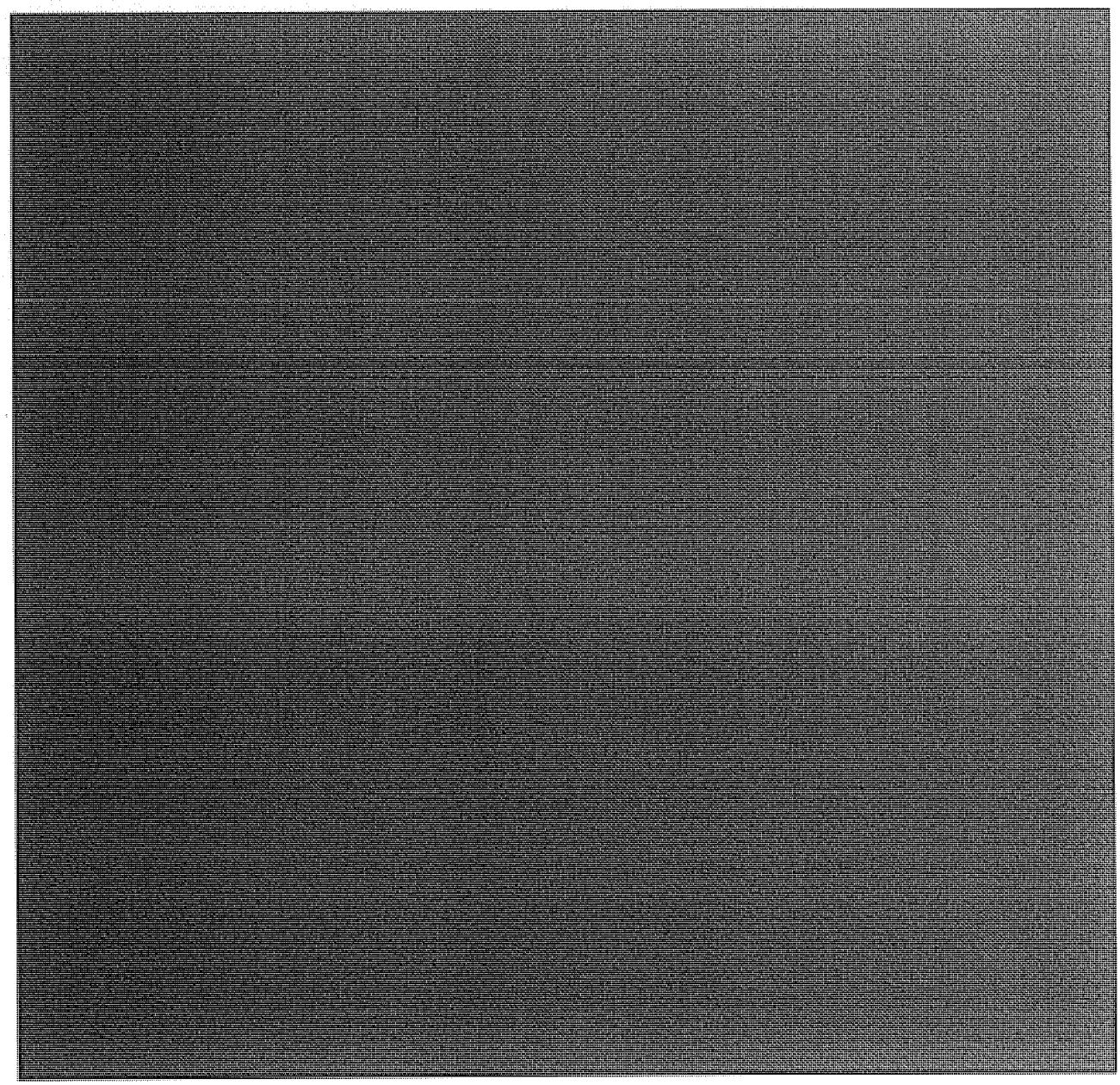
~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~



~~(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]

