadly terrorist attacks of September 11, 2001. The review examined the ODNI's involvement in the Program from the period beginning with the stand-up of the ODNI in April 2005 through the termination of the Program in January 2007.

~~(TS//STLW//SI//OC/NF)~~ The ODNI's primary role in the Program was the preparation of the threat assessments that summarized the al Qaeda terrorist threat to the United States and were used to support the periodic reauthorization of the Program. That role began in April 2005, shortly after the ODNI stand-up and contemporaneous with the arrival of General Michael Hayden as the first Principal Deputy Director of National Intelligence (PDDNI). Prior to his ODNI appointment, Hayden was Director of NSA. In April 2005, ODNI personnel in the National Counterterrorism Center (NCTC) began to prepare the first of 12 Program threat assessments. In coordination with the Department of Justice (DOJ), then Director of National Intelligence (DNI) John Negroponte or PDDNI Hayden approved 12 ODNI-prepared threat assessments over an 18-month period. Once approved by the DNI or PDDNI, the Program threat assessments were reviewed and approved by the Secretary of Defense, and were subsequently used by DOJ, NSA, and White House personnel in support of the Program reauthorization. In addition to the preparation of the threat assessments, we found that NCTC used Program information in producing analytical products that were distributed to senior IC community officials and analysts. [redacted]

~~(TS//STLW//SI//OC/NF)~~ During the review, we made several related findings and observations. We learned that the ODNI usage of Program-derived information in ODNI intelligence products was consistent with the standard rules and procedures for handling NSA intelligence. We learned that ODNI personnel were not involved in nominating specific targets for collection through the Program. While ODNI personnel were identified as having contact [redacted] regarding the Program, we found that those communications were limited in frequency and scope. We also found that the ODNI intelligence oversight components -- the Civil Liberties Protection Officer (CLPO), Office of General Counsel (OGC), and the OIG -- had little involvement in oversight of the Program and had limited opportunity to participate in Program oversight due to delays in ODNI oversight personnel being granted access to the

Program and temporary resource limitations attendant to the stand-up of the ODNI. Finally, we found that the 2008 amendments to Executive Order 12333 and the current ODNI staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

II. (U) INTRODUCTION

~~(TS//STLW//SI//OC/NF)~~ *The Foreign Intelligence Surveillance Act Amendments Act of 2008*, Pub L. No. 110-261, 122 Stat. 2438 (hereafter "FISA Amendments Act") required the IGs of the DOJ, ODNI, NSA, Department of Defenses (DOD), and any other element of the intelligence community that participated in the President's Surveillance Program to conduct a comprehensive review of the Program.[1] The FISA Amendments Act defined the "President's Surveillance Program" as the "intelligence activity involving communications authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005." In response to this tasking, the IGs of the following five agencies were identified as having a role in Program review: DOJ, ODNI, NSA, DOD, and the Central Intelligence Agency (CIA).

~~(S//NF)~~ The participating IGs organized the review in a manner where each OIG conducted a review of its own agency's involvement in the Program. CIA IG John Helgerson was initially designated by the IGs to coordinate the review and oversee the preparation of an interim report due within 60 days after the enactment of the Act, and a later final report due not later than 1 year after the enactment of the Act.[2] Because of IG Helgerson's recent retirement, DOJ IG Glenn Fine was selected to coordinate the preparation of the final report. This report contains the results of the ODNI OIG review.

III. (U) SCOPE AND METHODOLOGY

~~(TS//STLW//SI//OC/NF)~~ We sought to identify the role of the ODNI in implementing the Program beginning with the stand-up of the ODNI in April 2005 through the Program's termination in January 2007. This review examined the:

A. Role of the ODNI and its component the National Counterterrorism Center (NCTC) in drafting and coordinating the threat assessments that supported the periodic reauthorization of the Program;

---

[1] ~~(S//NF)~~ The Program is also known within the Intelligence Community by the cover term STELLARWIND. The Program is a Top Secret/Sensitive Compartmented Information (SCI) program.

[2] (U) The participating IGs submitted an interim report, dated September 10, 2008, to the Chairman and Ranking member of the Senate Select Committee on Intelligence (SSCI) and a revised interim report, dated November 24, 2008, to the Chairman and Ranking member of the House of Representatives Permanent Select Committee on Intelligence (HPSCI).

