EXHIBIT A,
Part 1 of 5

ST-09-0002 WORKING DRAFT
OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

24 March 2009

(U) TABLE OF CONTENTS

WORKING DRAFT

I. (U) INTRODUCTION

Background

(U//FOUO) On 4 October 2001, President George W. Bush issued a memorandum entitled "AUTHORIZATION FOR SPECIFIED ELECTRONIC SURVEILLANCE ACTIVITIES DURING A LIMITED PERIOD TO DETECT AND PREVENT ACTS OF TERRORISM WITHIN THE UNITED STATES." The memorandum was 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.

(TS//SI//OR/NF) The 4 October 2001 Presidential authorization delegated authority to the Secretary of Defense, who further delegated it to the Director of National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) to conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority.

(TS//SI//OR/NF) The Authorization specified that NSA could acquire the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata[1] 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. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority. [2]

(U) This Report

(U//FOUO) This report provides the classified results of the NSA Office of the Inspector General (OIG) review of the President's Surveillance Program (PSP) as mandated in the FISA Amendments Act (FAA) of 2008. It includes the facts necessary to describe from NSA's perspective:

[1] (U)Metadata is data that describes content, events, or networks associated with SIGINT targets.
[2] (U)The Authority changed over time. See Appendix B for details.

- ☒ establishment of the PSP (Section One)
- ☒ implementation and product of the PSP (Section Two)
- ☒ access to legal reviews of the PSP and access to information about the PSP (Section Three)
- ☒ interaction with the Foreign Intelligence Surveillance Court (FISC) and transition to court orders related to the PSP (Section Four)
- ☒ oversight of PSP activities at NSA (Section Five)

(U) President's Surveillance Program Terminology

(U//FOUO) For purposes of this report, the PSP, or "the Program," refers to NSA activities conducted under the authority of the 4 October 2001 memorandum and subsequent renewals, hereafter known as "the Authorization." As mandated by the FAA, this review includes activities authorized by the President between 11 September 2001 and 17 January 2007 and those activities continued under FISC authority. This includes the program described by the President in a 17 December 2005 radio address as the Terrorist Surveillance Program, which was content collected under the Authorization.

WORKING DRAFT

II. REVIEW CATEGORIES

(U) ONE: ESTABLISHMENT OF THE AUTHORITY

(U//FOUO) Immediately after the attacks of 11 September 2001, NSA considered how to work within existing SIGINT authorities to counter the terrorist threat within the United States and adjusted SIGINT processes accordingly. Shortly thereafter, in response to a White House request, the Director of NSA identified SIGINT collection gaps. The Counsel to the Vice President used this information to draft the Presidential authorization that established the PSP.

(U) Actions Taken After 9/11

(TS//SI//NF) On 14 September 2001, three days after terrorist attacks in the United States, General Hayden approved the targeting of terrorist-associated foreign telephone numbers on communication links between the United States and foreign countries where terrorists were known to be operating. Only specified, pre-approved numbers were allowed to be tasked for collection against U.S.-originating links. He authorized this collection at Special Collection Service and Foreign Satellite sites with access to links between the United States and countries of interest, including Afghanistan. According to the Deputy General Counsel, General Hayden determined by 26 September that any Afghan telephone number in contact with a U.S. telephone number on or after 26 September was presumed to be of foreign intelligence value and could be disseminated to the FBI.

(TS//SI//NF) NSA OGC said General Hayden's action was a lawful exercise of his power under Executive Order (E.O.) 12333, *United States Intelligence Activities*, as amended. The targeting of communication links with one end in the United States was a more aggressive use of E.O. 12333 authority than that exercised by former Directors. General Hayden was operating in a unique environment in which it was a widely held belief that additional terrorist attacks on U.S. soil were imminent. General Hayden said this was a "tactical decision."

(U//FOUO) On 2 October 2001, General Hayden briefed the House Permanent Select Committee on Intelligence (HPSCI) on this decision and later informed members of the Senate Select Committee on Intelligence (SSCI) by telephone. He had also informed DCI George Tenet.

