~~TOP SECRET//HCS//SI//NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

[redacted] (S)

Docket Number: BR 06-05

EXHIBIT C

MEMORANDUM OF LAW IN SUPPORT OF APPLICATION FOR CERTAIN TANGIBLE THINGS FOR INVESTIGATIONS TO PROTECT AGAINST INTERNATIONAL TERRORISM

~~TOP SECRET//HCS//SI//NOFORN~~

Derived from Application of the United States to the Foreign Intelligence Surveillance Court in the above-captioned matter.

[redacted]

INTRODUCTION (U)

One of the greatest challenges the United States faces in the ongoing conflict with [redacted] is finding operatives of the enemy. As this Court is aware, one of the most significant tools that the U.S. Government can use to accomplish that task is metadata analysis. Under this Court's order in [redacted] Opinion and Order, No. PR/TT [redacted] ("[redacted]"), and subsequent related authorizations, the National Security Agency (NSA) is currently collecting metadata in bulk from electronic communications and applying sophisticated analytic tools to identify and find [redacted]. The attached Application seeks this Court's authorization to collect in bulk [redacted] certain business records—call detail records, or "telephony metadata"—so that the NSA may use these same analytic tools to identify and find operatives of [redacted]. (~~TS//SI//NF~~)

The attached Application for business records is made pursuant to title V of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1861 et seq., as amended, "Access to Certain Business Records for Foreign Intelligence Purposes," to capitalize upon the unique opportunities the United States has for identifying communications of [redacted]. The collection sought here will make possible a potentially powerful tool that the Government has to discover enemy communications: metadata analysis. For telephone calls, metadata essentially consists of routing information that includes the telephone number of the calling party, the telephone number of the called party, and the date, time and duration of the call. It does not include the substantive content of the communication or the name, address, or financial information of a subscriber or customer. Relying solely on such metadata, the Government can analyze the contacts made by a telephone number reasonably suspected to be associated with a terrorist, and

thereby possibly identify other, previously unknown, terrorists. The primary advantage of metadata analysis as applied to telephony metadata is that it enables the Government to analyze past connections and [redacted] That analysis is possible, however, only if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related. In addition, individually targeted collection of metadata is inadequate for tracking the communications of terrorists who [redacted]. ~~(TS//SI//NF)~~

In the attached Application, therefore, the Government requests that this Court order the production, in bulk and on an ongoing basis, of certain business records [redacted] For billing and fraud detection purposes, [redacted] "call detail records" that contain routing information, including which telephone number called which other telephone number at what date and time, and for how long, i.e., "metadata." The Application fully satisfies all requirements of title V of FISA. In particular, the Application seeks the production of tangible things "for" an international terrorism investigation. 50 U.S.C. § 1861(a)(1). In addition, the Application includes a statement of facts demonstrating that there are reasonable grounds to believe that the business records sought are "relevant" to an authorized investigation. *Id.* § 1861(b)(2). Although the call detail records [redacted] contain large volumes of metadata, the vast majority of which will not be terrorist-related, the scope of the business records request presents no infirmity under title V. All of the business records to be collected here are relevant to FBI investigations into [redacted] because the NSA can effectively conduct metadata analysis only if it has the data in bulk. ~~(TS//SI//NF)~~

In addition, even if the metadata from non-terrorist communications were deemed not relevant, nothing in title V of FISA demands that a request for the production of "any tangible things" under that provision collect *only* information that is strictly relevant to the international terrorism investigation at hand. Were the Court to require some tailoring to fit the information that will actually be terrorist-related, the business records request detailed in the Application would meet any proper test for reasonable tailoring. Any tailoring standard must be informed by a balancing of the government interest at stake against the degree of intrusion into any protected privacy interests. Here, the Government's interest is the most compelling imaginable: the defense of the Nation in wartime from attacks that may take thousands of lives. On the other side of the balance, the intrusion is minimal. As the Supreme Court has held, there is no constitutionally protected interest in metadata, such as numbers dialed on a telephone. Any intrusion is further reduced because only data connected to telephone numbers reasonably suspected to be terrorist-associated will ever be viewed by any human being. Indeed, only a tiny fraction (estimated by the NSA to be 0.000025% or one in four million) of the call detail records collected actually will be seen by a trained NSA analyst. Under the procedures the Government will apply, metadata reflecting the activity of a particular telephone number will only be seen by a human analyst if a computer search has established a connection to a terrorist-associated telephone number. (~~TS//SI//NF~~)

The Application is completely consistent with this Court's ground breaking and innovative decision [redacted] in [redacted]. In that case, the Court authorized the installation and use of pen registers and trap and trace devices to collect bulk e-mail metadata [redacted]. The Court found that all of "the information likely to be

obtained" from such collection "is relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c)(2), [redacted] at 25-54. The Court explained that "the bulk collection of meta data—i.e., the collection of both a huge volume and high percentage of unrelated communications—is necessary to identify the much smaller number of [redacted] communications." *Id.* at 49. Moreover, as was the case in [redacted], this Application promotes both of the twin goals of FISA: facilitating the foreign-intelligence collection needed to protect American lives while at the same time providing judicial oversight to safeguard American freedoms. (~~S~~)

BACKGROUND (U)

A. The Al Qaeda Threat (~~S~~)

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 jetliners, each carefully selected to be fully loaded with 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 direct blow at the leadership of the Government of the United States. 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. These attacks shut down air travel in the United States,

disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy. (U)

Before the September 11th attacks, al Qaeda had promised to attack the United States. In 1998, Osama bin Laden declared a "religious" war against the United States and urged that it was the moral obligation of all Muslims to kill U.S. civilians and military personnel. *See* Statement of Osama bin Laden, Ayman al-Zawahiri, et al., *Fatwah Urging Jihad Against Americans*, published in Al-Quds al-'Arabi (Feb. 23, 1998) ("To kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim."). Al Qaeda carried out those threats with a vengeance; they attacked the U.S.S. Cole in Yemen, the United States Embassy in Nairobi, and finally the United States itself in the September 11th attacks. (U)

It is clear that al Qaeda is not content with the damage it wrought on September 11th. Just a few months ago, Osama bin Laden pointed to "the explosions that . . . have take[n] place in the greatest European capitals" as evidence that "the mujahideen . . . have been able to break through all the security measures taken by" the United States and its allies. Osama bin Laden, audiotape released on Al-Jazeera television network (Federal Bureau of Investigation trans., Jan. 19, 2006). He warned that "the delay of [sic] inflicting similar operations in America has not been due to any impossibility of breaking through your security measures[,] for those operations are underway and you will see them in your midst as soon as they are done." *Id.* Several days later, bin Laden's deputy, Ayman al-Zawahiri, warned that the American people are destined for "a future colored by blood, the smoke of explosions and the shadows of terror." Ayman al-

Zawahiri, videotape released on the Al-Jazeera television network (Jan. 30, 2006). These recent threats were just the latest in a series of warnings since September 11th by al Qaeda leaders who have repeatedly promised to deliver another, even more devastating attack on America. *See, e.g.*, Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 24, 2004) (warning United States citizens of further attacks and asserting that "your security is in your own hands"); Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 18, 2003) ("We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States . . . ."); Ayman al-Zawahiri, videotape released on the Al-Jazeera television network (Oct. 9, 2002) ("I promise you [addressing the 'citizens of the United States'] that the Islamic youth are preparing for you what will fill your hearts with horror"). As recently as December 7, 2005, al-Zawahiri professed that al Qaeda "is spreading, growing, and becoming stronger," and that al Qaeda is "waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders' own homes." Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). Indeed, since September 11th, al Qaeda has staged several large-scale attacks around the world, including in Tunisia, Kenya and Indonesia, killing hundreds of innocent people. In addition, Ayman al-Zawahiri claimed that al Qaeda played some role in the July 2005 attacks on London. *See* Declaration of John S. Redd, Director, National Counterterrorism Center ¶ 35 (May 22, 2006) (Exhibit B to the Application) ("NCTC Declaration"). Given that al Qaeda's leaders have repeatedly made good on their threats and that al Qaeda has demonstrated its ability to insert foreign agents into the United States to execute attacks, it is clear that the threat continues. (~~TS//SI//NF~~)

Reliable intelligence indicates that [redacted] remains intent on striking the United States and U.S. interests. See NCTC Declaration ¶¶ 5-7, 8, 11-13. "[redacted] is an international

organization with a global presence, with members located in at least 40 countries, and the capability to strike US interests anywhere in the world." *Id.* ¶ 5. Indeed, [redacted] "continues its efforts to reconstitute communication links to a transnational network of [redacted] personnel and affiliated groups." *Id.* ¶ 39. Recent intelligence suggests that [redacted] has become "keenly" interested in soft targets, especially those that are densely populated. *Id.* ¶¶ 17, 75. [redacted] and its affiliates consistently have expressed an interest in attacking U.S. rail and mass transit systems, as well as continuing to target the civil aviation sector, including U.S. passengers and Western aircraft overseas. *Id.* ¶¶ 74-80. Moreover, the Intelligence Community is concerned that the next [redacted] attack in the United States might use chemical, biological, radiological or nuclear weapons, "especially given [redacted] clear intent to develop such capabilities and use them to strike the Homeland." *Id.* ¶ 81. In sum, [redacted] continues to present "a credible threat for a massive attack against the US Homeland." *Id.* ¶ 91. By helping to find and identify members and agents of [redacted], particularly those who are already within the United States, the proposed request for business records would greatly help the United States prevent another such catastrophic terrorist attack, one that [redacted] itself has claimed would be larger than the attacks of September 11th. ~~(TS//SI//HCS//OC,NF)~~