B. NCTC's use of Program information to support counterterrorism analysis;

C. NCTC's role in identifying Program targets and tasking Program collection;

D. [redacted] and

F. Role of the ODNI in providing compliance oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ During the review, we interviewed 23 current or former ODNI officials and employees involved in the Program. The ODNI personnel we interviewed were cooperative and helpful. Our interviews included the following ODNI senior officials:

John Negroponte, former Director of National Intelligence
Michael McConnell, former Director of National Intelligence
Michael V. Hayden, former Principal Deputy Director of National Intelligence
Ronald Burgess, former Acting Principal Deputy Director of National Intelligence
David R. Shedd, Deputy Director of National Intelligence for Policy, Plans, and Requirements
Alexander W. Joel, Civil Liberties Protection Officer
Edward Maguire, former Inspector General
Benjamin Powell, former General Counsel
Corin Stone, Deputy General Counsel and Acting General Counsel
Joel Brenner, former National Counterintelligence Executive[3]
John Scott Redd, former NCTC Director
Michael Leiter, NCTC Director

~~(S//NF)~~ In addition to the interviews noted above, we reviewed Program-related documents made available by the NSA OIG, the DOJ OIG, and the ODNI OGC.

IV. (U) DISCUSSION OF FINDINGS

~~(TS//STLW//SI//OC/NF)~~ The following discussion contains our findings regarding the topics identified above. First, we briefly describe the terrorist attacks of September 11, 2001, and the initial government response to the attacks, including the authorization of the President's Surveillance Program. Next, we discuss the ODNI and NCTC role in implementing the Program. Finally, we set forth our conclusions and observations.

A. (U) Initial Response by the President and Congress to the Terrorist Attacks of September 11, 2001

(U) The devastating al Qaeda terrorist attacks against the United States quickly triggered an unprecedented military and intelligence community response to protect the

[3] (U) Brenner was the NSA Inspector General before joining the ODNI.

country from additional attacks. The following quote describes the initial terrorist attacks and the intended al Qaeda goal to deliver a decapitating strike against our political institutions.

> (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial airliners, each carefully selected to be fully loaded with jet fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States – to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths – the highest single-day death toll from hostile foreign attacks in the Nation's history.[4]

(U) On September 14, 2001, in response to the attacks, the President issued a *Declaration of National Emergency by Reason of Certain Terrorist Attacks* stating that "(a) national emergency exists by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and continuing immediate threat of further attacks on the United States."[5]

(U) On September 18, 2001, by an overwhelming majority in both the Senate and House of Representatives, a joint resolution was passed that authorized the use of United States military force against those responsible for the terrorist attacks launched against the United States. The joint resolution, also known as the *Authorization for Use of Military Force (AUMF)*, is often cited by White House and DOJ officials as one of the principal legal authorities upon which the Program is based. In relevant part, the AUMF provides:[6]

> (a) IN GENERAL – That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organization or persons, in order to

---

[4] (U) This summary of the events of September 11, 2001, was prepared by DOJ personnel and is set forth in the unclassified DOJ "White Paper" entitled *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, dated January 19, 2006.

[5] (U) Proclamation 7463, 66 Fed. Reg. No. 181, September 14, 2001.

[6] (U) *Authorization for Use of Military Force*, Section 2(a), Pub. L. No. 170-40, 115 Stat. 224, September 18, 2001.

prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

~~(TS//STLW//SI//OC/NF)~~ On October 4, 2001, three days before the start of overt military action against the al Qaeda and Taliban terrorist camps, the President authorized the Secretary of Defense to implement the President's Surveillance Program.[7] The Program, a closely held top-secret NSA electronic surveillance project, authorized the Secretary of Defense to employ within the United States the capabilities of the DOD, including but not limited to the signals intelligence capabilities of the NSA, to collect international terrorism-related foreign intelligence information under certain specified circumstances. Each Program reauthorization was supported by a written threat assessment, approved by a senior Intelligence Community official, that described the threat of a terrorist attack against the United States.

(U) On October 7, 2001, in a national television broadcast, the President announced the start of military operations against al Qaeda and Taliban terrorist camps in Afghanistan.[8]

~~(TS//STLW//SI//OC/NF)~~ On April 22, 2005, the ODNI began operations as the newest member of the Intelligence Community. The ODNI was created, in part, in response to the findings of the *Independent National Commission on Terrorist Attacks Upon the United States* (hereafter 9/11 Commission) that recommended the creation of a national "Director of National Intelligence" to oversee and coordinate the planning, policy, and budgets of the Intelligence Community.[9] In late April 2005, ODNI personnel began to prepare the threat assessments used in the periodic reauthorization of the Program. In June 2005, ODNI officials began to approve the threat assessments.

B. ~~(TS//STLW//SI//OC/NF)~~ ODNI Role in Preparing Threat Assessments in Support of the Program Reauthorizations

~~(TS//STLW//SI//OC/NF)~~ Prior to the ODNI's involvement in the Program, the Program was periodically reauthorized approximately every 30 to 45 days pursuant to a reauthorization process overseen by DOJ, NSA, and White House personnel. Each reauthorization relied, in part, on a written threat assessment approved by a senior Intelligence Community official that described the current threat of a terrorist attack against the United States and contained the approving official's recommendation regarding the need to reauthorize the Program. Before the ODNI's involvement in the

---

[7] ~~(TS//STLW//SI//OC/NF)~~ The NSA materials we reviewed identified October 4, 2001, as the date of the first Program authorization.