(TS) At the same time NSA was assessing collection gaps and increasing efforts against terrorist targets immediately after the 11 September attacks, it was responding to Department of Defense (DoD), Director of Central Intelligence Community Management Staff questions about its ability to counter the new threat.

(U) Need to Expand NSA Authority

(U//FOUO) General Hayden said that soon after he told Mr. Tenet about NSA actions to counter the threat, Mr. Tenet shared the information with the "Oval Office." Mr. Tenet relayed that the Vice President wanted to know if NSA could be doing more. General Hayden replied that nothing else could be done within existing NSA authorities. In a follow-up telephone conversation, Mr. Tenet asked General Hayden what could be done if he had additional authorities. General Hayden said that these discussions were not documented.

(U//FOUO) NSA Identifies SIGINT Collection Gaps

(TS//SI//NF) To respond to the Vice President, General Hayden met with NSA personnel who were already working to identify and fill SIGINT collection gaps in light of the recent terrorist attacks. General Hayden stated that he met with personnel to identify which additional authorities would be operationally useful and technically feasible. In particular, discussions focused on how NSA might bridge the "international gap." An NSA Technical Director described that gap in these terms:

> *"Here is NSA standing at the U.S. border looking outward for foreign threats. There is the FBI looking within the United States for domestic threats. But no one was looking at the foreign threats coming into the United States. That was a huge gap that NSA wanted to cover."*

(TS//SI//NF) **Possible Solutions.** Among other things, NSA considered how to tweak transit collection—the collection of communications transiting through but not originating or terminating in the United States. NSA personnel also resurfaced a concept proposed in 1999 to address the

Millennium Threat. NSA proposed that it would perform contact chaining on metadata it had collected. Analysts would chain through masked U.S. telephone numbers to discover foreign connections to those numbers, without specifying, even for analysts, the U.S. number involved. In December 1999, the Department of Justice (DoJ), Office of Intelligence Policy Review (OIPR) told NSA that the proposal fell within one of the FISA definitions of electronic surveillance and, therefore, was not permissible when applied to metadata associated with presumed U.S. persons (i.e., U.S. telephone numbers not approved for targeting by the FISC).

(TS//SI//NF) **Collection gaps not adequately filled by FISA authorized intercept.** NSA determined that FISA authorization did not allow sufficient flexibility to counter the new terrorist threat. First, it believed that because of technological advances, the jurisdiction of the FISC went beyond the original intent of the statute. For example, most communications signals no longer flowed through radio ~~signals~~ signals or via phone systems as they did in 1978 when the FISA was written. By 2001, Internet communications were used worldwide, undersea cables carried huge volumes of communications, and a large amount of the world's communications passed through the United States. Because of language used in the Act in 1978, NSA was required to obtain court orders to target email accounts used by non-U.S. persons outside the United States if it intended to intercept the communications at a webmail service within the United States. Large numbers of terrorists were using such accounts in 2001.

(TS//SI//NF) Second, NSA believed that the FISA process was unable to accommodate the number of terrorist targets or the speed with which they changed their communications. From the time NSA sent FISA requests to the DoJ, OIPR until the time data arrived at NSA, the average wait was between four and six weeks. Terrorists could have changed their telephone numbers or internet addresses before NSA received FISC approval to target them. NSA believed the large number of terrorist targets and their frequently changing communications would have overwhelmed the existing FISA process.

(TS//SI//NF) Emergency FISA provision not an option. NSA determined that even using emergency FISA court orders would not provide the speed and flexibility needed to counter the terrorist threat. First, although the emergency authorization provision permitted 72 hours of surveillance without obtaining a court order, it did not—as many believed—allow the Government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would ultimately be acceptable to the FISC. He had to be certain the court

would grant a warrant before initiating emergency surveillance. Additionally, before NSA surveillance requests were submitted to the Attorney General, they had to be reviewed by NSA intelligence officers, NSA attorneys, and Department of Justice attorneys. Each reviewer had to be satisfied that standards had been met before the request proceeded to the next review group, and each request was certified by a senior official in the DoD, usually the Secretary or Deputy Secretary. From the time NSA sent a request to Justice's OIPR until the time data arrived at NSA, the average wait was between a day and a day and a half. In the existing threat environment with U.S. interests at risk, NSA deemed the wait too long.