B. [redacted] Use of Telephones to Communicate ~~(S)~~

[redacted] use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, [redacted] make domestic U.S. telephone calls. For purposes of preventing terrorist attacks against the United States, the most analytically significant [redacted] telephone communications are those that either have one end in the United States or that are purely domestic, because those

communications are particularly likely to identify individuals who are associated with [redacted] in the United States whose activities may include planning attacks on the homeland. *See* Declaration of Lieut. Gen. Keith B. Alexander, U.S. Army, Director, NSA ¶ 5 (May 22, 2006) (Exhibit A to the Application) ("NSA Declaration"). The vast majority of the call detail records sought in the attached Application would include records of telephone calls that either have one end in the United States or are purely domestic, including local calls, although some records would relate to communications in which both ends were outside the United States. The United States needs to sort through this telephony metadata to find and identify [redacted] and thereby acquire vital intelligence that could prevent another deadly terrorist attack. ~~(TS//SI//NF)~~

C. **Discovering the Enemy: Metadata Analysis** ~~(TS//SI//NF)~~

Analyzing metadata from international and domestic telecommunications—such as information showing which telephone numbers have been in contact with which other telephone numbers, for how long, and when[1]—can be a powerful tool for discovering communications of terrorist operatives. Collecting and archiving metadata is thus the best avenue for solving the following fundamental problem: although investigators do not know *exactly* where the terrorists' communications are hiding in the billions of telephone calls flowing through the United States today, we do know that they *are there*, and if we archive the data now, we will be able to use it in a targeted way to find the terrorists tomorrow. NSA Declaration ¶¶ 7-11. As the NSA has explained, "[t]he ability to accumulate a metadata archive and set it aside for carefully controlled

[1] For telephone calls, "metadata" includes comprehensive communications routing information, including the telephone number of the calling party, the telephone number of the called party, and the date, time and duration of the call, as well as communications device and trunk identifiers. A "trunk" is a communication line between two switching systems. *Newton's Telecom Dictionary* 853 (20th ed. 2004). Telephony metadata does not include the content of the communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. ~~(S)~~

searches and analysis will substantially increase NSA's ability to detect and identify members of al Qaeda and its affiliates." *Id.* ¶ 8; *see also* [redacted] at 43-45. (~~TS//SI//NF~~)

Collecting and archiving metadata offers at least two invaluable capabilities to analysts that are unavailable from any other approach. First, it allows for retrospective "contact chaining." For example, analysts may learn that a particular telephone number is associated with [redacted] perhaps because it was found in the cell phone directory of a recently captured [redacted] agent. By examining metadata that has been archived over a period of time, analysts can search to find the contacts that have been made by that "seed" telephone number. The ability to see who communicates with whom may lead to the discovery of other terrorist operatives, may help to identify hubs or common contacts between targets of interest who were previously thought to be unconnected, and may help to discover individuals willing to become FBI assets. Indeed, computer algorithms can identify not only the first tier of contacts made by the telephone number reasonably suspected to be associated with [redacted] but also the further contacts made by the first and second tiers of telephone numbers. NSA Declaration ¶ 9. Going out beyond the first tier enhances the ability of analysts to find terrorist connections by increasing the chances that they will find previously unknown terrorists. A seed telephone number, for example, may be in touch with several telephone numbers previously unknown to analysts. Following the contact chain out two additional "hops" to examine the contacts made by the first two tiers of telephone numbers may reveal a contact that connects back to a different terrorist-associated telephone number already known to the analyst. Going out to the third tier is useful for telephony because, unlike e-mail traffic, which includes the heavy use of "spam," a telephonic device does not lend itself to simultaneous contact with large numbers of individuals. (~~TS//SI//NF~~)

The capabilities offered by such searching of a collected archive of metadata are vastly more powerful than chaining that could be performed on data collected pursuant to national security letters issued by the Government under 18 U.S.C. § 2709 and targeted at individual telephone numbers. If investigators find a new telephone number when [redacted]s captured, and the Government issues a national security letter for the local and long distance toll billing records for that particular account, it would only be able to obtain the first tier of telephone numbers that the [redacted] number has been in touch with. To find an additional tier of contacts, new national security letters would have to be issued for each telephone number identified in the first tier. The time it would take to issue the new national security letters would necessarily mean losing valuable data. And the data loss in the most critical cases would only be increased by terrorists' [redacted] Moreover, because telephone companies generally only keep call detail records in an easily accessible medium for up to two years, historical chaining analysis on the number may lead analysts to other individuals [redacted] by revealing the contacts that were made by a terrorist-associated telephone number more than two years ago. *See* NSA Declaration ¶ 12. ([redacted])

The second major tool analysts can use with an archive of collected metadata is [redacted]. Skilled analysts can then use a [redacted] to determine whether there is another telephone number within the archived metadata that shows a [redacted] Obviously, such [redacted] is a critical tool for

keeping up with terrorists [redacted] *See* NSA Declaration ¶ 11. It provides an invaluable capability that could not be reproduced through any other mechanism [redacted]. Such analysis can be performed only if the Government has collected and archived the data [redacted] ~~(TS//SI//NF)~~

E. The Foreign Intelligence Surveillance Act (U)

FISA provides a mechanism for the Government to obtain business records—here, call detail records—[redacted] containing precisely the type of communications data that is vital for the metadata analysis described above—including the telephone number of the calling party, the telephone number of the called party, and the date, time and duration of the call. Section 501 of FISA, as recently amended by section 106 of the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 196-200 (Mar. 9, 2006) ("USA PATRIOT Reauthorization Act"), authorizes the Director of the FBI or his designee to apply to this Court

> for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution.

50 U.S.C. § 1861(a)(1).[2] ~~(S)~~

[2] The call detail records sought in the attached Application would not be collected by a "pen register" or "trap and trace device" as defined by 18 U.S.C. § 3127. Each of these terms refers to a "device or process" which either "records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"—a pen register, *id.* § 3127(3), or "captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication"—a trap and trace device, *id.* § 3127(4). As the definitions make clear, pen registers and trap and

LEGAL ANALYSIS (U)

I. The Application Fully Complies with All Statutory Requirements. (U)

Section 501(c)(1) of FISA, as amended, directs the Court to enter an ex parte order requiring the production of tangible things if the judge finds that the Government's application meets the requirements of subsections 501(a) and (b). The most significant of those requirements are that the tangible things, which include business records, are "for" an investigation to protect against international terrorism. 50 U.S.C. § 1861(a)(1). Section 501(b)(2)(A) indicates that this requirement is one of relevance, providing that the Government's application must include

> a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) [*i.e.*, following Attorney General-approved Executive Order 12333 guidelines and not conducted of a U.S. person solely on the basis of First Amendment-protected activities] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of facts that they pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.

Id. § 1861(b)(2)(A).[3] (U)

---

trace devices are mechanical "device[s]," or perhaps software programs ("process[es]"), that "record" or "decode" data as communications signals are passing through the particular spot in the communications network where the "device" or "process" has been installed, or that "capture" data in a similar fashion. *See, e.g.*, *United States Telecom Ass'n v. FBI*, 276 F.3d 620, 623 (D.C. Cir. 2002) ("Pen registers are devices that record the telephone numbers dialed by the surveillance's subject; trap and trace devices record the telephone numbers of the subject's incoming calls."). The mechanism by which the NSA would receive call detail records does not involve any such "device or process." Instead, [redacted] would copy and transmit the call detail records, [redacted] independently compile in their normal course of business, to the NSA in real or near-real time. (TS//SI//NF)

[3] Until recently, section 501(b)(2) provided only that the Government's application "specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2) (Supp. I 2001). According to the legislative history of the USA PATRIOT Reauthorization Act, the provision was amended "to clarify that the

Thus, section 501(b)(2) of FISA requires that an application for an order requiring the production of business records must include a statement of facts showing that there are "reasonable grounds to believe" that certain criteria are met: (1) that the business records are relevant to an authorized investigation, other than a threat assessment, that is being conducted, for example, to protect against international terrorism; (2) that the investigation is being conducted under guidelines approved by the Attorney General under Executive Order 12333; and (3) that the investigation is not being conducted of a U.S. person solely upon the basis of activities protected by the First Amendment. *Id.* § 1861(b)(2)(A). All of these criteria are met here. (U)

Taking the last two requirements first, the attached Application establishes that the business records sought are for FBI investigations into [redacted] investigations which are being conducted under Attorney General-approved 12333 guidelines and that are not being conducted of any U.S. persons solely upon the basis of First Amendment-protected activities. In addition, the attached Application and accompanying declarations by the Directors of the NSA and National Counterterrorism Center certainly demonstrate that there are "reasonable grounds to believe" that the business records sought are "relevant" to authorized investigations to protect against international terrorism. (~~S~~)

A. The Business Records Sought Meet the Relevance Standard. (U)

Information is "relevant" to an authorized international terrorism investigation if it bears upon, or is pertinent to, that investigation. *See* 13 Oxford English Dictionary 561 (2d ed. 1989) ("relevant" means "[b]earing upon, connected with, pertinent to, the matter in hand"); Webster's

tangible things sought by [an order under section 501] must be 'relevant' to an authorized preliminary or full investigation . . . to protect against international terrorism." H.R. Conf. Rep. No. 109-333, at 90 (2005). (U)

Third New Int'l Dictionary 1917 (1993) ("relevant" means "bearing upon or properly applying to the matter at hand . . . pertinent"); *see also Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (noting that the phrase "relevant to the subject matter involved in the pending action" in Fed. R. Civ. Proc. 26(b)(1) has been "construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case"); *cf.* Fed. R. Evid. 401 ("'Relevant evidence' means evidence having *any* tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.") (emphasis added). Indeed, section 501(b)(2) establishes a presumption that the Government has satisfied the relevancy requirement if it shows that the business records sought "pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation." 50 U.S.C. § 1861(b)(2)(A). The USA PATRIOT Reauthorization Act added this presumption to section 501(b) to outline certain situations in which the Government automatically can establish relevance; the presumption was not intended to change the relevance standard for obtaining business records under section 501. *See* Pub. L. No. 109-177, § 106, 120 Stat. 196; H.R. Conf. Rep. No. 109-333, at 91 (Section 501(b)(2) "also requires a statement of facts to be included in the application that shows there are reasonable grounds to believe the tangible things sought are relevant, and, if such facts show reasonable grounds to believe that certain specified connections to a foreign power or an agent of a foreign power are present, the tangible things sought are presumptively relevant. *Congress does not intend to prevent the FBI from obtaining tangible things that it currently can obtain under section [501].*") (emphasis added). (U)

