

SECRET

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

\_\_\_\_\_  
IN RE DNI/AG CERTIFICATION 2010-A. )  
\_\_\_\_\_ )

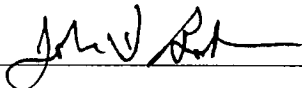
Docket Number 702(i)-10-02

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, “contains all the required elements and that the [amended] targeting and minimization procedures adopted in accordance with [50 U.S.C. § 1881a(d)-(e)] are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States.”

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such certification, as amended, and the use of such procedures, as amended, are approved.

ENTERED this 19<sup>th</sup> day of August 2010.

  
\_\_\_\_\_  
JOHN D. BATES  
Judge, United States Foreign  
Intelligence Surveillance Court

I, Beverly C. Queen, Deputy Clerk,  
FISC, certify that this document  
is a true and correct copy of  
the original.



SECRET

SECRET//ORCON,NOFORN

**CERTIFICATION OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND THE  
ATTORNEY GENERAL PURSUANT TO SUBSECTION 702(g) OF THE FOREIGN  
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

**IN THE MATTER OF FOREIGN GOVERNMENTS, FOREIGN FACTIONS, FOREIGN  
ENTITIES, AND FOREIGN-BASED POLITICAL ORGANIZATIONS**

**DNI/AG 702(g) Certification 2010-A**

Based on the representations made in the supporting affidavits of General Keith B. Alexander, United States Army, Director of the National Security Agency (NSA), Leon E. Panetta, Director, Central Intelligence Agency (CIA), and Robert S. Mueller, III, Director, Federal Bureau of Investigation (FBI), in the above-referenced matter, the Director of National Intelligence and the Attorney General, being duly sworn, hereby certify that: (S//OC,NF)

- (1) there are procedures in place that will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to --
  - a. ensure that an acquisition authorized pursuant to subsection 702(a) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), is limited to targeting persons reasonably believed to be located outside the United States; and
  - b. prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States;
- (2) the minimization procedures with respect to such acquisition --
  - a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and

SECRET//ORCON,NOFORN

Classified by: The Attorney General  
Reason: 1.4(c)  
Declassify on: 15 July 2035

- b. will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court;
- (3) guidelines have been adopted in accordance with subsection 702(f) of the Act to ensure compliance with the limitations in subsection 702(b) of the Act and to ensure that an application for a court order is filed as required by the Act;
- (4) the procedures and guidelines referred to in sub-paragraphs (1), (2), and (3) above are consistent with the requirements of the fourth amendment to the Constitution of the United States;
- (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
- (6) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- (7) the acquisition complies with the limitations in subsection 702(b) of the Act. (S)

As described in the above-referenced affidavit of General Alexander, the foreign intelligence information to be acquired pursuant to this certification concerns foreign powers as defined in 50 U.S.C. § 1801(a)(1) ("foreign governments or any components thereof, whether or not recognized by the United States"); 50 U.S.C. § 1801(a)(2) ("factions of foreign nations, not substantially composed of United States persons"); 50 U.S.C. § 1801(a)(3) ("entities openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments"); 50 U.S.C. § 1801(a)(5) ("foreign-based political organizations, not substantially composed of United States persons"); and 50 U.S.C. § 1801(a)(6) ("entities directed and controlled by a foreign government or governments"). A list of foreign powers satisfying these statutory definitions is attached herewith as Exhibit F. If NSA seeks to acquire foreign intelligence information concerning additional foreign powers as defined in

**SECRET//ORCON,NOFORN**

50 U.S.C. § 1801(a)(1), (2), (3), (5), or (6), NSA may target consistent with this certification non-United States persons reasonably believed to be located outside the United States who possess, are expected to receive, and/or are likely to communicate foreign intelligence information concerning those additional foreign powers, provided that NSA notifies the Attorney General and Director of National Intelligence within five business days of implementing such targeting. Such notification will include a description of the factual basis for NSA's determination that the additional government, faction, entity, or political organization is a foreign power as defined in 50 U.S.C. § 1801(a)(1), (2), (3), (5), or (6). (S//OC,NF)

On the basis of the foregoing, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, as described above, is authorized, and such authorization shall be effective on August 17, 2010, or on the date upon which the Foreign Intelligence Surveillance Court issues an order pursuant to subsection 702(i)(3) of the Act, whichever is later. Such targeting is authorized for a period of one year from the effective date of this authorization. This authorization reauthorizes DNI/AG 702(g) Certification 2009-A ("In the Matter of Foreign Governments, Foreign Factions, Foreign Entities, and Foreign-Based Political Organizations"), which was authorized by the Director of National Intelligence and Attorney General pursuant to section 702(g) of the Act on July 29, 2009. (S//OC,NF)

