

1 BETH S. BRINKMANN  
 Deputy Assistant Attorney General  
 2 DOUGLAS N. LETTER  
 Terrorism Litigation Counsel  
 3 JOSEPH H. HUNT  
 Director, Federal Programs Branch  
 4 VINCENT M. GARVEY  
 Deputy Branch Director  
 5 ANTHONY J. COPPOLINO  
 Special Litigation Counsel  
 6 MARCIA BERMAN  
 Senior Trial Counsel  
 7 PAUL E. AHERN  
 Trial Attorney  
 8 U.S. Department of Justice  
 Civil Division, Federal Programs Branch  
 9 20 Massachusetts Avenue, N.W.  
 Washington, D.C. 20001  
 10 Phone: (202) 514-4782  
 Fax: (202) 616-8460

11 *Attorneys for the Government Defendants*

12  
 13 **UNITED STATES DISTRICT COURT**  
 14 **NORTHERN DISTRICT OF CALIFORNIA**  
 15 **SAN FRANCISCO DIVISION**

16 IN RE NATIONAL SECURITY AGENCY )  
 17 TELECOMMUNICATIONS RECORDS )  
 18 LITIGATION )

**No. M:06-cv-01791-VRW**

**EXHIBIT 2 TO GOVERNMENT  
 DEFENDANTS' MEMORANDUM IN  
 SUPPORT OF RENEWED MOTION  
 TO DISMISS AND FOR  
 SUMMARY JUDGMENT**

19 This Document Relates Solely To:

20 *Shubert et al. v. United States of America et. al.* )  
 21 (Case No. 07-cv-00693-VRW) )  
 22 )  
 23 )  
 24 )

**PUBLIC DECLARATION OF  
 LT. GEN. KEITH B. ALEXANDER,  
 DIRECTOR OF THE  
 NATIONAL SECURITY AGENCY**

Date: December 15, 2009  
 Time: 10:00 a.m.  
 Courtroom: 6, 17<sup>th</sup> Floor  
 Chief Judge Vaughn R. Walker

1 I, Lieutenant General Keith B. Alexander, do hereby state and declare as follows:

2 **I. Introduction**

3  
4 1. I am the Director of the National Security Agency (NSA), an intelligence agency  
5 within the Department of Defense. I am responsible for directing the NSA, overseeing the  
6 operations undertaken to carry out its mission and, by specific charge of the President and the  
7 Director of National Intelligence, protecting NSA activities and intelligence sources and methods.  
8 I have been designated an original TOP SECRET classification authority under Executive Order  
9 No. 12958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Executive Order No. 13292, 68  
10 Fed. Reg. 15315 (Mar. 25, 2003) (reprinted in 3 C.F.R. 2003 Comp. at 196 and at 50 U.S.C.A.  
11 § 435 (Supp. 2009)), and Department of Defense Directive No. 5200.1-R, Information Security  
12 Program Regulation, 32 C.F.R. § 159a.12 (2000).  
13

14 2. The purpose of this declaration is to support an assertion of the military and state  
15 secrets privilege (hereafter "state secrets privilege") by the Director of National Intelligence  
16 (DNI) as the head of the intelligence community, as well as the DNI's assertion of a statutory  
17 privilege under the National Security Act. Specifically, in the course of my official duties, I have  
18 been advised of this litigation and the allegations in the plaintiffs' Amended Complaint. As  
19 described herein, various classified facts related to the plaintiffs' allegations are subject to the  
20 DNI's state secrets privilege assertion. The disclosure of information discussed throughout this  
21 declaration, which relates to NSA intelligence information, activities, sources, methods, and  
22 relationships, reasonably could be expected to cause exceptionally grave damage to the national  
23 security of the United States. In addition, it is my judgment that sensitive state secrets are so  
24 central to the subject matter of the litigation that any attempt to proceed in the case risks the  
25 disclosure of the secrets described herein and exceptionally grave damage to the national security  
26  
27  
28

1 of the United States. Through this declaration, I also hereby invoke and assert the NSA's  
2 statutory privilege set forth in section 6 of the National Security Agency Act of 1959, Public Law  
3 No. 86-36 (codified as a note to 50 U.S.C. § 402) ("NSA Act"), to protect the information related  
4 to NSA activities described below. The statements made herein are based on my personal  
5 knowledge of NSA activities and operations, and on information available to me as Director of  
6 the NSA.  
7