The FBI currently has over 1,000 open National Security Investigations targeting [redacted] Osama bin Laden [redacted] As we have explained above, the bulk telephony metadata sought in the attached Application is relevant to the FBI's investigations into [redacted] because, when acquired, stored, and processed, the telephony metadata would provide vital assistance to investigators in tracking down [redacted] operatives. Although admittedly a substantial portion of the telephony metadata that is collected would not relate to operatives of [redacted],[4] the intelligence tool that the Government hopes to use to find [redacted] communications—metadata analysis—requires collecting and storing large volumes of the metadata to enable later analysis. All of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection. ~~(TS//SI//NF)~~

Archiving and analyzing the metadata sought in the attached Application will assist the FBI in obtaining foreign intelligence and, in particular, in identifying the telephone numbers of [redacted] operating within the United States. For example, contact chaining and [redacted] of the archived information will allow the NSA to identify telephone numbers that have been in contact with telephone numbers the NSA reasonably suspects to be linked to [redacted] and its affiliates. NSA may provide such information to the FBI, which can determine whether an investigation should be commenced to identify the users of the telephone numbers and to determine whether there are any links to international terrorist activities. The NSA estimates that roughly 800 telephone numbers will be tipped annually to the FBI, CIA, or other appropriate U.S. government or foreign government agencies. NSA Declaration ¶ 18. The FBI would also

[4] The NSA expects that this business records request, over the course of a year, will result in the collection of metadata pertaining to [redacted] communications. *See* NSA Declaration ¶ 6. ~~(TS//SI//NF)~~

be able to ask the NSA to perform contact chaining [redacted] on terrorist-associated telephone numbers known to the FBI. (~~TS//SI//NF~~)

The call detail records sought in the attached Application are certainly "relevant" to an authorized investigation into [redacted] As this Court recently noted in [redacted] the requirement of relevance is a relatively low standard. [redacted] at 29. In that case, the Court was interpreting a similar, and quite possibly more stringent standard than that presented here. There, the Court found that section 402(a) of FISA was satisfied, i.e., that "the information likely to be obtained *is* . . . relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c) (emphasis added).[5] Here, by contrast, the Application need only establish that there are "reasonable grounds to believe" that the records sought are relevant to an authorized international terrorism investigation.[6] *Id.* § 1861(b)(2)(A). (~~TS//SI//NF~~)

In evaluating whether metadata collected in bulk is "relevant" to investigations into [redacted] this Court has recognized that, "for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in

[5] Although the Government argued that the statute did not permit the Court to look behind the Government's certification of relevance, the Court assumed for purposes of the case that it should consider the basis for the certification. *See* [redacted] at 26-28. (~~TS//SI//NF~~)

[6] The "reasonable grounds to believe" standard is simply a different way of articulating the probable cause standard. *See Maryland v. Pringle*, 540 U.S. at 371 (quoting *Brinegar v. United States*, 338 U.S. 160, 175 (1949) ("'The substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). As the Supreme Court has recently explained, "[t]he probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Rather than being "technical," these probabilities "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Brinegar*, 338 U.S. at 176; *see also Pringle*, 540 U.S. at 370 (quoting *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quoting *Brinegar*)). In addition, probable cause "does not require the fine resolution of conflicting evidence that a reasonable-doubt or even a preponderance standard demands." *Gerstein v. Pugh*, 420 U.S. 103, 121 (1975); *see also Illinois v. Gates*, 462 U.S. 213, 235 (1983) ("Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the [probable cause] decision."). (U)

determining the potential significance of intelligence-related information. Such deference is particularly appropriate in this context, where the Court is not charged with making independent probable cause findings." [redacted] at 30-31. In [redacted] this Court noted that the proposed activity would result in the collection of metadata pertaining to [redacted] of electronic communications, all but a very small fraction of which could be expected to be unrelated to [redacted] *Id.* at 39-40, 48. Nonetheless, this Court found that the bulk collection of metadata "is necessary to identify the much smaller number of [redacted] communications" and that therefore, "the scope of the proposed collection is consistent with the certification of relevance." *Id.* at 48-49. In part that was because the NSA had explained, as it does here, that "more precisely targeted forms of collection against known accounts would tend to screen out the 'unknowns' that NSA wants discover, so that NSA needs bulk collection in order to identify unknown [redacted] *Id.* at 42. Just as the bulk collection of e-mail metadata was relevant to FBI investigations into [redacted] so is the bulk collection of telephony metadata described herein. ~~(TS//SI//NF)~~

B. **The Proposed Collection Is Appropriately Tailored.** (U)

Title V of FISA does not expressly impose any requirement to tailor a request for tangible things precisely to obtain solely records that are strictly relevant to the investigation. To the extent, however, the Court construes the "relevance" standard under Title V to require some tailoring of the requested materials to limit overbreadth, the request for tangible things proposed here is not overbroad. As this Court concluded in [redacted] "the applicable relevance standard does not require a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [redacted]-related FBI

investigations."[7] *Id.* at 49-50. Instead, it is appropriate to use as a guideline the Supreme Court's "special needs" jurisprudence, which balances any intrusion into privacy against the government interest at stake to determine whether a warrant or individualized suspicion is required. *See Board of Educ. v. Earls*, 536 U.S. 822, 829 (2002); *see generally* [redacted] at 50-52.[8] Here, the Government's interest is overwhelming. It involves thwarting terrorist attacks that could take thousands of lives. "This concern clearly involves national security interests beyond the normal need for law enforcement and is at least as compelling as other governmental interests that have been held to justify searches in the absence of individualized suspicion." [redacted] at 51-52; *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted). The privacy interest, on the other hand, is minimal. As we explain below, *see infra* § II, the type of data at issue is not constitutionally protected; and it would never even be *seen* by any human being unless a terrorist connection were first established. Indeed, only a tiny fraction (estimated to be 0.000025% or one in four million) of the call detail records included in the archive actually would be seen by a trained analyst.[9]

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

---

[7] As noted above, the relevance standard being interpreted in the pen register context in [redacted] that found in section 402 of FISA—is quite possibly more stringent than that required to be met by an application for business records under section 501 of FISA. ~~(S)~~

[8] Because, as we explain below, there is no Fourth Amendment-protected interest in the telephony metadata at issue here, the actual *standards* applied under Fourth Amendment balancing are far more rigorous than any that the Court should read into the statutory requirement that the business records sought under section 501 be "relevant" to an international terrorism investigation. Nevertheless, the balancing *methodology* applied under the Fourth Amendment—balancing the Government's interest against the privacy interest at stake—can provide a useful guide for analysis here. ~~(S)~~

[9] The NSA would conduct contact chaining three "hops" out, i.e., to include the first three tiers of contacts made by the reasonably suspected [redacted] telephone number. Even though a substantial portion of the telephone numbers in those first three tiers of contacts may not be used by terrorist operatives, they are all "connected" to the seed telephone number. ~~(TS//SI//NF)~~

And, as this Court recently found, "the Government need not make a showing that it is using the least intrusive means available. Rather, the question is whether the Government has chosen 'a reasonably effective means of addressing' the need." [redacted] at 52-53 (quoting *Earls*, 536 U.S. at 837) (internal citations omitted); *see also Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995) ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Here, as in [redacted] "senior responsible officials, whose judgment on these matters is entitled to deference . . . have articulated why they believe that bulk collection and archiving of meta data are necessary to identify and monitor [redacted] whose . . . communications would otherwise go undetected." [redacted] at 53-54. Such bulk collection is thus a "reasonably effective means to this end." *Id.* at 54. ~~(TS//SI//NF)~~

> In sum, as this Court previously concluded in the pen register context,
>
> the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [redacted] and thereby obtaining information likely to be relevant to ongoing FBI investigations. In these circumstances, the certification of relevance is consistent with the fact that only a very small proportion of the huge volume of information collected will be directly relevant to the FBI's [redacted] investigations.