**Amendment 1 to DNI/AG 702(g) Certifications 2008-A and 2009-A**

Furthermore, in accordance with subsection 702(i)(1)(C) of the Act, the NSA, FBI, and CIA minimization procedures authorized for use under DNI/AG 702(g) Certifications 2008-A and 2009-A are hereby amended. Specifically, the use of the NSA, FBI, and CIA minimization procedures attached herewith as Exhibits B, D, and E, respectively, in connection with foreign

**SECRET//ORCON,NOFORN**

SECRET//ORCON,NOFORN

intelligence information acquired in accordance with DNI/AG 702(g) Certifications 2008-A and 2009-A is authorized.<sup>1</sup> Such authorization shall be effective on August 17, 2010, or on the date upon which the Foreign Intelligence Surveillance Court issues an order concerning these amendments pursuant to subsection 702(i)(3) of the Act, whichever is later. (S//OC,NF)

*---- The remainder of this page intentionally left blank ----*

---

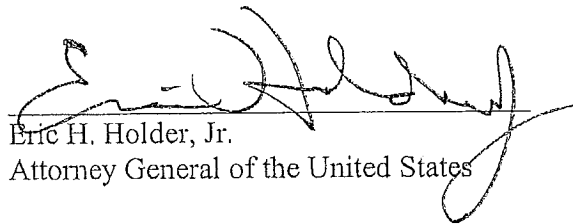
<sup>1</sup> As certified above, these minimization procedures meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act and will be submitted herewith for approval by the Foreign Intelligence Surveillance Court. (S//OC,NF)

SECRET//ORCON,NOFORN

SECRET//ORCON,NOFORN

VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing certification in the Matter of Foreign Governments, Foreign Factions, Foreign Entities, and Foreign-Based Political Organizations, DNI/AG 702(g) Certification 2010-A, are true and correct to the best of my knowledge and belief. I further declare under penalty of perjury that the facts set forth in the foregoing amendments to the minimization procedures to be used in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications 2008-A and 2009-A are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746 on July 15, 2010. (S)



Eric H. Holder, Jr.  
Attorney General of the United States

SECRET//ORCON,NOFORN

SECRET//ORCON,NOFORN

VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing certification in the Matter of Groups Engaged in International Terrorism or Activities in Preparation Therefor, DNI/AG 702(g) Certification 2010-B, are true and correct to the best of my knowledge and belief. I further declare under penalty of perjury that the facts set forth in the foregoing amendment to the minimization procedures to be used in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications 2008-B and 2009-B are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746 on July 15, 2010. (S)



David C. Gompert  
Acting Director of National Intelligence

SECRET//ORCON,NOFORN

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

## EXHIBIT A

**PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING  
NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED  
OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE  
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE  
SURVEILLANCE ACT OF 1978, AS AMENDED**

2009 JUL 22 PM 3:14

CLERK OF COURT

(S) These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

**I. (U) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES**

(S) NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including information concerning the communications facility or facilities used by that person.

(S) NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance to determine what that lead information discloses about the person's location; (2) they conduct research in NSA databases, available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information) to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct technical analyses of the facility or facilities to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

(TS//SI) In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108



overseas, or it will target Internet links that terminate in a foreign country. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

**(S) Lead Information**

(S) When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including the location of the facility or facilities being used by the potential target.

(S) The following are examples of the types of lead information that NSA may examine:

- a) Has the target stated that he is located outside the United States? For example, has NSA or another intelligence agency collected a statement or statements made by the target indicating that he is located outside the United States?
- b) Has a human intelligence source or other source of lead information indicated that the target is located outside the United States?
- c) Does the lead information provided by an intelligence or law enforcement agency of the United States government or an intelligence or law enforcement service of a foreign government indicate that the target is located outside the United States?
- d) Was the lead information about the target found on a hard drive or other medium that was seized in a foreign country?
- e) With whom has the target had direct contact, and what do we know about the location of such persons? For example, if lead information indicates the target is in direct contact with several members of a foreign-based terrorist organization or foreign-based political organization who themselves are located overseas, that may suggest, depending on the totality of the circumstances, that the target is also located overseas.

