

UNITED STATES OF AMERICA

v.

KHALID SHAIKH MOHAMMAD, WALID  
MUHAMMAD SALIH MUBARAK BIN  
‘ATTASH, RAMZI BIN AL SHIBH, ALI  
ABDUL-AZIZ ALI, MUSTAFA AHMED  
ADAM AL HAWSAWI

**AE284(AAA Sup.)**

**Defense Notice of Joinder, Factual**

Supplement and Argument to  
to AE284(WBA) Motion to Compel the  
Production of Information related to the  
Monitoring and/or Collection of  
Attorney-Client Privileged Information

2 April 2014

1. **Timeliness:** This Notice of Joinder, Factual Supplement and Argument is timely filed.
2. **Relief Requested:** The defendant below joins in the motion and argument by Mr. bin ‘Attash in the underlying motion. The Commission should order the United States Government to produce documents, records, recorded communications, papers, photographs, and/or tangible objects concerning Intelligence Community (IC) monitoring of defense communications.
3. **Overview:** Mr. al Baluchi fully joins in the co-defendant’s motion at AE284. He supplements his joinder herein by submitting his own ongoing discovery requests.
4. **Burden of Proof:** The defense bears the burden of proof.
5. **Relevant Facts:**
  - a. On 27 March 2014, Mr. bin ‘Attash filed motion AE284 “Defense Motion to Compel the Production of Information Related to the Monitoring and/or Collection of Attorney-Client Privileged Information.”
  - b. Mr. bin ‘Attash included attachments to his brief contains his relevant discovery requests. As indicated below, Mr. al Baluchi has made discovery requests seeking the same or similar information.

c. On 21 May 2013, Mr. al Baluchi propounded a discovery request<sup>1</sup> requesting information relating to apparent electronic monitoring in defense counsel's building AV-34 office:

(1) Please produce any document regarding installation or maintenance of electronic monitoring capabilities in the defense attorney office, including but not limited to "as-built" drawings.

(2) Please identify a person with full knowledge of electronic monitoring capabilities in the defense attorney office and make him or her available for interview.

(3) Please produce all information and documents regarding electronic monitoring conducted in the defense attorney office from 1 January 2008 to present.

To date, Mr. al Baluchi has not received any response to his discovery request DR-050-AAA.

d. On 10 June 2013, Mr. al Baluchi propounded a discovery request<sup>2</sup> regarding IC monitoring of defense counsel:

**Request #1:**

All documents and information pertaining to IC policies and procedures governing the collection of electronic surveillance information on detailed defense counsel's telephone numbers.

**Request #2:**

All electronic surveillance information in the possession of the United States, including, without limitation, the IC, relating to detailed defense counsel's telephone numbers during the period 28 February 2011 to the present.

**Request #3:**

All documents and information pertaining to intelligence community members' special policies and procedures, if any, for gathering, recording, and storing electronic surveillance information derived from communications that originate with or are received by attorneys who are communicating in their professional capacities, including attorneys representing defendants in criminal cases and accused in military justice and military commission proceedings.

e. On 7 August 2013, Mr. al Baluchi supplemented this request<sup>3</sup> by (1) updating the definitions of "IC" and "electronic surveillance information"; and (2) requesting all electronic

---

<sup>1</sup> Attachment B, DR-050-AAA, 21 May 2013.

<sup>2</sup> Attachment C, DR-062-AAA, 10 June 2013.

<sup>3</sup> Attachment D, DR-062A-AAA, 7 August 2013.

surveillance information in the possession of the United States relating to detailed defense counsel's email addresses during the period 28 February 2011 to the present.”

f. To date, Mr. al Baluchi has not received any response to his discovery requests DR-062-AAA and DR-062A-AAA.

**6. Law and Argument:**

Mr. al Baluchi fully joins in and adopts the arguments set forth by Mr. bin ‘Attash in the principal brief.

**7. Request for Oral Argument:** The defense requests oral argument.

**8. Witnesses:** None.

**9. Conference with Opposing Counsel:** The prosecution opposes the requested relief.

**10. Attachments:**

- A. Certificate of Service;
- B. DR-050-AAA, 21 May 2013;
- C. DR-062-AAA, 10 June 2013;
- D. DR-062A-AAA, 7 August 2013;
- E. NSA Minimization Procedures.

Very respectfully,

//s//  
JAMES G. CONNELL, III  
Learned Counsel  
  
Counsel for Mr. al Baluchi

//s//  
STERLING R. THOMAS  
Lt Col, USAF  
Defense Counsel

# **Attachment A**

**CERTIFICATE OF SERVICE**

I certify that on the 2nd day of April, 2014, I electronically filed the foregoing document with the Clerk of the Court and served the foregoing on all counsel of record by email.