Id. ~~(TS//SI//NF)~~

C. **The Government Will Apply Strict Minimization Procedures to the Use of the Collected Data.** (~~S~~)

The Government can assure the Court that, although the data collected under the attached Application will necessarily be broad in order to achieve the critical intelligence objectives of metadata analysis, the use of that information will be strictly tailored to identifying terrorist communications and will occur solely according to strict procedures and safeguards, including particular minimization procedures designed to protect U.S. person information. These procedures and safeguards are almost identical to the requirements imposed by this Court in [redacted] which authorized collection of a similar volume of metadata. (~~TS//SI//NF~~)

First, as described in the attached Declaration from the Director of the NSA, the NSA will query the archived data solely when it has identified a known telephone number for which, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted]; provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution." NSA Declaration ¶ 13.[10] Similarly, [redacted] would be undertaken only with respect to such an identified "seed" telephone number. For example, when an [redacted] operative is apprehended, his cellular telephone may contain a phone book listing telephone numbers. Telephone numbers listed in such a phone book would satisfy the "reasonable articulable suspicion" standard. This same

[10] For example, a telephone number of a U.S. person could not be a seed number "if the *only* information thought to support the belief that the [number] is associated with [redacted] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of 'advocacy . . . directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action.' *Brandenberg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam)." [redacted] at 58. (~~TS//SI//NF~~)

standard is, in effect, the standard applied in the criminal law context for a "*Terry*" stop. *See Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968); *see also Illinois v. Wardlow*, 528 U.S. 119, 123 (2000) (police officer may conduct a brief, investigatory *Terry* stop "when the officer has a reasonable, articulable suspicion that criminal activity is afoot").[11] It bears emphasis that, given the types of analysis the NSA will perform, no information about a telephone number will ever be accessed by or presented in an intelligible form to any person unless either (i) that telephone number has been in direct contact with a reasonably suspected terrorist-associated telephone number or is linked to such a number through one or two intermediaries, or (ii) a computer search has indicated that the telephone number has the [redacted] ~~(TS//SI//NF)~~

In addition, any query of the archived data would require approval from one of seven people: the Signals Intelligence Directorate Program Manager for Counterterrorism Special Projects; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or one of four specially authorized Counterterrorism Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. NSA Declaration ¶ 19. NSA's Office of General Counsel (OGC) would review and approve proposed queries of archived metadata based on seed accounts reasonably believed to be used by U.S. persons. *Id.* ¶ 16. Finally, NSA's OGC will brief analysts concerning the authorization requested in the Application and the limited circumstances in which queries to the archive are permitted, as well

[11] The "reasonable articulable suspicion" standard that the Government will impose on itself with respect to data collected through this Application is higher than that required by statute or the Constitution. Under FISA, the only standard to be satisfied prior to collecting information via a request for business records is that the information be relevant to an international terrorism investigation. The Fourth Amendment requires a "reasonable articulable suspicion" to justify a minimally intrusive *Terry* stop. Here, no Fourth Amendment interests are even implicated. (U)

as other procedures and restrictions regarding the retrieval, storage and dissemination of the archived data. *Id.* ~~(TS//SI//NF)~~

Second, NSA will apply several mechanisms to ensure appropriate oversight over the use of the metadata. The NSA will apply the existing (Attorney General approved) guidelines in United States Signals Intelligence Directive 18 (1993) ("USSID 18") (Exhibit D to the Application) to minimize the information reported concerning U.S. persons. NSA Declaration ¶ 17. Prior to disseminating any U.S. person information, the Chief of Information Sharing Services in the Signals Intelligence Directorate must determine that the information is related to counterterrorism information and is in fact necessary to understand the foreign intelligence information or to assess its importance. *Id.*; *see* USSID 18, § 7.2 (NSA reports may include the identity of a U.S. person only if the recipient of the report has a need to know that information as part of his official duties and, *inter alia*, the identity of the U.S. person is necessary to understand the foreign intelligence information or to assess its importance). The Director of the NSA will direct the NSA Inspector General and General Counsel to submit an initial report to him 45 days after the receipt of records pursuant to the Order assessing the adequacy of the management controls for the processing and dissemination of U.S. person information. NSA Declaration ¶ 22. The Director of the NSA will provide the findings of that report to the Attorney General. *Id.* ~~(TS//SI//NF)~~

In addition, every time one of the limited number of NSA analysts permitted to search the archived data carries out such a search, a record will be made, and the analyst's login and IP address, and the date, time and details of the search will be automatically logged to ensure an auditing capability. NSA Declaration ¶ 16. The NSA's OGC will monitor both the designation of individuals with access to the archived data and the functioning of this automatic logging

capability. *Id.* The NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate Oversight Compliance Office will periodically review this program. *Id.* ¶ 22. At least every ninety days, the Department of Justice will review a sample of NSA's justifications for querying the archived data. *Id.* ¶ 19. The Director of the NSA himself will, in coordination with the Attorney General, inform the Congressional Intelligence Oversight Committees of the Court's decision to issue the Order. *Id.* ¶ 23. ~~(TS//SI//NF)~~

Third, the collected metadata will not be kept online (that is, accessible for queries by cleared analysts) indefinitely. The NSA has determined that for operational reasons it is important to retain the metadata online for five years, at which time it will be destroyed. *Id.* ¶ 20. The U.S. Government has a strong operational interest in retaining data online for five years to determine [redacted] contacts associated with newly-discovered "seed" telephone numbers. *Id.* In addition, moving data off-line requires significant resources, raises the possibility of corruption and loss of data, and would incur probable delays in moving data back online for it to be accessed when needed. *See generally* [redacted] Order (Feb. 28, 2006). ~~(TS//SI//NF)~~

Finally, when and if the Government seeks an extension of any order from the Court requiring the production of business records containing telephony metadata, it will provide a report about the queries that have been made and the application of the reasonable articulable suspicion standard for determining that queried telephone numbers were terrorist related. NSA Declaration ¶ 24. ~~(TS//SI//NF)~~

II. The Application Fully Complies with the First and Fourth Amendments to the Constitution. (U)

There is, of course, no constitutionally protected privacy interest in the information contained in call detail records, or telephony metadata. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court squarely rejected the view that an individual can have a Fourth Amendment protected "legitimate expectation of privacy regarding the numbers he dialed on his phone." *Smith*, 442 U.S. at 742 (internal quotation marks omitted). The Court concluded that telephone subscribers know that they must convey the numbers they wish to call to the telephone company for the company to complete their calls. Thus, they cannot claim "any general expectation that the numbers they dial will remain secret." *Id.* at 743; *see also id.* at 744 (telephone users who "voluntarily convey[]" information to the phone company "in the ordinary course" of making a call "assum[e] the risk" that this information will be passed on to the government or others) (internal quotation marks omitted). Even if a subscriber could somehow claim a subjective intention to keep the numbers he dialed secret, the Court found that this was not an expectation that society would recognize as reasonable. To the contrary, the situation fell squarely into the line of cases in which the Court had ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44.[12] Although the telephony metadata that would be obtained here would include not only telephone numbers dialed, but also the length and time of the calls and other routing information, there is no reasonable expectation that such information, which is routinely collected by the telephone companies for billing and fraud detection purposes, is private. The information contained in the

[12] *See also United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a *third* party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). (U)

call detail records [redacted] in no way resembles the substantive contents of telephone communications that are protected by the Fourth Amendment. *See Katz v. United States*, 389 U.S. 347 (1967). (~~S~~)

Moreover, as this Court has previously found, because of the absence of a reasonable expectation of privacy in metadata, the large number of individuals whose telephony metadata will be obtained "is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." [redacted] at 63. Nor would the derivative use of the archived metadata through contact chaining or [redacted] be prohibited by the Fourth Amendment. *See id.* at 63-66; *United States v. Calandra*, 414 U.S. 338, 354 (1974) (Grand jury "[q]uestions based on illegally obtained evidence are only a derivative use of the product of a past unlawful search and seizure. They work no new Fourth Amendment wrong."). (~~TS//SI//NF~~)

The proposed business records request is also consistent with the First Amendment. Good faith law enforcement investigation and data-gathering activities using legitimate investigative techniques do not violate the First Amendment, at least where they do not violate the Fourth Amendment. *See Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1064 (D.C. Cir. 1978); *see also* [redacted] at 66 ("The weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as part of a good-faith criminal investigation."); *cf. Laird* v. *Tatum*, 408 U.S. 1, 10, 13 (1972) (the "subjective 'chill'" stemming from "the mere existence, without more, of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose" does not constitute a

cognizable injury). As this Court recognized in the context of the Government's application to collect e-mail metadata in bulk,

> the proposed collection of meta data is not for ordinary law enforcement purposes, but in furtherance of the compelling national interest of identifying and tracking [redacted] operatives and ultimately of thwarting terrorist attacks. The overarching investigative effort against [redacted] is not aimed at curtailing First Amendment activities and satisfies the "good faith" requirement . . . .

Id. at 68. (~~TS//SI//NF~~)

Nonetheless, we are mindful of this Court's admonition that, because "the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgment of First Amendment rights of innocent persons . . . special restrictions on the accessing, retention, and dissemination of such information are necessary to guard against such misuse." *Id.* The strict restrictions proposed here on access to, and processing and dissemination of, the data are almost identical to those imposed by this Court in [redacted] *Compare* NSA Declaration ¶¶ 13-24 *with* [redacted] at 82-87.[13] In addition, the Department of Justice would review a sample of NSA's justifications for querying the archived data at least every ninety days. (~~TS//SI//NF~~)

[13] One minor difference is that for operational reasons the NSA seeks to retain the telephony metadata collected online for five, rather than four and a half, years. *Compare* NSA Declaration ¶ 20 *with* [redacted] Order [redacted] (approving retention online of the bulk e-mail metadata for four and a half years). (TS//SI//NF)

CONCLUSION (U)

For the foregoing reasons, the Court should grant the requested Order. (U)

Respectfully submitted,

Dated: May 23, 2006

ALBERTO R. GONZALES
Attorney General

STEVEN G. BRADBURY
Acting Assistant Attorney General,
Office of Legal Counsel

JAMES A. BAKER
Counsel for Intelligence Policy

JOHN A. EISENBERG
Deputy Assistant Attorney General,
Office of Legal Counsel
[redacted]

U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

All redactions taken in accordance with one or more of the following FOIA exemptions and statutes:
(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)
(b) (3) - 18 USC 798

~~SECRET~~

848

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES
SIGNALS INTELLIGENCE
DIRECTIVE

18

27 July 1993

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

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

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

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 ~~(Attention:~~ [redacted] 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~~

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

28 October 1997

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE (USSID) 18

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

CHANGE 1

LETTER OF PROMULGATION

~~(FOUO)~~ This hard copy change provides replacement pages for your copy of USSID 18, dated 27 July 1993.

Actions: 1. *Change references to "P05" to read "P02" in paragraphs 5.4.d.(3), 7.1. (last line), 7.2.c.(6) (lines 3 and 5), 7.3.c.(1) (lines 2 and 3), 7.5 ., 8.3.b., and 8.4.b. in the basic USSID 18.*

2. From your copy of USSID 18 remove and destroy pages A–1/1 through A–1/8.

3. Insert new pages A–1/1 through A–1/9 (replacement of pages in above action). These pages update the USSID to reflect current changes in standard minimization procedures for NSA electronic surveillances.