**(S) Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target**

(S) NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, as well as publicly available information, to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, NSA databases may include a report produced by the Central Intelligence Agency (CIA) with the fact that a known terrorist is using a telephone with a particular number, or detailed information on worldwide telephony numbering plans for wire and wireless telephone systems.

**(S) NSA Technical Analysis of the Facility**

(S) NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

(S) For telephone numbers:

- a) Identify the country code of the telephone number, and determine what it indicates about the person's location.
- b) Review commercially available and NSA telephone numbering databases for indications of the type of telephone being used (e.g. landline, wireless mobile, satellite, etc.), information that may provide an understanding of the location of the target.

(S) For electronic communications accounts/addresses/identifiers:

Review NSA content repositories and Internet communications data repositories (which contain, among other things, Internet communications metadata) for previous Internet activity. This information may contain network layer (e.g., Internet Protocol addresses) or machine identifier (e.g., Media Access Control addresses) information, which NSA compares to information contained in NSA's communication network databases and commercially available Internet Protocol address registration information in order to determine the location of the target.

**(S) Assessment of the Non-United States Person Status of the Target**

(S) In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, lead information provided by an intelligence or law enforcement service of a foreign government may indicate not only that the target is located in a foreign country, but that the target is a citizen of that or another foreign country. Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

(S) Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person.

(S) In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

**(S) Assessment of the Foreign Intelligence Purpose of the Targeting**

(S) In assessing whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

- a. With respect to telephone communications:
  - Information indicates that the telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
  - Information indicates that a user of the telephone number has communicated directly with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
  - Information indicates that the telephone number is listed in the telephone directory of a telephone used by an individual associated with a foreign power or foreign territory;
  - Information indicates that the telephone number has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
  - Publicly available sources of information (e.g., telephone listings) match the telephone number to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
  - Information contained in various NSA-maintained knowledge databases containing foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register and trap or trace device, or other information, reveals that the telephone number has been previously used by an individual associated with a foreign power or foreign territory;<sup>1</sup> or

---

<sup>1</sup> (TS//SI//NF) The NSA knowledge databases that would be used to satisfy this factor contain fused intelligence information concerning international terrorism culled from signals intelligence, human intelligence, law enforcement information, and other sources. The information compiled in these databases is information that assists the signals intelligence system in effecting collection on intelligence targets. For example, a report produced by the CIA may include the fact that a known terrorist is using a telephone with a particular number. NSA would include that information in its knowledge databases.

- Information made available to NSA analysts as a result of processing telephony metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the telephone number is used by an individual associated with a foreign power or foreign territory.
- b. With respect to Internet communications:
- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
  - Information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;
  - Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
  - Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
  - Public Internet postings match the electronic communications account/address/identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
  - Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;
  - Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or
  - Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory,

or are extensively used by individuals associated with a foreign power or foreign territory.

## II. (S) POST-TARGETING ANALYSIS BY NSA

(S//SI) After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States. Such analysis may include:

For telephone numbers:

- Routinely comparing telephone numbers tasked pursuant to these procedures against information that has been incidentally collected from the Global System for Mobiles (GSM) Home Location Registers (HLR). These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.
- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

For electronic communications accounts/addresses/identifiers:

- Routinely checking all electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against available databases that contain Internet communications data (including metadata) to determine if an electronic communications account/address/identifier was accessed from overseas. Such databases contain communications contact information and summaries of communications activity from NSA signals intelligence collection. The foreign access determination is made based on comparing the Internet Protocol address associated with the account activity to other information NSA possesses about geographical area(s) serviced by particular Internet Protocol addresses. If the IP address associated with the target activity is identified as a U.S.-based network gateway (e.g., a Hotmail server) or a private Internet Protocol address, then NSA analysts will be required to perform additional research to determine if the access was in a foreign country using additional criteria such as machine identifier or case notation (NSA circuit identifier) of a communications link known to be foreign. Such databases normally maintain information about such activity for a 12-month period. This data will be used in an attempt to rule out false positives from U.S.-based network gateways. If the account access is determined to be from a U.S.-based machine, further analytic checks will be performed using content collection to determine if the target has moved into the United States.

- Routinely comparing electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against a list of electronic communications accounts/addresses/identifiers already identified by NSA as being accessed from inside the United States. This will help ensure that no target has been recognized to be located in the United States.
- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

(S) If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. In cases where NSA cannot resolve an apparent conflict between information indicating that the target has entered the United States and information indicating that the target remains located outside the United States, NSA will presume that the target has entered the United States and will terminate the acquisition from that target. If at a later time NSA determines that the target is in fact located outside the United States, NSA may re-initiate the acquisition in accordance with these procedures.