[8] (U) The CNN.com webpage article entitled *President announces opening of attack*, dated, October 7, 2001, provides a summary of the President's announcement and describes the national television broadcast.

[9] (U) While the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) that created the ODNI was signed by the President on December 17, 2004, the actual ODNI stand-up occurred months later. The official ODNI history, *A Brief History of the ODNI's Founding*, sets April 22, 2005, as the date when the ODNI commenced operations.

Program, every threat assessment prepared by the Intelligence Community in support of the Program reauthorization identified the threat of a terrorist attack against the United States and recommended that the Program be reauthorized. Accordingly, the Program was regularly reauthorized during the approximately 3-year period prior to the involvement of the ODNI. During that period, the Director of Central Intelligence or his designee approved 31 threat assessments in support of the reauthorization of the Program.

~~(TS//STLW//SI//OC/NF)~~ In reviewing the circumstances that led to the decision to transfer responsibility for preparing the Program threat assessments to the ODNI, we found that the ODNI does not have identifiable records regarding that decision. Senior ODNI officials involved with the Program told us that after the merger of the Terrorist Threat Integration Center (TTIC) into the NCTC, and the later incorporation of NCTC into the ODNI, it made sense for the ODNI to take responsibility for preparing the Program threat assessments as both TTIC and NCTC previously handled that task. Former PDDNI Hayden told us that the primary reason that the ODNI become involved in the Program was the statutory creation of the new DNI position as the senior Intelligence Community advisor to the President. When Ambassador Negroponte was confirmed as the first DNI, Hayden and other senior intelligence officials believed that DNI Negroponte, as the President's new senior intelligence advisor, should make the Intelligence Community's recommendation to the President regarding the need to renew the Program. Hayden commented that the new DNI's involvement in this important intelligence program enhanced the DNI's role as the leader of the Intelligence Community and gave immediate credibility to the ODNI as a new intelligence agency.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI became involved in the Program, the preparation and approval of the threat assessments became the ODNI's primary Program role.[10] Beginning in April 2005, and continuing at about 30 to 45 day intervals until the Program's termination in January 2007, ODNI personnel prepared and approved 12 written threat assessments in support of the periodic reauthorization of the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel who prepared the documents following an established DOJ format used in earlier Program reauthorizations. NCTC analysts prepared the threat assessments in a memorandum format, usually 12 to 14 pages in length. Senior ODNI and NCTC officials told us that each threat assessment was intended to set forth the ODNI's view regarding the current threat of an al Qaeda attack against the United States and to provide the DNI's recommendation whether to continue the Program. NCTC personnel involved in preparing the threat assessments told us that the danger of a terrorist attack described in the threat assessments was sobering and "scary," resulting in the threat assessments becoming known by ODNI and Intelligence Community personnel involved in the Program as the "scary memos."

---

[10] ~~(TS//STLW//SI//OC/NF)~~ The joint interim report prepared by the participating IGs notified congressional oversight committees that the review would examine the ODNI's involvement in preparing "threat assessments and legal certifications" submitted in support of the Program. Because we did not identify any ODNI officials executing a legal certification, we treated our review of the legal certifications to be the same as the review of the threat assessments. The Attorney General made legal certifications in support of the Program that are addressed in the DOJ OIG report.

~~(TS//STLW//SI//OC/NF)~~ During interviews, ODNI personnel said they were aware that the threat assessments were relied upon by DOJ and the White House as the basis for continuing the Program and further understood that if a threat assessment identified a threat against the United States, the Program was likely to be reauthorized. NCTC analysts also said that on a less frequent basis they prepared a related document that set forth a list of al Qaeda-affiliated groups that they understood were targets of the Program. Both the threat assessments and the less frequent list of al Qaeda-affiliated groups underwent the same ODNI approval process.