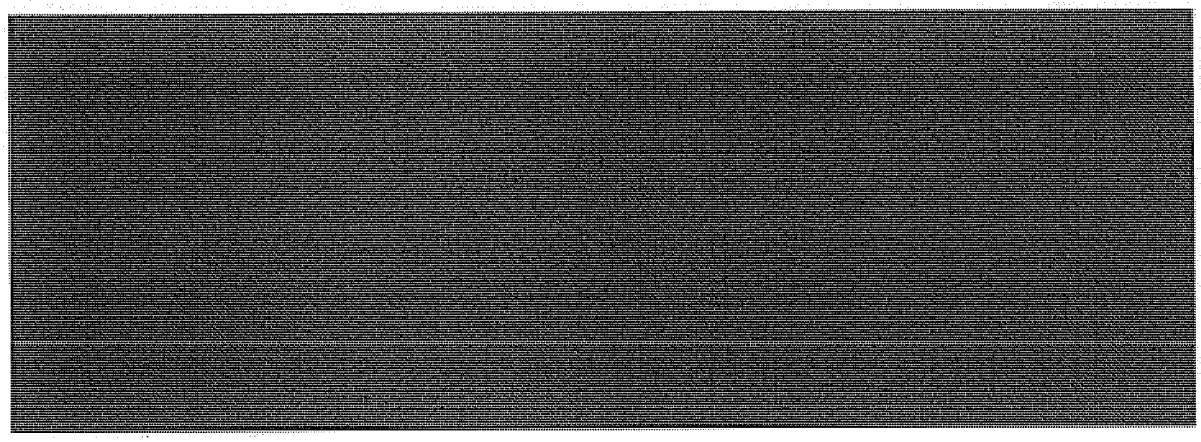
~~(S//NF)~~ [redacted] officials also told us that working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that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

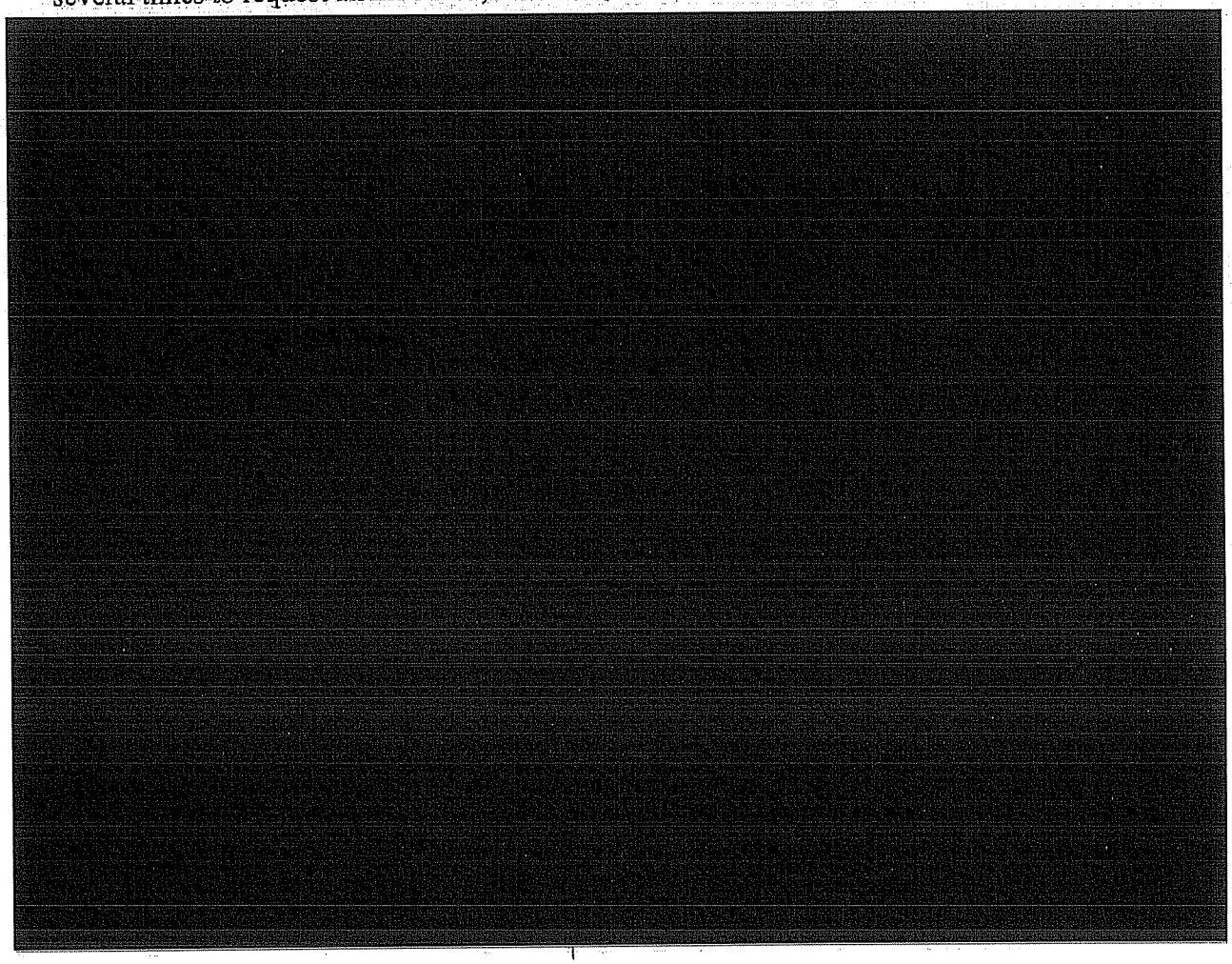
This page intentionally left blank.