(S) If NSA determines that a target who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

### III. (U) DOCUMENTATION

(S) Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

(S) A citation is a reference that identifies the source of the information, such as a report number or communications intercept identifier, which NSA will maintain. The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

(S) Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

### IV. (U) OVERSIGHT AND COMPLIANCE

(S) NSA's Signals Intelligence Directorate (SID) Oversight and Compliance, with NSA's Office of General Counsel (OGC), will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. SID Oversight and Compliance has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. SID

Oversight and Compliance will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. SID Oversight and Compliance will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, SID Oversight and Compliance will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

(S) The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur at least once every sixty days.

(S) NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

(S) NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

(S) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will take the following steps:

- 1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

- 2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

**V. (U) DEPARTURE FROM PROCEDURES**

(S) If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7-28-09  
Date

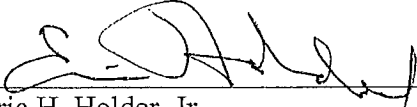
  
Eric H. Holder, Jr.  
Attorney General of the United States



EXHIBIT B

MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN  
CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE  
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE  
SURVEILLANCE ACT OF 1978, AS AMENDED

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT

2009 JUL 22 PM 3:14

CLERK OF COURT

Section 1 - Applicability and Scope (U)

These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. (U)

Section 2 - Definitions (U)

In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

- (a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public 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 will 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)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

- (e) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications. (S//SI)
- (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//SI)
- (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//SI)
- (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 8 U.S.C. § 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 targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be 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 acquisition. (S//SI)

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

- (1) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will 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 acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. (S//SI)
- (2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition 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, 6, and 8 of these procedures. (C)
- (3) Magnetic tapes or other storage media that contain acquired communications may be processed. (S)
- (4) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target 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, 6, and 8 of these procedures. (S//SI)
- (5) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 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, will not include United States person

names or identifiers and will be limited to those selection terms reasonably likely to return information about foreign intelligence targets. (S//SI)

- (6) Further processing, retention and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below. (S//SI)

(c) Destruction of Raw Data (C)

Communications and other information, including that reduced to graphic or "hard copy" form such as facsimile, telex, computer data, or equipment emanations, will 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 will be destroyed upon recognition, and may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. (S//SI)

(d) Change in Target's Location or Status (S//SI)

- (1) In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay. (S//SI)
- (2) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person, will be treated as domestic communications under these procedures. (S//SI)

Section 4 - Acquisition and Processing - 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 in the United States 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 will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will 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. Additionally, all proposed disseminations of information constituting United States person attorney-client

privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination. (S//SI)

Section 5 - Domestic Communications (U)

A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that: (S)

- (1) the communication is reasonably believed to contain significant foreign intelligence information. Such communication may be provided to the Federal Bureau of Investigation (FBI) (including United States person identities) for possible dissemination by the FBI in accordance with its minimization procedures; (S)
- (2) the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes; (S)
- (3) the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability. Such communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such communications 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//SI)
  - 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//SI)
  - b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or (S//SI)

- (4) the communication contains information pertaining to a threat of serious harm to life or property. (S)

Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact. Moreover, technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes. (S//SI)

Section 6 - Foreign Communications of or Concerning United States Persons (U)

(a) Retention (U)

Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act 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 five years unless the Signals Intelligence Director, 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//SI)

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 or 8 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 of the information 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) 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 or the United States person's identity is necessary to understand or assess a communications security vulnerability, 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 the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or
- (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 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting

procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (U)

(c) Provision of Unminimized Communications to CIA and FBI (S//NF)

- (1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. (S//SI/NF)
- (2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. (S//SI)

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)

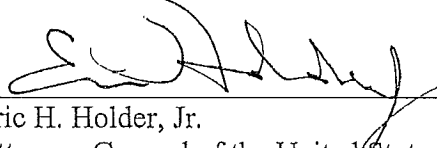
Section 8 - Collaboration with Foreign Governments (S//SI)

- (a) Procedures for the dissemination of evaluated and minimized information. Pursuant to Section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with subsections 6(b) and 7 of these NSA minimization procedures. (S)
- (b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated: (S)



- (1) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA. (S)
- (2) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data. (S)
- (3) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA. (S)
- (4) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA. (S)
- (5) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures. (S)

7-28-09  
Date

  
Eric H. Holder, Jr.  
Attorney General of the United States