~~(TS//STLW//SI//OC/NF)~~ We examined the ODNI process for preparing the Program documents, particularly the threat assessments, and found that the documents were drafted by experienced NCTC analysts under the supervision of the NCTC Director and his management staff, who were ultimately responsible for the accuracy of the information in the documents. We determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide-variety of Intelligence Community sources. ODNI personnel told us that during the period when the ODNI prepared the threat assessments, the Intelligence Community had access to fully evaluated intelligence that readily supported the ODNI assessments that al Qaeda terrorists remained a significant threat to the United States.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI threat assessments were approved within NCTC and by the NCTC Director, the documents were forwarded through an established approval chain to senior ODNI personnel who independently satisfied themselves that the documents were accurate, properly prepared, and in the appropriate format. Throughout the ODNI preparation and approval process, the threat assessments were also subject to varying degrees of review and comment by DOJ and OGC attorneys, including then General Counsel Benjamin Powell and Deputy General Counsel Corin Stone. Powell said his review of the threat assessments was not a legal review, but was focused on spotting issues that might merit further review or analysis. Powell said he relied on DOJ to conduct the legal review. Once the draft threat assessments were subjected to this systematic and multi-layered management and legal review, the documents were provided to the DNI or PDDNI for consideration and, if appropriate, approval. Overall, we found the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI or PDDNI approval.

~~(TS//STLW//SI//OC/NF)~~ Negroponte told us that because of time-sensitive issues present in 2005 relating to the ongoing ODNI start-up as a new agency and other Intelligence Community matters requiring his attention, he tasked his deputy, then PDDNI Hayden, to oversee the ODNI approval of the threat assessments and related documents. Negroponte told us that when making this decision, he was aware of Hayden's prior experience with the Program during Hayden's earlier assignment as Director of NSA. In June 2005, shortly after his arrival at ODNI, Hayden received and approved the first ODNI threat assessment. Hayden later approved the next six ODNI threat assessments. After Hayden left the ODNI in May 2006 to become Director of CIA, Negroponte approved the next five ODNI threat assessments, including a December

2006 threat assessment used in the final reauthorization of the Program. In total, Negroponte and Hayden approved 12 ODNI threat assessments prepared in support of the Program reauthorizations.[11]

~~(TS//STLW//SI//OC/NF)~~ In discussing the ODNI process used to prepare and approve the threat assessments, Negroponte told us he was "extremely satisfied" with the quality and content of the threat assessments provided for his approval. He did not recall any inaccuracies or problems relating to preparation of the ODNI threat assessments. Negroponte said the al Qaeda threat information described in the Program threat assessments was consistent with the terrorism threat information found in *The President's Daily Briefing* and other senior-level Intelligence Community products he had read. Hayden had a similar view. Negroponte and Hayden separately told us that when they approved the threat assessments, credible intelligence was readily available to the Intelligence Community that demonstrated the ongoing and dangerous al Qaeda terrorist threat to the United States. Similarly, Negroponte and Hayden each told us that the nature and scope of the al Qaeda terrorist threat to the United States was well documented and easily supported the ODNI threat assessments used in the Program reauthorizations.

~~(TS//STLW//SI//OC/NF)~~ Because of questions raised in the media about the legal basis for the Program, we asked the ODNI personnel involved in the preparation or approval of the threat assessments about their concerns, if any, regarding the legal basis for the Program. We found that ODNI personnel involved in the Program generally understood that the Program had been in operation for several years and was approved by senior Intelligence Community and DOJ officials. During our interviews, ODNI officials told us they were satisfied with the legal basis for the Program, primarily because of their knowledge that the Attorney General and senior DOJ attorneys had personally approved the Program and remained directly involved in the Program reauthorization process. We did not identify any ODNI personnel who believed that the program was unlawful.

~~(TS//STLW//SI//OC/NF)~~ Former ODNI General Counsel Powell told us that after his Program briefings in early 2006, he had questions regarding the DOJ description of the legal authority for the Program but lacked the time to conduct his own legal review of the issue given the many time-sensitive ODNI legal issues that required his attention. Powell said he understood the rationale of DOJ's legal opinion that the Program was lawful and described the DOJ opinion as a "deeply complex issue" with "legal scholarship on both sides." Powell said he recognized that he was a latecomer to a complex legal issue that was previously and continuously approved by DOJ, personally supported by the Attorney General, and was being transitioned to judicial oversight – an idea he strongly supported. Powell said he relied on the DOJ legal opinion regarding the Program and directed his efforts to supporting the Program's transition to judicial oversight under traditional FISA, the 2007 Protect America Act, and the subsequent FISA Amendments Act of 2008.

[11] ~~(TS//STLW//SI//OC/NF)~~ The DNI and PDDNI together approved 12 of the 43 threat assessments used in support of the Program reauthorizations. CIA officials approved the other 31 threat assessments.

~~(TS//STLW//SI//OC/NF)~~ Negroponte recalled having regular contact with senior NSA and DOJ officials who raised no legal concerns to him about the Program. He said he remembered attending a Program-related meeting that included members of the FISA Court who did not raise any legal concerns to him about the authority for the Program and seemed generally supportive of the Program. Negroponte also recalled attending meetings in which the Program was briefed to congressional leadership who not did raise legal concerns to him. Overall, the direct involvement of DOJ and other senior Intelligence Community officials in the Program resulted in Negroponte and other ODNI personnel having few, if any, concerns about the legal basis for the Program.