~~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.

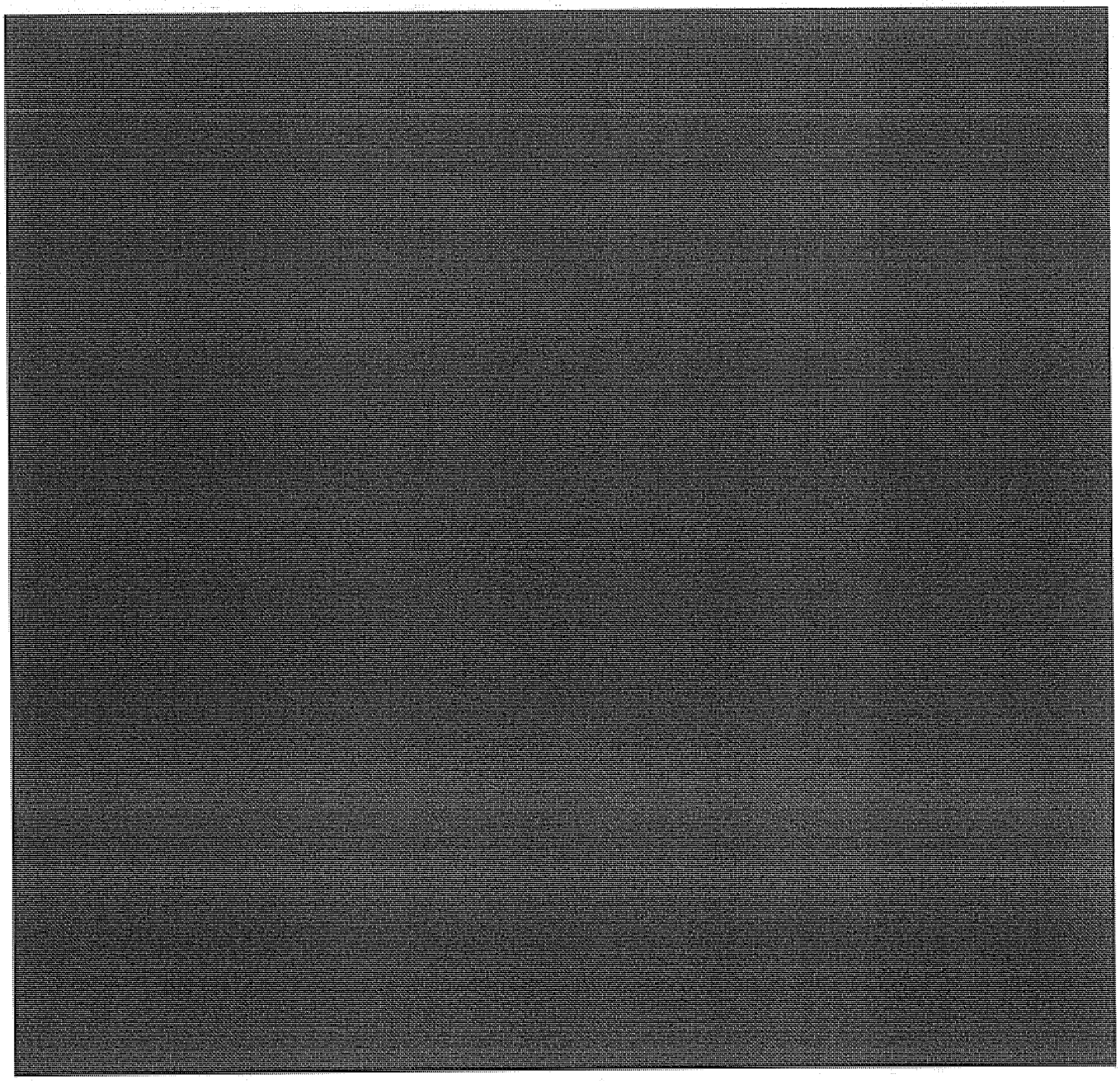
~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