4. In the last paragraph of the Letter of Promulgation change to read: "Questions and comments concerning this USSID should be addressed to the Office of General Counsel, NSA/CSS, NSTS 963–3121 or [redacted]

5. On the Table of Contents (page iv), change the title of Appendix 1 to Annex A to read "Standardized Minimization Procedures For NSA Electronic Surveillances".

FOR THE EXECUTIVE AGENT:

[redacted]
USSID Manager

NOTE: DESTROY THIS PAGE AFTER POSTING THE ENCLOSED CHANGE MATERIAL. RETAIN THE ORIGINAL LETTER OF PROMULGATION WITH USSID 18.

~~FOR OFFICIAL USE ONLY~~

CHANGE REGISTER

CHANGE			ENTERED	
No.	Date	Authority (Msg Cite/DTG, Hard Copy (HC))	Date	By

TABLE OF CONTENTS

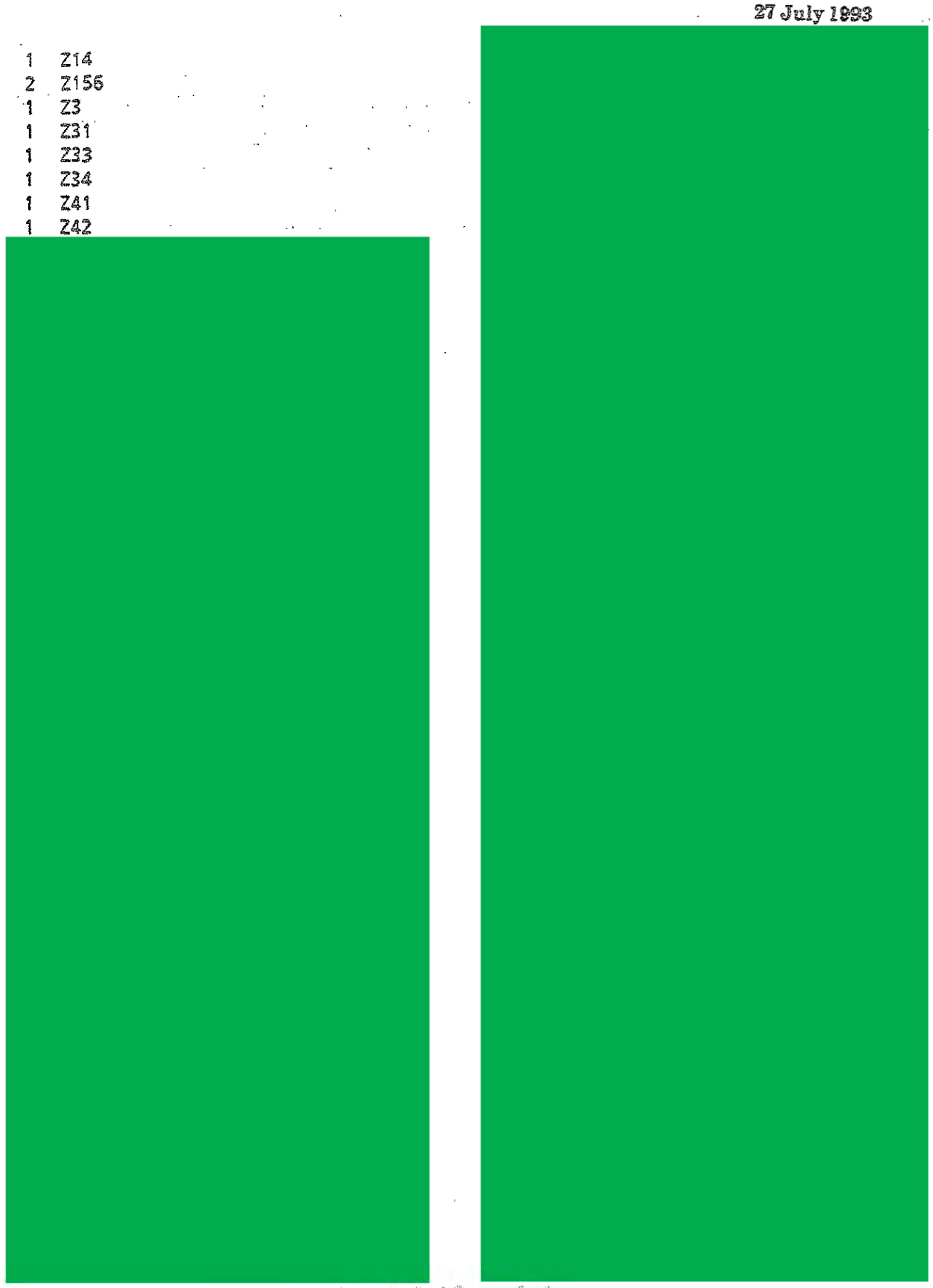
DISTRIBUTION

2	A041
2	A055
3	A1095
8	A111
1	A112
4	A113
2	A114
2	A12
1	A13
1	A131
3	A132
4	A133
4	A134
1	A135
4	A136
2	A14
1	A153
1	A209
2	A21
1	A22
2	A23
1	A405
2	A42
2	A609
1	A62
1	A63
1	A64
1	A641
1	A65
6	A67
1	A72
1	B04
3	B05
1	B109
2	B209
5	B21
1	B22
2	B23
1	B26
1	B3094
1	B3095
3	B31
4	B312
6	B32
12	B33
5	B34
10	B35
1	B351/[redacted]
1	B409
14	B41
10	B42
4	B43
7	B44
3	B45
1	B461
1	B5094
6	B521
1	B522
1	B54
1	B5423
1	B55
1	B56
4	B609
1	B61
1	B63
1	B646
2	B709
2	B7095
26	B71
3	B72
15	B73
4	B75
1	CSPO
1	CMATT
12	D1
6	D2
1	D3
1	DCN
1	E
1	E09
1	E1
1	E11
1	E31
3	E32
1	E32/B
1	E32/G
3	E42
1	E54