## 8 **II. Summary**

9 3. I have reviewed the Amended Complaint in this case. Plaintiffs allege, in sum,  
10 that, after the 9/11 attacks, the NSA received presidential authorization to engage in surveillance  
11 activities far broader than the publicly acknowledged "Terrorist Surveillance Program" ("TSP"),  
12 which was limited to the interception of specific international communications involving persons  
13 reasonably believed to be associated with al Qaeda and affiliated terrorist organizations.  
14 Plaintiffs allege that the NSA, with the assistance of telecommunications companies, Amended  
15 Compl. ¶¶ 5-8, conducts a "dragnet" surveillance program involving the interception of  
16 "virtually every telephone, internet and/or email communication that has been sent from or  
17 received within the United States since 2001" as part of an alleged Presidentially-authorized  
18 "program" after 9/11, *id.* ¶¶ 1, 4. I cannot disclose on the public record the nature of any NSA  
19 information implicated by the plaintiffs' allegations. However, as described further below, the  
20 disclosure of information related to the NSA's activities, sources and methods implicated by the  
21 plaintiffs' allegations reasonably could be expected to cause exceptionally grave damage to the  
22 national security of the United States and, for this reason, are encompassed by the DNI's state  
23 secrets and statutory privilege assertions, as well as by my own statutory privilege assertion, and  
24 should be protected from disclosure in this case. In addition, it is my judgment that sensitive  
25  
26  
27  
28

1 state secrets are so central to the subject matter of the litigation that any attempt to proceed in the  
2 case risks the disclosure of the classified privileged national security information described  
3 herein and exceptionally grave damage to the national security of the United States.

### 4 **III. Background Information**

#### 5 **A. The National Security Agency**

6  
7 4. The NSA was established by Presidential Directive in 1952 as a separately  
8 organized agency within the Department of Defense. The NSA's foreign intelligence mission  
9 includes the responsibility to collect, process, analyze, produce, and disseminate signals  
10 intelligence (SIGINT) information, of which communications intelligence (COMINT) is a  
11 significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes,  
12 and (c) the support of military operations. *See* Executive Order 12333, § 1.7(c), 46 Fed. Reg.  
13 59941 (Dec. 4, 1981), as amended.<sup>1</sup>

14  
15 5. The NSA's SIGINT responsibilities include establishing and operating an  
16 effective unified organization to conduct SIGINT activities set forth in E.O. No. 12333,  
17 § 1.12(b), as amended. In performing its SIGINT mission, NSA has developed a sophisticated  
18 worldwide SIGINT collection network. The technological infrastructure that supports the NSA's  
19 foreign intelligence information collection network has taken years to develop at a cost of  
20 billions of dollars and untold human effort. It relies on sophisticated collection and processing  
21 technology.  
22

23  
24 6. There are two primary reasons for gathering and analyzing foreign intelligence  
25 information. The first, and most important, is to gain information required to direct U.S.  
26

27  
28 <sup>1</sup> Section 1.7(c) of E.O. 12333, as amended, specifically authorizes the NSA to "Collect  
(including through clandestine means), process, analyze, produce, and disseminate signals  
intelligence information for foreign intelligence and counterintelligence purposes to support  
national and departmental missions."

1 resources as necessary to counter external threats and in support of military operations. The  
2 second reason is to obtain information necessary to the formulation of U.S. foreign policy.  
3 Foreign intelligence information provided by the NSA is thus relevant to a wide range of  
4 important issues, including military order of battle; threat warnings and readiness; arms  
5 proliferation; international terrorism; counter-intelligence; and foreign aspects of international  
6 narcotics trafficking.  
7