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.

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~~

(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]

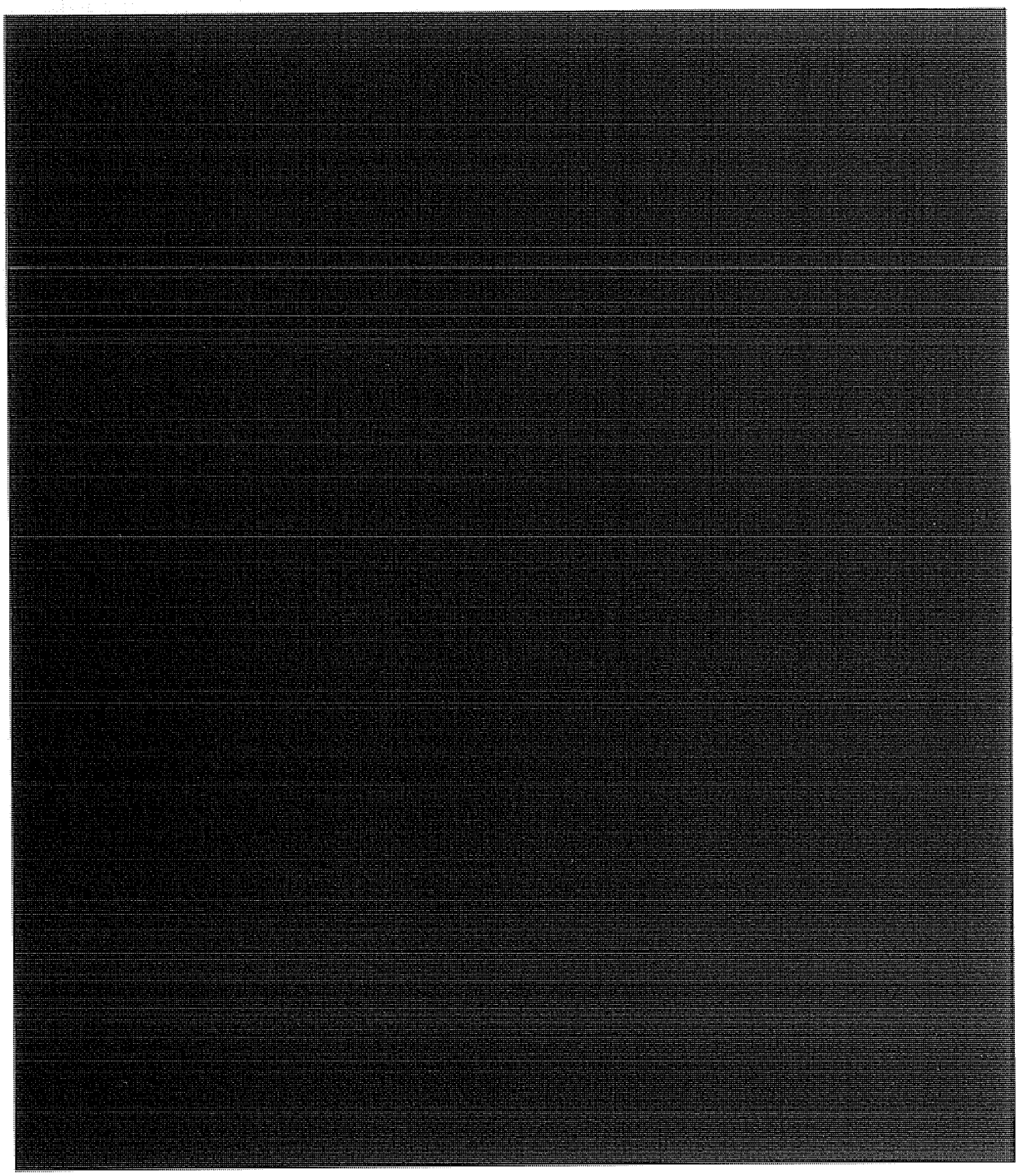
- **(U) NSA-FISC interaction and transition to court orders**