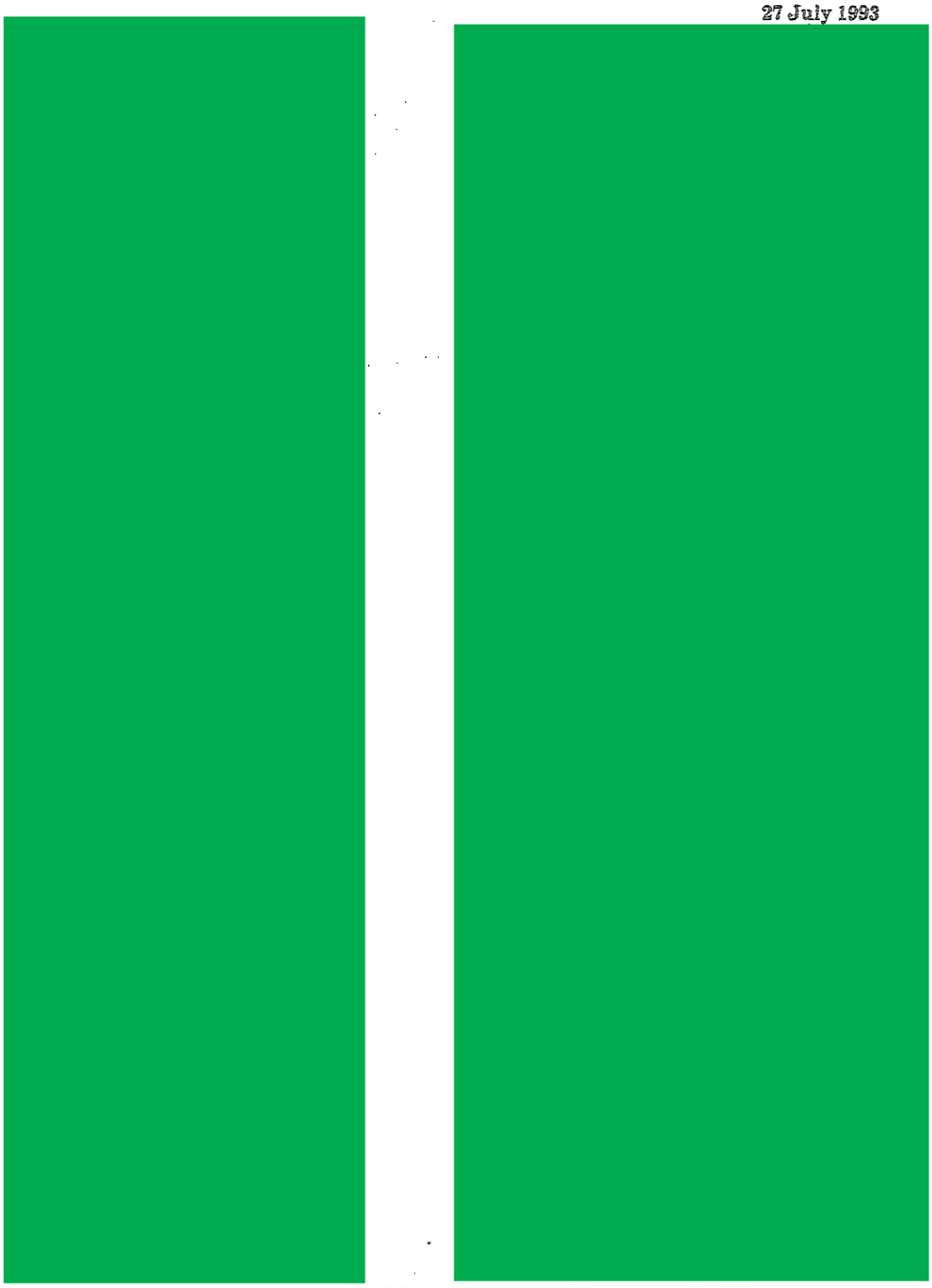
TOTAL COPIES 1193

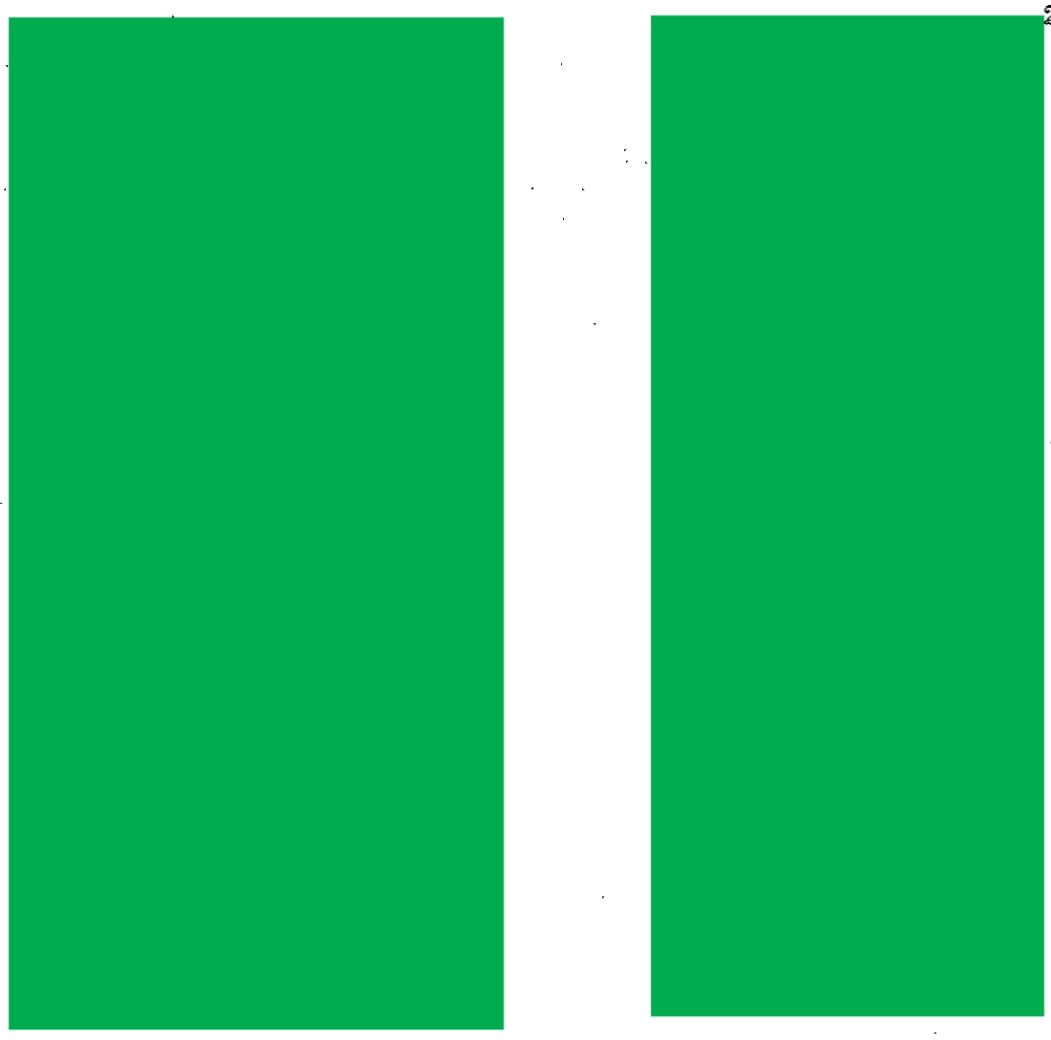
1	G01
2	G111
3	G112
1	G112 [redacted]
1	G133
1	G133C
2	G223
2	G23
1	G24 (SLO)
1	G27
2	G31
1	G33
1	G35
1	G36
1	G364
2	G36N
2	G41
1	G412
1	G42
1	G421
1	G44
1	G45
2	G5 NSOC (ASGC)
1	G5 NSOC (BSGC)
1	G5 NSOC (NALA)
1	G5 NSOC (NMJIC)
1	G5 NSOC (SRO)
1	G5 NSOC (WSGC)
1	G509
1	G561
1	G562
1	G564
1	G58
1	G71
1	I11
2	I2
1	J23
1	J25
1	J34
1	K1
1	K13
2	K2
1	K34
1	K4
1	K41
2	K42
1	K43
3	K51
1	K52 [redacted]
1	K609
1	K609
1	L091
1	LAO
1	M091
1	M31
1	M5
1	M51
1	M52
1	N22
1	N252
1	N511
1	N5209
1	P042
1	P043
1	P0433
150	P0442 (STOCK)
1	P05
6	P052
3	P0522
1	P0533
1	P0541
1	P05A
1	Q109
1	Q32
1	S9
1	T09
2	T093
1	V09
1	W04
1	W05
1	W109
1	W15
1	W16
1	W17
1	W174
1	W18
1	W2091
1	W21
1	W232
1	W27
1	W309
2	W31
1	W32
2	W33
1	W335 (SOC)
1	W341
3	W4
1	X41
1	Z03
1	Z09
5	Z109
1	Z11

1 Z14
2 Z156
1 Z3
1 Z31
1 Z33
1 Z34
1 Z41
1 Z42



[redacted]





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: ~~P05~~ 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, other than [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. ~~(C-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 P8S. P02

7.2. ~~(C 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 ~~P05~~ P03 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to ~~P05~~ P03 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. ~~(C 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, ~~P05~~ FO, the Deputy Chief, ~~P05~~ FO, 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.

(2) 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 ~~P05~~ FO2 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 ~~P05~~ 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: ~~P05~~ 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. ~~(C)~~ 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. ~~(C)~~ 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.

ANNEX A

PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) The Foreign Intelligence Surveillance Act (the Act) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. A complete copy of the Act is found at Annex B to NSA/CSS Directive 10-30. The Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States, all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy. The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General.

SECTION 2 - GENERAL

2.1. (U) Procedures and standards for securing Court orders or Attorney General certifications to conduct electronic surveillances are set forth in the Act. Requests for such orders or certifications should be forwarded by the appropriate Key Component through the NSA General Counsel to the Director, NSA/Chief, CSS and should be accompanied by a statement of the facts and circumstances justifying a belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which the surveillance will be directed are being used, or are about to be used, by that foreign power or agent. If the proposed surveillance meets the requirements of the Act and the Director approves the proposal, attorneys in the Office of the General Counsel will draw the necessary court application or request for Attorney General certification.

SECTION 3 - MINIMIZATION PROCEDURES

3.1. ~~(S-CCO)~~ Surveillances authorized by the Act are required to be carried out in accordance with the Act and pursuant to the court order or Attorney General certification authorizing that particular surveillance. In some cases, the court orders are tailored to address particular problems, and in those instances the NSA attorney will advise the appropriate NSA offices of the terms of the court's orders. In most cases, however, the court order will incorporate without any changes the standardized minimization procedures set forth in Appendix 1.

SECTION 4 - RESPONSIBILITIES

4.1. (U) The General Counsel will review all requests to conduct electronic surveillances as defined by the Act, prepare all applications and materials required by the Act, and provide pertinent legal advice and assistance to all elements of the United States SIGINT System.

4.2. (U) The Inspector General will conduct regular inspections and oversight of all SIGINT activities to assure compliance with this Directive.

4.3. (U) All SIGINT managers and supervisors with responsibilities relating to the Act will ensure that they and their personnel are thoroughly familiar with the Act, its implementing procedures, and any court orders or Attorney General certifications pertinent to their mission. Personnel with duties related to the Act will consult the General Counsel's office for any required legal advice and assistance or training of newly assigned personnel. Appropriate records will be maintained demonstrating compliance with the terms of all court orders and Attorney General certifications, and any discrepancies in that regard will be promptly reported to the offices of the General Counsel and Inspector General.

APPENDIX 1

Standard Minimization Procedures for NSA Electronic Surveillances

Table of Contents

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, DC

STANDARDIZED MINIMIZATION

PROCEDURES FOR NSA ELECTRONIC SURVEILLANCES

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978 (hereinafter "the Act"), the following procedures have been adopted by the Attorney General and shall be followed by the NSA in implementing this electronic surveillance: (U)

SECTION 1 – APPLICABILITY AND SCOPE (U)

These procedures apply to the acquisition, retention, use, and dissemination of non–publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of the Act. These procedures also apply to non–United States persons where specifically indicated. (U)

SECTION 2 – DEFINITIONS (U)

In addition to the definitions in Section 101 of the Act, the following definitions shall apply to these procedures:

(a) Acquisition means the collection by NSA through electronic means of a nonpublic communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization shall be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among:

(1) foreign powers;

(2) officers and employees of foreign powers; or

(3) a foreign power and officers or employees of a foreign power.