8       7. Foreign intelligence produced by COMINT activities is an extremely important  
9 part of the overall foreign intelligence information available to the United States and is often  
10 unobtainable by other means. Public disclosure of either the capability to collect specific  
11 communications or the substance of the information derived from such collection itself can  
12 easily alert targets to the vulnerability of their communications. Disclosure of even a single  
13 communication holds the potential of revealing intelligence collection techniques that are applied  
14 against targets around the world. Once alerted, targets can frustrate COMINT collection by  
15 using different or new encryption techniques, by disseminating disinformation, or by utilizing a  
16 different communications link. Such evasion techniques may inhibit access to the target's  
17 communications and therefore deny the United States access to information crucial to the  
18 defense of the United States both at home and abroad. COMINT is provided special statutory  
19 protection under 18 U.S.C. § 798, which makes it a crime to knowingly disclose to an  
20 unauthorized person classified information "concerning the communication intelligence activities  
21 of the United States or any foreign government."  
22  
23  
24  
25  
26  
27  
28

**B. September 11, 2001 and the al Qaeda Threat**

1  
2 8. On September 11, 2001, the al Qaeda terrorist network launched a set of  
3 coordinated attacks along the East Coast of the United States. Four commercial jetliners, each  
4 carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al  
5 Qaeda operatives. Those operatives targeted the Nation's financial center in New York with two  
6 of the jetliners, which they deliberately flew into the Twin Towers of the World Trade Center.  
7 Al Qaeda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third  
8 jetliner. Al Qaeda operatives were apparently headed toward Washington, D.C. with the fourth  
9 jetliner when passengers struggled with the hijackers and the plane crashed in Shanksville,  
10 Pennsylvania. The intended target of this fourth jetliner was most evidently the White House or  
11 the Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitation  
12 blow to the Government of the United States—to kill the President, the Vice President, or  
13 Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths—  
14 the highest single-day death toll from hostile foreign attacks in the Nation's history. In addition,  
15 these attacks shut down air travel in the United States, disrupted the Nation's financial markets  
16 and government operations, and caused billions of dollars of damage to the economy.

17  
18  
19  
20 9. On September 14, 2001, a national emergency was declared "by reason of the  
21 terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the  
22 continuing and immediate threat of further attacks on the United States." Presidential  
23 Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also  
24 immediately began plans for a military response directed at al Qaeda's training grounds and  
25 havens in Afghanistan. On September 14, 2001, both Houses of Congress passed a Joint  
26 Resolution authorizing the President of the United States "to use all necessary and appropriate  
27  
28

1 force against those nations, organizations, or persons he determines planned, authorized,  
2 committed, or aided the terrorist attacks” of September 11. Authorization for Use of Military  
3 Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001). Congress also expressly  
4 acknowledged that the attacks rendered it “necessary and appropriate” for the United States to  
5 exercise its right “to protect United States citizens both at home and abroad,” and acknowledged  
6 in particular that “the President has authority under the Constitution to take action to deter and  
7 prevent acts of international terrorism against the United States.” *Id.* pmb1.

9 10. Also after the 9/11 attacks, a Military Order was issued stating that the attacks of  
10 September 11 “created a state of armed conflict,” see Military Order by the President § 1(a), 66  
11 Fed. Reg. 57833, 57833 (Nov. 13, 2001), and that al Qaeda terrorists “possess both the capability  
12 and the intention to undertake further terrorist attacks against the United States that, if not  
13 detected and prevented, will cause mass deaths, mass injuries, and massive destruction of  
14 property, and may place at risk the continuity of the operations of the United States  
15 Government,” and concluding that “an extraordinary emergency exists for national defense  
16 purposes,” *id.* § 1(c), (g), 66 Fed. Reg. at 57833-34. Indeed, shortly after the attacks, NATO  
17 took the unprecedented step of invoking article 5 of the North Atlantic Treaty, which provides  
18 that an “armed attack against one or more of [the parties] shall be considered an attack against  
19 them all.” North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246.  
20  
21

22 11. As a result of the unprecedented attacks of September 11, 2001, the United States  
23 found itself immediately propelled into a worldwide war against a network of terrorist groups,  
24 centered on and affiliated with al Qaeda, that possesses the evolving capability and intention of  
25 inflicting further catastrophic attacks on the United States. That war is continuing today, at  
26 home as well as abroad. Moreover, the war against al Qaeda and its allies is a very different kind  
27  
28