~~(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.

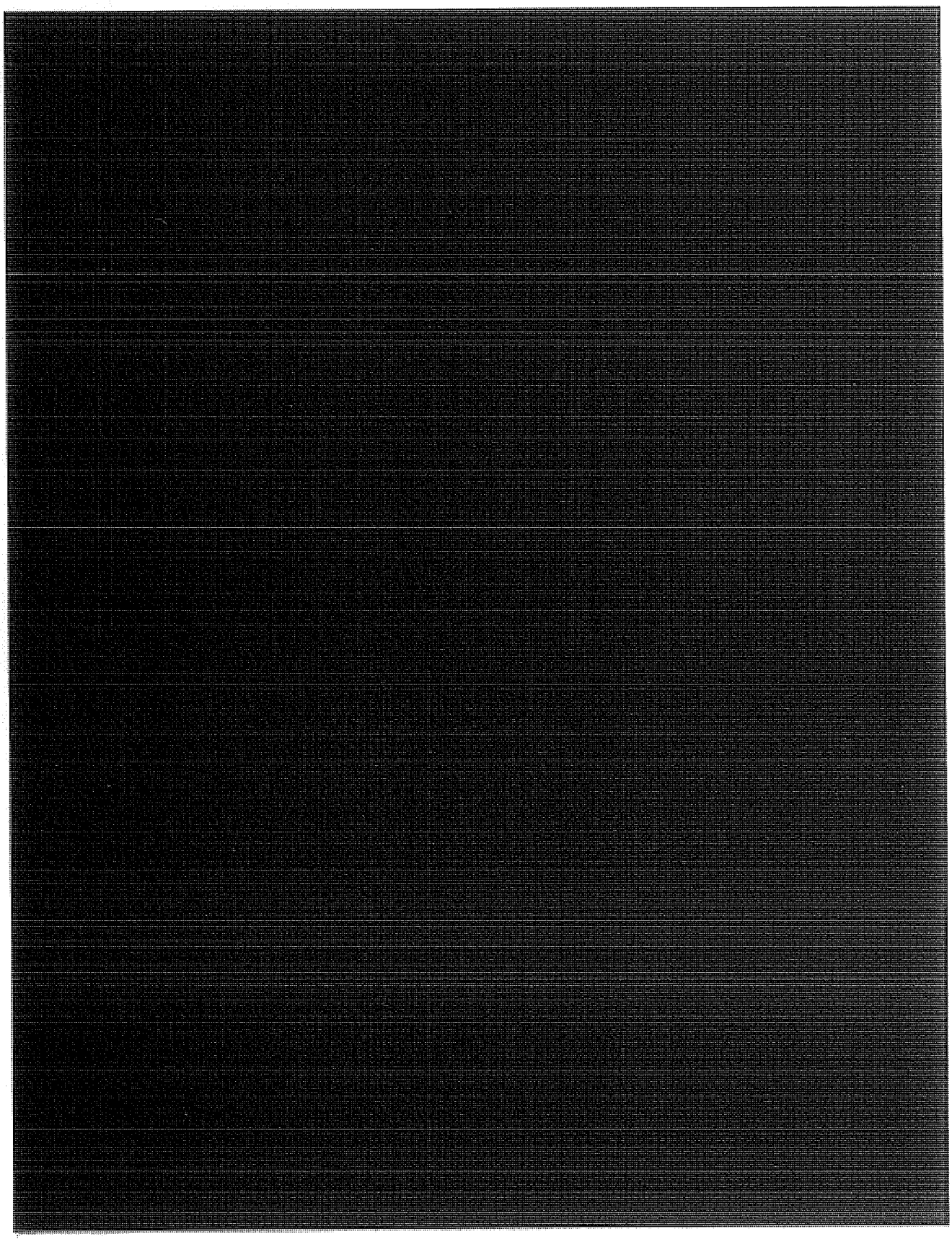
- **(U) Program oversight at NSA**

~~(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.