(U//FOUO) Early Efforts to Amend FISA

(TS//SI//NF) Given the limitations of FISA, there were early efforts to amend the statute. For example, shortly after 11 September, the HPSCI asked NSA for technical assistance in drafting a proposal to amend Section III of FISA that would give the President the authority to conduct electronic surveillances without a court order for the purpose of obtaining foreign intelligence information. On 20 September 2001, the NSA General Counsel wrote to Judge Alberto Gonzales, Counsel to the President, asking whether the proposal had merit. We found no record of a response.

(U//FOUO) We could not determine why early efforts to amend FISA were abandoned. Anecdotal evidence suggests that government officials feared the public debate surrounding any changes to FISA would compromise intelligence sources and methods.

(U) NSA identifies SIGINT collection gaps to Vice President's Office.

(TS//SI//NF) Because early discussions about expanding NSA's authority were not documented, we do not have records of specific topics discussed or people who attended General Hayden's meetings with White House representatives. General Hayden stated that after consulting with NSA personnel, he described to the White House how NSA collection of communications on a wire inside the United States was constrained by the FISA statute. Specifically, NSA could not collect from a wire in the United

States, without a court order, either content or metadata from communications links with either one or both ends in the United States. Furthermore, General Hayden pointed out that communications metadata did not have the same level of constitutional protection as content and that access to metadata of communications with one end in the United States would significantly enhance NSA's analytic capabilities. General Hayden suggested that the ability to collect communications with one end in the United States without a court order would increase NSA's speed and agility. General Hayden stated that after two additional meetings with the Vice President, the Vice President asked him to work with his Counsel, David Addington.

(U) Presidential Authorization Drafted and Signed

(TS//SI//OR/NF) According to General Hayden, the Vice President's Counsel, David Addington, drafted the first Authorization. General Hayden described himself as the "subject matter expert" but stated that no other NSA personnel participated in the drafting process, including the General Counsel. He also said that Department of Justice (DOJ) representatives were not involved in any of the discussions that he attended and he did not otherwise inform them.

(TS//SI//NF) General Hayden said he was "surprised with a small 's' " when the Authorization was signed on 4 October 2001, and that it only changed the location from which NSA could collect communications. Rules for minimizing U.S. person information still had to be followed.

(U//FOUO) SIGINT Activity Authorized by the President

(TS//SI//OR/NF) On 4 October 2001, the President delegated authority through the Secretary of Defense to the Director of NSA to conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority.

(TS//SI//STLW//NF) The Authorization allowed NSA to conduct four types of collection activity:

- [X] Telephony content
- [X] Internet content

☒ Telephony metadata

☒ Internet metadata

(TS//SI//NF) NSA could collect the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire 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. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority.

(U//FOUO) Subsequent Changes to the Authorization

(TS//SI//NF) After the first Presidential authorization, the specific terms, wording, or interpretation of the renewals periodically changed. (See Appendix B for a completed listing of changes.)

(TS//SI//NF) **Domestic Collection.** The wording of the first authorization could have been interpreted to allow domestic content collection where both communicants were located in the U.S. or were U.S. persons. General Hayden recalled that when the Counsel to the Vice President pointed this out, General Hayden told him that NSA would not collect domestic communications because 1) NSA was a foreign intelligence agency, 2) NSA infrastructure did not support domestic collection, and 3) his personal standard was so high that there would be no problem getting a FISC order for domestic collection.

(TS//SI//NF) **Afghanistan.** In January 2002, after the Taliban was forced out of power, Afghanistan was no longer specifically identified in the Authorization.

(TS//SI//NF) **Iraqi Intelligence Service.** For a limited period of time surrounding the 2003 invasion of Iraq, the President authorized the use of PSP authority against the Iraqi Intelligence Service. On 28 March 2003, the DCI determined that, based on then current intelligence, the Iraqi Intelligence service was engaged in terrorist activities and presented a threat to U.S. interests in the United States and abroad. Through the Deputy DCI, Mr. Tenet received the President's concurrence that PSP authorities could be used against the Iraqi Intelligence Service. NSA ceased using the Authority for this purpose in March 2004.