1 of war, against a very different enemy, than any other war or enemy the Nation has previously  
2 faced. Al Qaeda and its supporters operate not as a traditional nation-state but as a diffuse,  
3 decentralized global network of individuals, cells, and loosely associated, often disparate groups,  
4 that act sometimes in concert, sometimes independently, and sometimes in the United States, but  
5 always in secret—and their mission is to destroy lives and to disrupt a way of life through  
6 terrorist acts. Al Qaeda works in the shadows; secrecy is essential to al Qaeda's success in  
7 plotting and executing its terrorist attacks.  
8

9 12. After the September 11 attacks, the NSA received presidential authorization and  
10 direction to detect and prevent further terrorist attacks within the United States by intercepting  
11 the content<sup>2</sup> of communications for which there were reasonable grounds to believe that (1) such  
12 communications originated or terminated outside the United States and (2) a party to such  
13 communication was a member or agent of al Qaeda or an affiliated terrorist organization. The  
14 existence of this activity was disclosed by then-President Bush in December 2005 (and  
15 subsequently referred to as the "Terrorist Surveillance Program" or "TSP").<sup>3</sup>  
16  
17

#### 18 **INFORMATION SUBJECT TO PRIVILEGE ASSERTION**

19 13. I understand that the plaintiffs in this lawsuit allege that they are customers of  
20 telecommunications companies, *see* Amended Compl. ¶¶ 5-8, and that the NSA, with the  
21 assistance of telecommunications carriers, has indiscriminately intercepted the content of the  
22

---

23  
24 <sup>2</sup> The term "content" is used herein to refer to the substance, meaning, or purport of a  
communication, as defined in 18 U.S.C. § 2510(8).

25  
26 <sup>3</sup> On January 17, 2007, the Government made public the general facts that new orders of  
the Foreign Intelligence Surveillance Court had been issued that authorized the Government to  
27 target for collection international communications into or out of the United States where there is  
probable cause to believe that one of the communicants is a member or agent of al Qaeda or an  
28 associated terrorist organization; that, as a result of these orders, any electronic surveillance that  
had been occurring as part of the TSP was then being conducted subject to the approval of the  
FISA Court; and that, under these circumstances, the TSP was not reauthorized.

1 communications of millions of ordinary Americans as part an alleged presidentially authorized  
2 “Program” after 9/11. *See, e.g.* Amended Compl. ¶¶ 1-4; 47-96. Plaintiffs specifically allege  
3 that, pursuant to the alleged Program, the NSA continues to acquire the content of virtually all of  
4 the phone calls, emails, instant messages, text messages, web and other communications, both  
5 international and domestic, of practically every American, including the plaintiffs. *See, e.g.,*  
6 Amended Compl. ¶¶ 1-4. Plaintiffs also appear to allege that the NSA is collecting “call data,”  
7 again presumably including information concerning the plaintiffs’ communications. *See id.* ¶ 58.

9 14. In general and unclassified terms, the following categories of information are  
10 subject to the DNI’s assertion of the state secrets privilege and statutory privilege under the  
11 National Security Act, as well as my assertion of the NSA privilege:

- 12
- 13 A. Information that may tend to confirm or deny whether the  
14 plaintiffs have been subject to any alleged NSA intelligence  
15 activity that may be at issue in this matter; and
  - 16 B. Any information concerning NSA intelligence activities,  
17 sources, or methods that may relate to or be necessary to  
18 adjudicate plaintiffs’ allegations, including allegations that  
19 the NSA, with the assistance of telecommunications  
20 carriers, indiscriminately intercepts the content of  
21 communications and also, to the extent applicable to  
22 plaintiffs’ claim, the communications records of millions of  
23 Americans as part of an alleged “Program” authorized by  
24 the President after 9/11. *See, e.g.,* Amended Compl. ¶¶ 1-8,  
25 58.