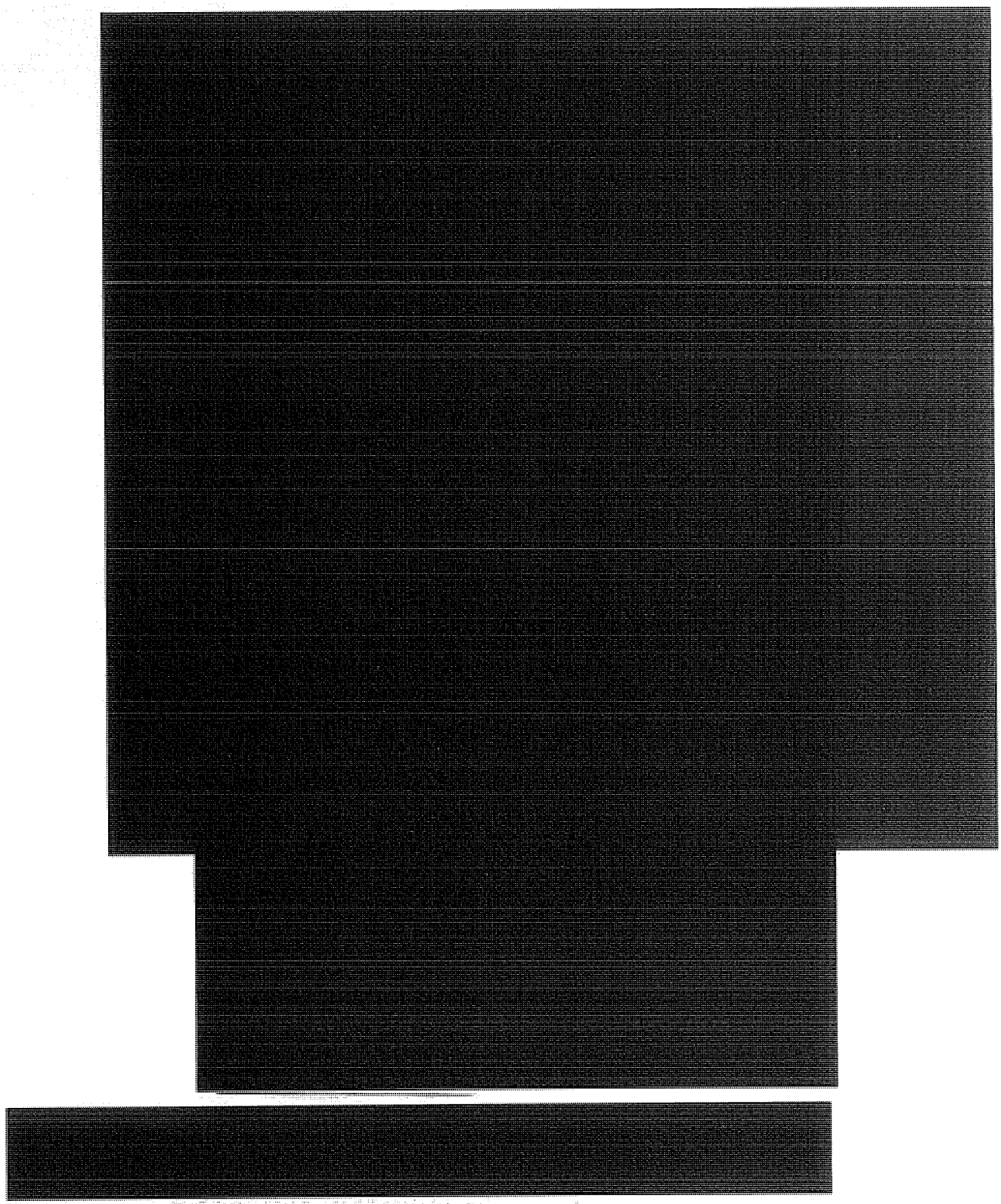
Procedures, 27 July 1993, prescribes policies and minimization procedures and assigns responsibilities to ensure that United States SIGINT System missions and activities are conducted in a manner that safeguards U.S. persons' Constitutional rights. (See Appendix G.)