All other communications are domestic communications. (S–CCO)

(f) Identification of a United States person means the name, unique title, address, or other personal identifier of a United States person in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S-CCO)~~

(g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

(h) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(i) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S-CCO)~~

(j) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

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

(2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with Title 8, United States Code, Section 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

(4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

SECTION 3 – ACQUISITION AND PROCESSING – GENERAL (U)

(a) Acquisition (U)

The acquisition of information by electronic surveillance shall be made in accordance with the certification of the Attorney General or the court order authorizing such surveillance and conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance. ~~(S-CCO)~~

(b) Verification (U)

At the initiation of the electronic surveillance, the NSA or the Federal Bureau of Investigation, if providing operational support, shall verify that the communication lines or telephone numbers being targeted are the lines or numbers of the target authorized by court order or Attorney General certification. Thereafter, collection personnel will monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance. ~~(S-CCO)~~

(c) Monitoring, Recording, and Processing (U)

(1) Electronic surveillance of the target may be monitored contemporaneously, recorded automatically, or both. (U)

(2) Personnel who monitor the electronic surveillance shall exercise reasonable judgement in determining whether particular information acquired must be minimized and shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either as clearly not relevant to the authorized purpose of the surveillance (e.g., the communication does not contain foreign intelligence information) or as containing evidence of a crime which may be disseminated under these procedures. ~~(S-CCO)~~

(3) Communications of or concerning United States persons that may be related to the authorized purpose of the surveillance may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, and 6 of these procedures. ~~(C)~~

(4) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S-CCO)~~

(5) Each communication shall be reviewed to determine whether it is a domestic or foreign communication to or from the targeted premises and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5 and 6 of these procedures. ~~(S-CCO)~~

(6) Magnetic tapes or other storage media containing foreign communications may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, shall not include United States person names or identifiers and shall be limited to those selection terms reasonably likely to identify [redacted] that are authorized for intentional collection under Executive Order 12333 implementing procedures. ~~(S-CCO)~~

(7) Further processing, retention and dissemination of foreign communications shall be made in accordance with Sections 4, 6, and 7, as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications shall be made in accordance with Sections 4 and 5 below. ~~(S-CCO)~~

(d) U.S. Persons Employed by the Foreign Power ~~(C)~~

Communications of or concerning United States persons employed by a foreign power may be used and retained as otherwise provided in these procedures except that:

(1) Such United States persons shall not be identified in connection with any communication that the person places or receives on behalf of another unless the identification is permitted under Section 6 of these procedures; and

(2) personal communications of United States persons that could not be foreign intelligence may only be retained, used, or disseminated in accordance with Section 5 of these procedures. ~~(S-CCO)~~

(e) Destruction of Raw Data ~~(C)~~

Communications and other information, including that reduced to graphic or "hard copy" form such as [redacted] shall be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet such retention standards and that are known to contain communications of or concerning United States persons shall be promptly destroyed. ~~(S-CCO)~~

(f) Non–pertinent Communications (U)

(1) Communications determined to fall within established categories of non–pertinent communications, such as those set forth in subparagraph (6) of this section, should not be retained unless they contain information that may be disseminated under Sections 5, 6, or 7 below. (U)

(2) Monitors may listen to all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be disseminated under Sections 5, 6, or 7 below. ~~(S-CCO)~~

(3) Communications of United States persons will be analyzed to establish categories of communications that are not pertinent to the authorized purpose of the surveillance. (U)

(4) These categories should be established after a reasonable period of monitoring the communications of the targets. (U)

(5) Information that appears to be foreign intelligence may be retained even if it is acquired as a part of a communication falling within a category that is generally non–pertinent. ~~(S-CCO)~~

(6) Categories of non–pertinent communications which may be applied in these surveillance include:

(i) Calls to and from United States Government officials;

(ii) Calls to and from children;

(iii) Calls to and from students for information to aid them in academic endeavors;

(iv) Calls between family members; and

(v) Calls relating solely to personal services, such as food orders, transportation, etc. ~~(S-CCO)~~

(g) Change in Target's Location or Status ~~(S-CCO)~~

(1) During periods of known extended absence by a targeted agent of a foreign power from premises under surveillance, only communications to which the target is a party may be retained and disseminated. ~~(S-CCO)~~

(2) When there is reason to believe that the target of an electronic surveillance is no longer a foreign power or an agent of a foreign power, or no longer occupies the premises authorized for surveillance, that electronic surveillance shall be immediately terminated, and shall not resume unless subsequently approved under the Act. When any person involved in collection or processing of an electronic surveillance being conducted pursuant to the Act becomes aware of information tending to indicate a material change in the status or location of a target, the person shall immediately ensure that the NSA's Office of General Counsel is also made aware of such information. ~~(S-CCO)~~

SECTION 4 – ACQUISITION AND PROCESSING – SPECIAL PROCEDURES (U)

(a) Collection Against Residential Premises ~~(S-CCO)~~

(1) An electronic surveillance directed against premises located in the United States and used for residential purposes shall be conducted by technical means designed to limit the information acquired to communications that have one communicant outside the United States; [redacted] The technical means employed shall consist of [redacted]

[redacted] equipment or equipment capable of identifying international [redacted] or other particular international communications known to be used by the targeted foreign power and its agents. Communications to or from the target residential premises that are processed through a [redacted] of a foreign power or agent of a foreign power located in a foreign country, or on the foreign country or foreign city telephone direct dialing codes (area codes) for the areas in which such foreign powers or agents are located. ~~(S-CCO)~~

(2) [redacted] (S-CCO)

(3) Domestic communications that are incidentally acquired during collection against residential premises shall be handled under Section 5 of these procedures. ~~(S-CCO)~~

(b) Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication shall be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the tape containing that conversation will be placed under seal and the Department of Justice, Office of Intelligence Policy and Review, shall be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. ~~(S-CCO)~~

SECTION 5 – DOMESTIC COMMUNICATIONS (U)

(a) Dissemination (U)

Communications identified as domestic communications shall be promptly destroyed, except that:

(1) domestic communications that are reasonably believed to contain foreign intelligence information shall be disseminated to the Federal Bureau of Investigation (including United States person identities) for possible further dissemination by the Federal Bureau of Investigation in accordance with its minimization procedures;

(2) domestic communications that do not contain foreign intelligence information, but that are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed, shall be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General; and

(3) domestic communications that are reasonably believed to contain technical data base information, as defined in Section 2(i), may be disseminated to the Federal Bureau of Investigation and to other elements of the U.S. SIGINT system. ~~(S-CCO)~~

(b) Retention (U)

(1) Domestic communications disseminated to Federal law enforcement agencies may be retained by the NSA for a reasonable period of time, not to exceed six months (or any shorter period set by court order), to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes. ~~(S-CCO)~~

(2) Domestic communications reasonably believed to contain technical data base information 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. ~~(S-CCO)~~

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S-CCO)~~

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements. ~~(S-CCO)~~

SECTION 6 – FOREIGN COMMUNICATIONS OF OR CONCERNING UNITED STATES PERSONS (U)

(a) Retention (U)

Foreign communications of or concerning United States persons acquired by the NSA in the course of an electronic surveillance subject to these procedures may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted 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.

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S-CCO)~~

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) the communication or information indicates that the United States person may be:

(A) an agent of a foreign power;

(B) a foreign power as defined in Section 101(a)(4) or (6) of the Act;

(C) residing outside the United States and holding an official position in the government or military forces of a foreign power;

(D) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(E) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material.

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information; but only after the agency that originated the information certifies that it is properly classified;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to Section 105 of the Act and the communication may relate to the foreign intelligence purpose of the surveillance;

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General. (U)

SECTION 7 – OTHER FOREIGN COMMUNICATIONS (U)

Foreign communications of or concerning a non–United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

SECTION 8 – COLLABORATION WITH FOREIGN GOVERNMENTS ~~(S-CCO)~~

(a) The sharing or exchange of foreign communications governed by these procedures with signals intelligence authorities of collaborating foreign governments (Second Parties) may be undertaken by the NSA only with the written assurance of the Second Party that the use of those foreign communications will be subject to the retention and dissemination provisions of these procedures. ~~(S-CCO)~~

(b) Domestic communications and communications to or from United States persons shall not be shared with Second Parties. ~~(S-CCO)~~

(c) Foreign plain text communications may be shared with Second Parties if they are first reviewed by NSA analysts, who shall remove references to United States persons that are not necessary to understand or assess the foreign intelligence information contained therein. ~~(S-CCO)~~

(d) Foreign enciphered or encoded communications may be shared with Second Parties without such prior review, provided that at least annually a representative sampling of those shared communications that can be deciphered or decoded is reviewed by the NSA to ensure that any references therein to United States persons are necessary to understand or assess the foreign intelligence information being dissemi-

nated. Corrective measures with respect to each target or line shall be undertaken as necessary to maintain compliance with the above dissemination standard. The results of each review shall be made available to the Attorney General or a designee. ~~(S-CCO)~~

Approved by Attorney General Janet Reno on 1 July 1997

ANNEX B

OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U)

SECTION 1 - GENERAL

1.1. (U) In accordance with the provisions of Section 2.6 of E.O. 12333, and the NSA/FBI Memorandum of Understanding of 25 November 1980, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the FBI in the conduct of its lawful functions. When requesting such assistance, the FBI will certify to the General Counsel of NSA that such equipment or technical knowledge is necessary to the accomplishment of one or more of the FBI's lawful functions.

1.2. (U) NSA may also provide expert personnel to assist FBI personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence. When requesting the assistance of expert personnel, the FBI will certify to the General Counsel that such assistance is necessary to collect foreign intelligence and that the approval of the Attorney General (and, when necessary, a warrant from a court of competent jurisdiction) has been obtained.

SECTION 2 - CONTROL

2.1. (U) No operational assistance as discussed in Section 1 shall be provided without the express permission of the Director, NSA/Chief, CSS, Deputy Director, NSA, the Deputy Director for Operations, or the Deputy Director for Technology and Systems. The Deputy Director for Operations and the Deputy Director for Technology and Systems may approve requests for such assistance only with the concurrence of the General Counsel.

ANNEX C

SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U)

SECTION 1 - POLICY

1.1. ~~(C)~~ Signals Intelligence support to U.S. and Allied military exercise command authorities is provided for in USSID 56 and DoD Directive 5200.17 (M-2). Joint Chiefs of Staff Memorandum MJCS111-88, 18 August 1988, and USSID 4, 16 December, 1988, establish doctrine and procedures for providing signals intelligence support to military commanders. The procedures in this Annex provide policy guidelines for safeguarding the rights of U.S. persons in the conduct of exercise SIGINT support activities.