26 The scope of this assertion includes but is not limited to:

- 27 (i) Information concerning the scope and operation  
28 of the now inoperative “Terrorist Surveillance Program”  
29 (“TSP”) regarding the interception of the content of certain  
30 one-end international communications reasonably believed  
31 to involve a member or agent of al-Qaeda or an affiliated  
32 terrorist organization, and any other information related to  
33 demonstrating that the NSA does not otherwise engage in  
34 the content surveillance dragnet that the plaintiffs allege;  
35 and

1 (ii) Any other information concerning NSA  
2 intelligence activities, sources, or methods that would be  
3 necessary to adjudicate the plaintiffs' claims, including, to  
4 the extent applicable, information that would tend to  
5 confirm or deny whether or not the NSA obtained from  
6 telecommunications companies communication  
7 transactional records; and

8 (iii) Information that may tend to confirm or deny  
9 whether any telecommunications carrier has provided  
10 assistance to the NSA in connection with any alleged  
11 activity.

12 **INFORMATION SUBJECT TO PRIVILEGE AND HARM OF DISCLOSURE**

13 15. As set forth in my classified declaration submitted for the Court's *in camera, ex*  
14 *parte* review, disclosure of information in the foregoing categories would cause exceptionally  
15 grave harm to national security. I briefly summarize the harms at issue below.

16 **A. Information That May Tend to Confirm or Deny Whether the Plaintiffs Have Been**  
17 **Subject to Any Alleged NSA Activities**

18 16. The first major category of information as to which I am supporting the DNI's  
19 assertion of privilege, and asserting the NSA's own statutory privilege, concerns information as  
20 to whether particular individuals, including the named plaintiffs in this lawsuit, have been  
21 subject to alleged NSA intelligence activities. As set forth below and in my classified  
22 declaration for *in camera, ex parte* review, disclosure of such information would cause  
23 exceptionally grave harm to the national security.

24 17. As a matter of course, the NSA cannot publicly confirm or deny whether any  
25 individual is subject to surveillance activities because to do so would tend to reveal actual  
26 targets. For example, if the NSA were to confirm in this case and others that specific individuals  
27 are not targets of surveillance, but later refuse to comment (as it would have to) in a case  
28 involving an actual target, a person could easily deduce by comparing such responses that the

1 person in the latter case is a target. The harm of revealing targets of foreign intelligence  
2 surveillance should be obvious. If an individual knows or suspects he is a target of U.S.  
3 intelligence activities, he would naturally tend to alter his behavior to take new precautions  
4 against surveillance. In addition, revealing who is not a target would indicate who has avoided  
5 surveillance and what may be a secure channel for communication. Such information could lead  
6 a person, secure in the knowledge that he is not under surveillance, to help a hostile foreign  
7 adversary convey information; alternatively, such a person may be unwittingly utilized or even  
8 forced to convey information through a secure channel. Revealing which channels are free from  
9 surveillance and which are not would also reveal sensitive intelligence methods and thereby  
10 could help any adversary evade detection and capitalize on limitations in NSA's capabilities.  
11

12  
13 **B. Information Related to NSA Activities, Sources, or Methods Implicated by the  
14 Plaintiffs' Allegations and the Harm to National Security of Its Disclosure**

15 **1. Plaintiffs' Allegations of a Communications Dragnet**

16 18. I am also supporting the DNI's assertion of privilege and asserting the NSA's  
17 statutory privilege over any other facts concerning NSA intelligence activities, sources, or  
18 methods that may relate to or be necessary to adjudicate the plaintiffs' claims and allegations,  
19 including that (i) the NSA is indiscriminately intercepting the content of communications of  
20 millions of ordinary Americans, *see, e.g.*, Amended Compl. ¶¶ 1-4, and (ii) to the extent relevant  
21 to this action, that the NSA is collecting the "call data" of people in the United States with the  
22 assistance of telecommunications carriers, presumably including information concerning the  
23 plaintiffs' communications. *See, e.g., id.* ¶¶ 5-8, 58. As described above, the scope of the  
24 government's privilege assertion includes but is not limited to: (1) facts concerning the operation  
25 of the now inoperative Terrorist Surveillance Program and any other NSA activities needed to  
26 demonstrate that the TSP was limited to the interception of the content of one-end foreign  
27  
28

1 communications reasonably believed to involve a member or agent of al Qaeda or an affiliated  
2 terrorist organization and that the NSA does not otherwise conduct a dragnet of content  
3 surveillance as the plaintiffs allege; and (2) information concerning whether or not the NSA  
4 obtains transactional communications records from telecommunications companies. As set forth  
5 below, the disclosure of such information would cause exceptionally grave harm to national  
6 security.