C. ~~(TS//STLW//SI//OC/NF)~~ NCTC Use of Program Information to Support Counterterrorism Analysis

~~(TS//STLW//SI//OC/NF)~~ The Program information was closely held within the ODNI and was made available to no more than 15 NCTC analysts for review and, if appropriate, use in preparing NCTC analytical products.[12] Generally, the NCTC analysts approved for access received the Program information in the form of finished NSA intelligence products. [redacted] The NCTC analysts said the Program information was subject to stringent security protections [redacted] The NCTC analysts told us they received training regarding proper handling of NSA intelligence. They said they handled the NSA intelligence, including Program information, consistent with the standard rules and procedures for handling NSA intelligence information, including the minimization of U.S. person identities.

~~(TS//STLW//SI//OC/NF)~~ Hayden told us that during his tenure as Director of NSA, he sought to disseminate as much Program information as possible to the Intelligence Community [redacted]

~~(TS//STLW//SI//OC/NF)~~ During our review, NCTC analysts told us they often did not know if the NSA intelligence available to them was derived from the Program. [redacted]

[12] ~~(TS//STLW//SI//OC/NF)~~ The number of NCTC analysts read into the Program ranged from 5 to 15 analysts.

[redacted] On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the Program, the analysts said they reviewed the Program information in the same manner as other NSA intelligence products and, if appropriate, incorporated the Program information into analytical products being prepared for the 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 Program information.

~~(TS//STLW//SI//OC/NF)~~ NCTC analysts with Program access said they had broad access to a wide variety of high quality and fully evaluated terrorism related intelligence. In particular, NCTC analysts told us that by virtue of their NCTC assignments, they had access to some of the most sensitive and valuable terrorism intelligence available to the Intelligence Community. NCTC analysts characterized the Program information as being a useful tool, but also noted that the Program information was only one of several valuable sources of information available to them from numerous collection sources and methods. During interviews, NCTC analysts and other ODNI personnel described the Program information as "one tool in the tool box," "one arrow in the quiver," or in other similar phrases to connote that the Program information was not of greater value than other sources of intelligence. The NCTC analysts we interviewed said they could not identify specific examples where the Program information provided what they considered time-sensitive or actionable intelligence, but they generally recalled attending meetings in which the benefits of the Program were discussed. [redacted] The NCTC analysts uniformly told us that during the period when NCTC prepared the threat assessment memoranda, the intelligence demonstrating the al Qaeda threat to the United States was overwhelming and readily available to the Intelligence Community.

~~(TS//STLW//SI//OC/NF)~~ When asked about the value of the Program, Hayden said "without the Program as a skirmish line you wouldn't know what you don't know." He explained that by using the Program to look at a "quadrant of communications" the Intelligence Community was able to assess the threat arising from those communications, which allowed Intelligence Community leaders to make valuable judgments regarding the allocation of national security resources. He said looking at the terrorist threat in this manner was similar to soldiers on a combat patrol who look in all directions for the threat and assign resources based on what they learn. Hayden said that NSA General Counsel Vito Potenza often described the Program as an "early warning system" for terrorist threats, which Hayden thought was an accurate description of the Program. Hayden told us the Program was extremely valuable in protecting the United States from an al Qaeda terrorist attack. Hayden cited [redacted]

[redacted] as examples where the Program information was effectively used to disrupt al Qaeda operatives.[13]

D. [redacted]

[redacted]

[redacted]

[redacted]

E. ~~(TS//STLW//SI//OC/NF)~~ No NCTC Role in Identifying Program Targets and Tasking Collection

~~(TS//STLW//SI//OC/NF)~~ We did not identify any information that indicated that ODNI or NCTC personnel were involved in identifying or nominating targets for collection within the Program. ODNI personnel told us that ODNI and NCTC are non-operational elements of the Intelligence Community and were not involved in nominating targets for Program collection.

F. ~~(S/NF)~~ ODNI Oversight of the Program

~~(TS//STLW//SI//OC/NF)~~ We examined the role of the ODNI oversight components -- CLPO, OIG, and OGC -- in providing compliance oversight for the Program. We found that while the Program was subject to oversight by the NSA OIG, the ODNI oversight components had a limited role in providing oversight for the Program. During the review, we learned that within the first year of the Program, then NSA Director Hayden obtained White House approval allowing the NSA IG and designated NSA OIG officials to be read into the Program to provide compliance oversight for the Program. In furtherance of the NSA oversight program, the NSA IG provided compliance reports and briefings to the NSA Director, NSA General Counsel, and cleared White House personnel, including the Counsel to the President.[16]