SECTION 2 - DEFINITIONS

2.1. (U) The term "Military Tactical Communications" means United States and Allied military exercise communications, within the United States and abroad, that are necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

SECTION 3 - PROCEDURES

3.1. ~~(C-CCO)~~ The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S. persons.

a. Collection efforts will be conducted in such a manner as to avoid, to the extent feasible, the intercept of non-exercise-related communications.

b. Military tactical communications may be stored and processed without deletion of references to U.S. persons if the names and communications of the U.S. persons who are exercise participants, whether military, government, or contractor, are contained in, or such communications constitute, exercise-related communications or fictitious communications or information prepared for the exercise.

c. Communications of U.S. persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible, provided that a record describing the signal or frequency user in technical and generic terms may be retained for signal identification and Collection-avoidance purposes. Inadvertently intercepted communications that contain anomalies in enciphered communications that reveal a potential vulnerability to United States communications security should be forwarded to the NSA Deputy Director for Information Systems Security.

d. Dissemination of military exercise communications, exercise reports, or information files derived from such communications shall be limited to those authorities and persons participating in the exercise or conducting reviews and critiques thereof.

ANNEX D

TESTING OF ELECTRONIC EQUIPMENT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) This Annex applies to the testing of electronic equipment that has the capability to intercept communications and other non-public information. Testing includes development, calibration, and evaluation of such equipment, and will be conducted, to the maximum extent practical, without interception or monitoring of U.S. persons.

SECTION 2 - PROCEDURES

2.1. (U) The USSS may test electronic equipment that has the capability to intercept communications and other information subject to the following limitations:

a. To the maximum extent practical, the following should be used:

(1) Laboratory-generated signals,

(2) Communications transmitted between terminals located outside the United States not used by any known U.S. person,

(3) Official government agency communications with the consent of an appropriate official of that agency, or an individual's communications with the consent of that individual,

(4) Public broadcast signals, or

(5) Other communications in which there is no reasonable expectation of privacy (as approved in each instance by the NSA General Counsel).

b. Where it is not practical to test electronic equipment solely against signals described in paragraph 2.1.a., above, testing may be conducted, provided:

(1) the proposed test is coordinated with the NSA General Counsel;

(2) the test is limited in scope and duration to that necessary to determine the capability of the equipment;

(3) no particular person is targeted without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and

(4) the test does not exceed 90 calendar days.

c. Where the test involves communications other than those identified in 2.1 .a. and a test period longer than 90 days is required, the Foreign Intelligence Surveillance Act requires that the test be approved by the Attorney General. Such proposals and plans shall be submitted by USSS elements through the General Counsel, NSA, to the Director, NSA/Chief, CSS for transmission to the Attorney General. The test proposal shall state the requirement for an extended test involving such communications, the nature of the test, the organization that will conduct the test, and the proposed disposition of any signals or communications acquired during the test.

2.2. (U) The content of any communication other than communications between non-U.S. persons outside the United States which are acquired during a test and evaluation shall be:

a. retained and used only for the purpose of determining the capability of the electronic equipment;

b. disclosed only to persons conducting or evaluating the test; and

c. destroyed before or immediately upon completion of the testing.

2.3. (U) The technical parameters of a communication, such as frequency, modulation, and time of activity of acquired electronic signals, may be retained and used for test reporting or collection-avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance, provided such dissemination and use are limited to testing, evaluation, or collection-avoidance purposes.

ANNEX E

SEARCH AND DEVELOPMENT OPERATIONS (U)

SECTION 1 - PROCEDURES

1.1. (U) This Annex provides the procedures for safeguarding the rights of U.S. persons when conducting SIGINT search and development activities.

1.2. ~~(S-CCO)~~ The USSS may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

a. Signals may be collected only for the purpose of identifying those signals that:

(1) may contain information related to the production of foreign intelligence or counterintelligence;

(2) are enciphered or appear to contain secret meaning;

(3) are necessary to assure efficient signals intelligence collection or to avoid the collection of unwanted signals; or,

(4) reveal vulnerabilities of United States communications security.

b. Communications originated or intended for receipt in the United States or originated or intended for receipt by U.S. persons shall be processed in accordance with Section 5 of USSID 18, provided that information necessary for cataloging the constituent elements of the signal environment may be processed and retained if such information does not identify a U.S. person. Information revealing a United States communications security vulnerability may be retained.

c. Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify U.S. persons. Communications equipment nomenclature may be disseminated. Information that reveals a vulnerability to United States communications security may be disseminated to the appropriate communications security authorities.

d. All information obtained in the process of search and development that appears to be of foreign intelligence value may be forwarded to the proper analytic office within NSA for processing and dissemination in accordance with relevant portions of USSID 18.

ANNEX F

ILLICIT COMMUNICATIONS (C)

SECTION 1 - PROCEDURES

1.1. ~~(C)~~ ~~The~~ USSS may collect, retain, process, and disseminate illicit communications without reference to the requirements concerning U.S. persons.

1.2. ~~(C)~~ The term "illicit communications" means a communication transmitted in violation of either the Communications Act of 1934 and regulations issued thereunder or international agreements, which because of its explicit content, message characteristics, or method of transmission, is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not U.S. persons.

ANNEX G

TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT (U)

SECTION 1 - APPLICABILITY

1.1. (U) This Annex applies to all USSS use of SIGINT collection and other surveillance equipment for training purposes.

SECTION 2 - POLICY

2.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment shall be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons or persons in the United States who have not given consent to such interception. Communications and information protected by the Foreign Intelligence Surveillance Act (FISA) (see Annex A) will not be collected for training purposes.

SECTION 3 - PROCEDURES

3.1. (U) The training of USSS personnel in the operation and use of SIGINT collection and other surveillance equipment shall include guidance concerning the requirements and restrictions of the FISA, Executive Order 12333, and USSID 18.

3.2. (U) The use of SIGINT collection and other surveillance equipment for training purposes is subject to the following limitations:

a. To the maximum extent practical, use of such equipment for training purposes shall be directed against otherwise authorized intelligence targets;

b. The contents of private communications of nonconsenting U.S. persons may not be acquired unless the person is an authorized target of electronic surveillance; and

c. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

3.3. (U) The limitations in paragraph 3.2. do not apply in the following instances:

a. Public broadcasts, distress signals, or official United States Government communications may be monitored, provided that, where government agency communications are monitored, the consent of an appropriate official is obtained; and

b. Minimal acquisition of information is permitted as required for calibration purposes.

3.4. (U) Information collected during training that involves authorized intelligence targets may be retained in accordance with Section 6 of USSID 18 and disseminated in accordance with Section 7 of USSID 18. Information other than distress signals collected during training that does not involve authorized intelligence targets or that is acquired inadvertently shall be destroyed as soon as practical or upon completion of the training and may not be disseminated outside the USSS for any purpose. Distress signals should be referred to the DDO.

ANNEX H

CONSENT FORMS (U)

SECTION 1 - PURPOSE

1.1. (U) The forms set forth in this Annex are for use in recording consent by U.S. persons for USSS elements to collect and disseminate foreign communications concerning that person. The first form is consent to collect and disseminate a U.S. person's communications as well as references to that person in foreign communications. The second form is consent to collect and disseminate only references to the U.S. person and does not include communications to or from that person.

1.2. (U) Section 4.1.c. of USSID 18 states that the Director, NSA/Chief, CSS has authority to approve the consensual collection of communications to, from or about U.S. persons. Elements of the USSS proposing to conduct consensual collection should forward a copy of the executed consent form and any pertinent information to the Director, NSA/Chief, CSS for approval.

1.3. (U) The forms provided on the following pages may be reproduced, provided the security classifications (top and bottom) are removed. It is the responsibility of the user to properly reclassify the document in accordance with requisite security guidelines.

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____, hereby consent to the National Security Agency undertaking to seek and disseminate communications to or from or referencing me in foreign communications for the purpose of _____
_____.

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only information that relates to the purpose stated above and is effective for the period _____ to _____.

Signals intelligence reports containing information derived from communications to or from me may only be disseminated to me and to _____. Signals intelligence reports containing information derived from communications referencing me may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12333.

_____
(SIGNATURE)

_____
(TITLE)

_____
(DATE)

USSID 18 ANNEX H
27 July 1993

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____, hereby consent to the National Security Agency undertaking to seek and disseminate references to me in foreign communications for the purpose of _____.

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period _____ to _____.

Signals intelligence reports containing information derived from communications referencing me and related to the purpose stated above may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12333.

_____
(SIGNATURE)

_____
(TITLE)

_____
(DATE)

ANNEX I

FORM FOR CERTIFICATION OF OPENLY ACKNOWLEDGED ENTITIES ~~(S-CCO)~~

The form below should be used for Director approvals for the collection of communications of entities that are openly acknowledged to be directed and controlled by a foreign power as specified in Section 4.1.c.(3) of USSID 18.

DIRECTOR, NSA/CHIEF, CSS

Certification for Openly Acknowledged Entities Under Section 4.A.1.(b) of the Classified Annex to DOD 5240.1R

Certification to the Attorney General:

~~(S-CCO)~~ The Director, NSA, hereby certifies that [redacted] located in the United States and openly acknowledged to be directed and controlled by *(Government X)*, is a new target of collection. The purpose of the surveillance is *(to collect* [redacted] *intelligence regarding Government X)* in accordance with valid intelligence requirements. The surveillance will entail intentional interception or deliberate selection of the target's international communications. Standard minimization procedures will be applied to any information collected that relates to U.S. persons.

_____

Director, NSA/Chief, CSS

Copy to: Deputy Secretary of Defense

ANNEX K

[redacted] (S-CCO)

[redacted]

[redacted]

(S-CCO) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]