7  
8 **(a) Information Related to the Terrorist Surveillance Program**

9 19. After the existence of the TSP was officially acknowledged in December 2005,  
10 the Government stated that the NSA's collection of the content of communications under the  
11 TSP was directed at international communications in which a participant was reasonably  
12 believed to be associated with al Qaeda or an affiliated organization. Plaintiffs' allegation that  
13 the NSA has undertaken indiscriminate surveillance of the content of millions of  
14 communications sent or received by people inside the United States after 9/11 under the TSP is  
15 therefore false, as I have previously stated in my prior declaration in this action. (See Dkt. 295  
16 ¶ 16 in 06-cv-1791-VRW). But to the extent the NSA must demonstrate that content  
17 surveillance was so limited, and was not plaintiffs' alleged content dragnet, or demonstrate that  
18 the NSA has not otherwise engaged in the alleged content dragnet, highly classified NSA  
19 intelligence sources and methods about the operation of the TSP and NSA intelligence activities  
20 would be subject to disclosure or the risk of disclosure. The disclosure of whether and to what  
21 extent the NSA utilizes certain intelligence sources and methods would reveal to foreign  
22 adversaries the NSA's capabilities, or lack thereof, enabling them to either evade particular  
23 channels of communications that are being monitored, or exploit channels of communications  
24 that are not subject to NSA activities – in either case risking exceptionally grave harm to national  
25  
26  
27  
28

1 security.

2 (b) **Plaintiffs' Allegations Concerning the Collection of Communications**  
3 **Records**

4 20. As noted above, plaintiffs also appear to allege that the NSA is collecting non-  
5 content "call data" of people in the United States, presumably including information concerning  
6 the plaintiffs' communications. *See, e.g.*, Amended Compl. ¶¶ 5-8, 58. Confirmation or denial  
7 of any information concerning whether the NSA collects communication records would also  
8 disclose information about whether or not the NSA utilizes particular intelligence sources and  
9 methods and, thus, the NSA's capabilities or lack thereof, and would cause exceptionally grave  
10 harm to national security.  
11

12 **2. Plaintiffs' Allegations that Telecommunications Companies have Assisted the**  
13 **NSA with the Alleged Activities**

14 21. Finally, I am also supporting the DNI's assertion of privilege, and asserting the  
15 NSA's statutory privilege, over information that may tend to confirm or deny whether or not any  
16 telecommunications provider has assisted the NSA with alleged intelligence activities. Plaintiffs  
17 allege that they are customers of telecommunications carriers that participated in the alleged  
18 surveillance activities that the plaintiffs seek to challenge. Disclosure of any information that  
19 may tend to confirm or deny whether any particular telecommunications carrier assists the NSA  
20 with alleged intelligence activities would cause exceptionally grave harm to national security.  
21

22 \* \* \*

1 22. Any further elaboration on the public record concerning these matters would  
2 reveal information that would cause the very harm that my privilege assertion and the DNI's  
3 privilege assertion are intended to prevent. As noted, my separate classified declaration,  
4 submitted solely for *in camera*, *ex parte* review, provides a more detailed explanation of the  
5 information and harms to national security at issue.  
6

7 **CONCLUSION**

8 23. In sum, I support the DNI's assertion of the state secrets privilege and statutory  
9 privilege to prevent the disclosure of the information described herein and detailed herein. I also  
10 assert a statutory privilege under Section 6 of the National Security Agency Act with respect to  
11 the information described herein that concerns the functions of the NSA. Public disclosure of the  
12 aforementioned intelligence sources, methods and activities could reasonably be expected to  
13 cause exceptionally grave harm to the national security of the United States. Consequently,  
14 because proceedings in this case risk disclosure of privileged and classified intelligence-related  
15 information, I respectfully request that the Court not only protect that information from  
16 disclosure but also dismiss this case to prevent exceptionally grave harm to the national security  
17 of the United States.  
18  
19

20 I declare under penalty of perjury that the foregoing is true and correct.  
21

22  
23 DATE: 30 Oct 09

Keith B. Alexander  
24 KEITH B. ALEXANDER  
25 LTG, USA  
26 Director  
27 National Security Agency  
28