~~(TS//STLW//SI//OC/NF)~~ In reviewing the ODNI oversight role regarding the Program, we found that the ODNI oversight components had limited involvement in oversight of the Program. We found that the opportunity for the ODNI to participate in Program oversight was limited by the fact that ODNI oversight personnel were not

[redacted]

[15] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[16] ~~(S//NF)~~ According to the General Counsel to the President's Intelligence Oversight Board (IOB), the IOB members and staff were not read into the Program and did not receive compliance reports from the NSA IG.

granted timely access to the Program by the White House personnel responsible for approving access. In addition, we found that the newly formed ODNI oversight offices were in varying stages of agency stand-up and lacked the necessary experienced staff and resources to effectively participate in oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ For example, General Counsel Powell received Program access after his arrival in January 2006, but his predecessor, then Acting General Counsel Corin Stone, was not read into the Program until a few days before Powell in January 2006, several months after the Program became operational within ODNI and only after she had read about the Program in a December 2005 newspaper article.[17] Similarly, CLPO Alexander Joel, who is responsible for reviewing the privacy and civil liberties implications of intelligence activities, requested but did not receive Program access until October 2006, shortly before the Program terminated.[18] Joel told us that Negroponte and Hayden supported his request for Program access, but White House staff delayed approval for several months. Joel said that while waiting for approval of his Program access, Hayden gave him some insight about the Program that did not require the disclosure of compartmented information. Joel found this information helpful in planning his later review. Finally, then ODNI Inspector General Edward Maguire and his oversight staff did not obtain Program access until 2008, long after the Program had terminated.[19]

~~(TS//STLW//SI//OC/NF)~~ Once read into the Program, Powell and Joel were provided with reasonable access to NSA compliance reports and briefings relating to the NSA OIG oversight program. Powell told us that he was satisfied that the NSA IG provided a reasonable degree of Program oversight. Similarly, Joel said he believed that he had received full disclosure regarding the NSA oversight program and found the NSA oversight effort to be reasonable.

~~(TS//STLW//SI//OC/NF)~~ We also learned that the members of the President's Privacy and Civil Liberties Oversight Board (PCLOB) reviewed the Program, in part, in association with Joel.[20] The PCLOB review was contemporaneous with Joel's review

---

[17] (U//~~FOUO~~) Powell was appointed General Counsel in January 2006 and served in that position as a recess appointment until his Senate confirmation in April 2006. Prior to his appointment, Powell was an Associate Counsel to the President and Special Assistant to the President where he worked on initiatives related to the Intelligence Community. However, Powell was not read into the Program while serving at the White House.

[18] (U//~~FOUO~~) Joel is the Civil Liberties Protection Officer (CLPO) with the responsibility for ensuring that the protection of privacy and civil liberties is incorporated in the policies and procedures of the Intelligence Community. The CLPO responsibilities are set forth in the Section 103d of *Intelligence Reform and Terrorism Prevention Act of 2004.*

[19] ~~(S//NF)~~ While OIG personnel were not read into the Program until 2008, OIG officials were alerted to the existence of the NSA collection program through a December 2005 newspaper report. Shortly after that report, the NSA IG told ODNI OIG officials that the NSA OIG was conducting oversight of that NSA program. PDDNI Hayden also told IG Maguire that the NSA program was subject to NSA OIG oversight.

[20] (U) The PCLOB was created by the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, which requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism (P.L. 108-458, 2004).

and resulted in an independent and generally favorable finding regarding the NSA implementation of the Program. After the PCLOB review, a PCLOB board member published an editorial article, in part, quoted below, that summarized his observations regarding the NSA effort in implementing the Program.

> There were times, including when the Board was "read into" and given complete access to the operation of the Terrorist Surveillance Program that I wondered whether the individuals doing this difficult job on behalf of all of us were not being too careful, too concerned, about going over the privacy and liberties lines – so concerned, with so many internal checks and balances, that they could miss catching or preventing the bad guys from another attack. And I remember walking out of these briefing sessions in some dark and super-secret agency with the thought: I wish the American people could meet these people and observe what they are doing.[21]

~~(S//NF)~~ In sum, the ODNI oversight components had limited and belated involvement in the oversight of the Program. However, once read into the Program, Powell and Joel determined that the Program was subject to reasonable oversight by the NSA OIG. Moreover, the initial White House delay in granting ODNI oversight personnel access to the Program occurred prior to the 2008 revision to Executive Order (EO) 12333, which expressly grants ODNI oversight components broad access to any information necessary to performing their oversight duties. In particular, EO 12333 provides in relevant part that:

> Section 1.6 *Heads of Elements of the Intelligence Community*. The heads of elements of the Intelligence Community shall:
>
> (h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy and civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their duties.