~~(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]

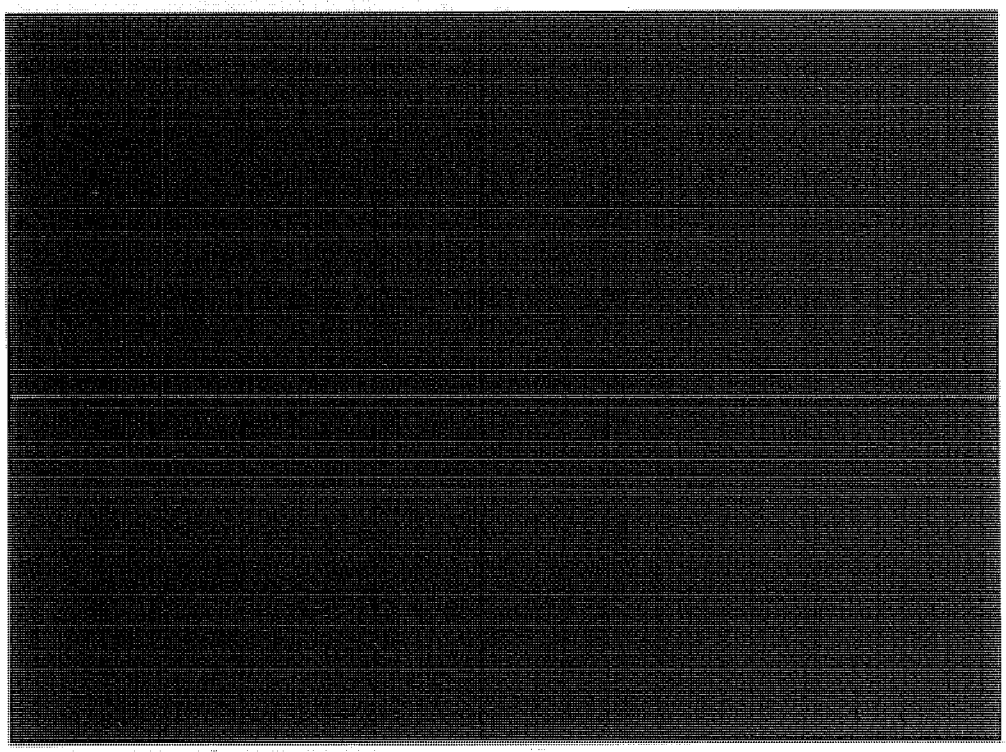
~~(S//NF)~~ In Oval Office Meeting, DCI Explained NSA Director's Decision to Expand Operations under Existing SIGINT Authorities

(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.

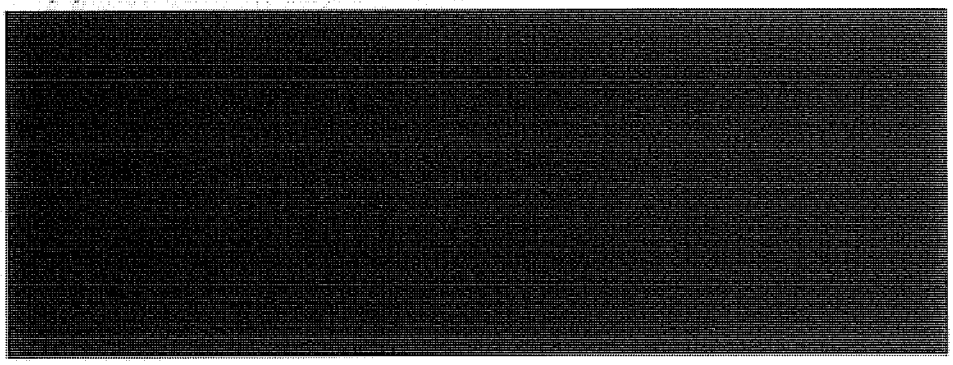
(U) Vice President Asked What Other Authorities NSA Needed

[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]

[1] ~~(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

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

[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.