~~(TS//STLW//SI//OC/NF)~~ EO 12333, as amended, clarifies and strengthens the ODNI's ability to provide compliance oversight. In light of the recent change to EO 12333, and with current staffing, we believe that ODNI's oversight components have sufficient resources and authority to perform their responsibilities to conduct oversight of closely held intelligence activities, assuming timely notification.

---

[21] (U) The quote is taken from a May 5, 2007, article by former PCLOB member Lanny Davis, entitled, "*Why I Resigned From The President's Privacy and Civil Liberties Oversight Board – And Where We Go From Here.*" The article was published on webpage of The Huffington Post, www.huffingtonpost.com.

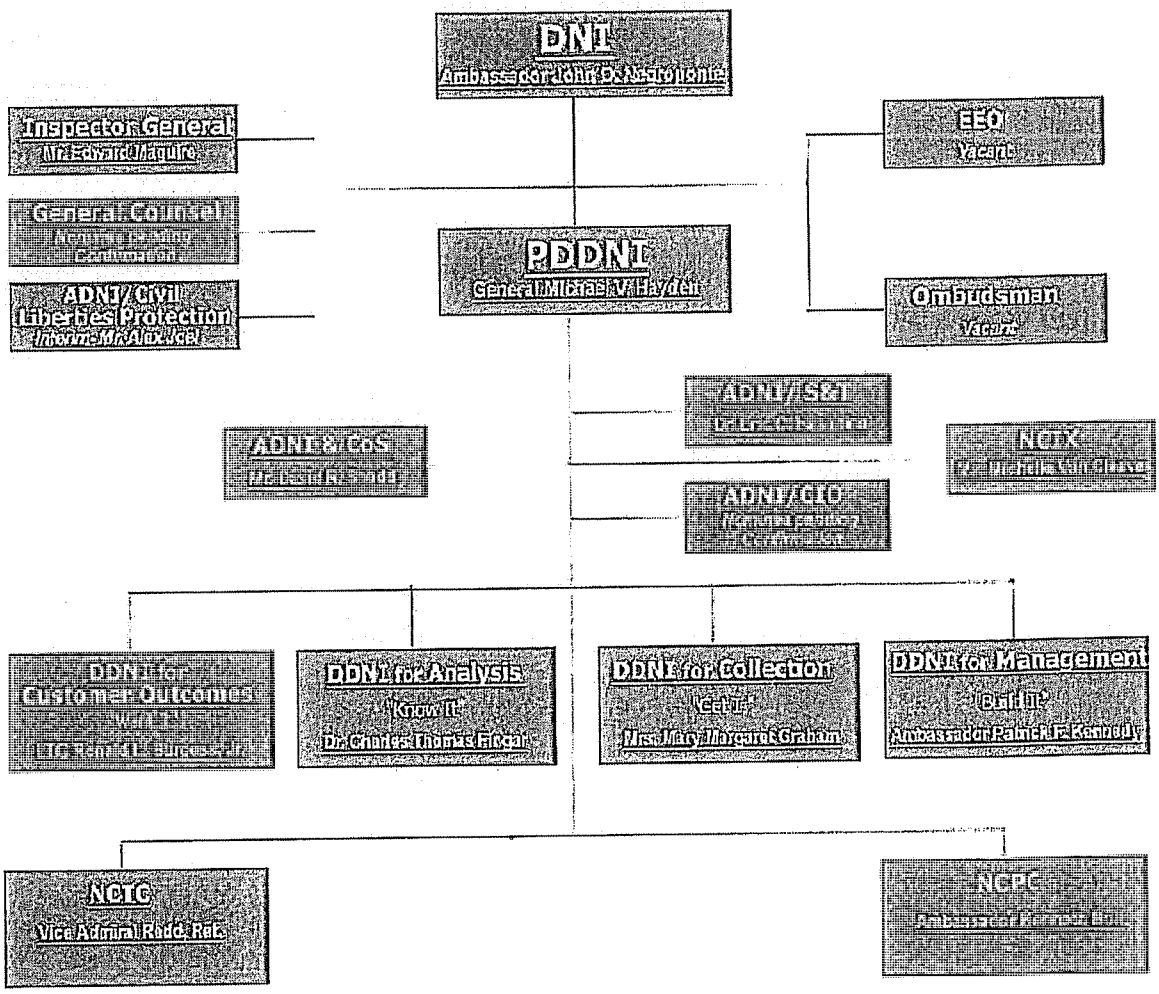
V. (U) CONCLUSION

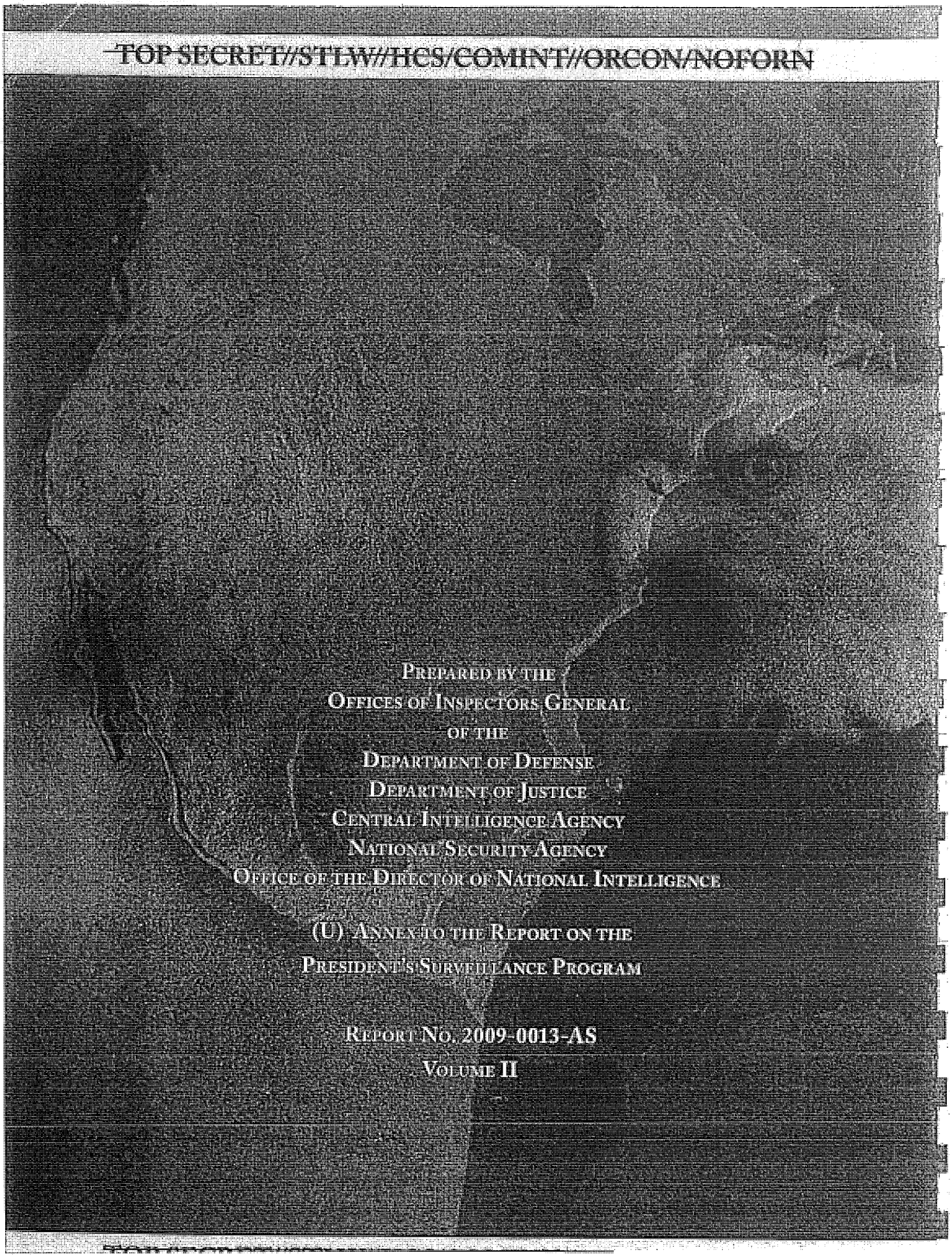
~~(TS//STLW//SI//OC/NF)~~ We found that the ODNI's primary role in the Program was the preparation of 12 ODNI threat assessments approved by the DNI or PDDNI for use in the Program reauthorizations. The ODNI-prepared threat assessments set forth the ODNI's view regarding the existing threat of an al Qaeda terrorist attack against the United States and provided the DNI's recommendation regarding the need to reauthorize the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel under the supervision of knowledgeable NCTC supervisors. We noted that the threat assessments were subject to review by OGC and DOJ attorneys before approval. Additionally, we found that the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI approval. Overall, we found the ODNI process for the preparation and approval of the threat assessments was responsible and effective.

~~(TS//STLW//SI//OC/NF)~~ We also found that the ODNI oversight components played a limited role in oversight of the Program. The limited ODNI oversight role was due to delays in obtaining Program access for ODNI oversight personnel and to temporary resource limitations related to the stand-up of the agency. However, we believe that the 2008 amendments to EO 12333 and improved staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

This page intentionally left blank.

VI. (U) APPENDIX - STRUCTURE OF THE ODNI – 2005





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) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS

VOLUME II

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