*//s//*

JAMES G. CONNELL, III

*Learned Counsel*

## **Attachment B**



UNCLASSIFIED//FOR PUBLIC RELEASE  
DEPARTMENT OF DEFENSE  
OFFICE OF THE CHIEF DEFENSE COUNSEL  
OFFICE OF MILITARY COMMISSIONS  
1620 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1620

21 May 2013

MEMORANDUM FOR Trial Counsel

FROM: Sterling R. Thomas, Lt Col, USAF, Military Defense Counsel for Mr. al Baluchi

SUBJECT: DEFENSE REQUEST FOR DISCOVERY (**DR-050-AAA**)

Pursuant to R.M.C. 701, the Due Process Clause of the Fifth Amendment, the Confrontation Clause to the Sixth Amendment, and the Compulsory Process Clause of the Sixth Amendment to the United States Constitution, Mr. al Baluchi, through counsel, hereby requests that the government produce all recordings, books, papers, documents, photographs, tangible objects, building, places, and/or the reports/results of examinations, tests, or experiments that relate to electronic monitoring capabilities in Mr. al Baluchi's attorney's office (Room [REDACTED] Defense) located in Building AV-34, Guantanamo Bay Naval Station.

Definitions:

"*Defense attorney office*" means Room [REDACTED] Defense, Building AV-34, Guantanamo Bay Naval Station.

"*Electronic monitoring capabilities*" mean audio, video, or electronic surveillance devices of any kind, whether or not connected to a recording device or actively in use at any given time. This phrase includes but is not limited to the audio device pictured below, labeled as "Intellisense Model FG-730."



DR-050-AAA  
2013-05-21  
Appellate Exh bit 284 (AAA Sup)  
Page 7 of 28

UNCLASSIFIED//FOR PUBLIC RELEASE

In particular, Mr. al Baluchi requests the following:

- (1) Please produce any document regarding installation or maintenance of electronic monitoring capabilities in the defense attorney office, including but not limited to “as-built” drawings.
- (2) Please identify a person with full knowledge of electronic monitoring capabilities in the defense attorney office and make him or her available for interview.
- (3) Please produce all information and documents regarding electronic monitoring conducted in the defense attorney office from 1 January 2008 to present.

Please do not hesitate to contact me with any questions or concerns.

Very respectfully,

//s//

Sterling R. Thomas,  
Lieutenant Colonel, USAF  
Military Defense Counsel for Mr. al Baluchi

# Attachment C



UNCLASSIFIED//FOR PUBLIC RELEASE  
**DEPARTMENT OF DEFENSE**  
**OFFICE OF THE CHIEF DEFENSE COUNSEL**  
1620 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1620

10 June 2013

MEMORANDUM FOR Trial Counsel

FROM: Sterling R. Thomas, Lt. Col, USAF, Defense Counsel for Mr. al Baluchi

SUBJECT: DEFENSE REQUEST FOR DISCOVERY (**DR-062-AAA**)

**Definitions:**

1. "IC" means the Central Intelligence Agency (CIA); National Security Agency (NSA); Defense Intelligence Agency (DIA); the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the Army, Navy, Air Force, and Marine Corps; the Federal Bureau of Investigation (FBI); the Department of the Treasury and the Department of Energy; the staff elements of the Director of Central Intelligence; and all those otherwise identified in or designated pursuant to section 6.1(z) of Executive Order 13526, as amended; section 3(4) of the National Security Act of 1947, as amended; or section 3.5 of Executive Order 12333, as amended.
2. "Electronic surveillance information" means information relating to the monitoring, recording, gathering, or interception of telephonic, e-mail, text messaging and other electronic communications, including, without limitation, information, recordings, and records related to the communications' contents or substance; identities of participants; phone numbers and/or e-mail addresses of participants; locations of participants; and duration of communications.
3. "Detailed defense counsel's telephone numbers" [REDACTED]

Defendant, by and through undersigned counsel pursuant to RMC 701, the Due Process Clause of the Fifth Amendment, the Confrontation Clause to the Sixth Amendment, and the Compulsory Process Clause of the Sixth Amendment to the United States Constitution, hereby requests that the government produce the following information:

**Request #1:**

All documents and information pertaining to IC policies and procedures governing the collection of electronic surveillance information on detailed defense counsel's telephone numbers.

**Request #2:**

All electronic surveillance information in the possession of the United States, including, without limitation, the IC, relating to detailed defense counsel's telephone numbers during the period 28 February 2011 to the present.

**Request #3:**

All documents and information pertaining to intelligence community members' special policies and procedures, if any, for gathering, recording, and storing electronic surveillance information derived from communications that originate with or are received by attorneys who are communicating in their professional capacities, including attorneys representing defendants in criminal cases and accused in military justice and military commission proceedings.

Very Respectfully,  
//s//  
Sterling Thomas,  
Lieutenant Colonel, USAF  
Military Defense Counsel for Mr. al Baluchi

DR-062-AAA  
2013-06-10

# Attachment D

7 August 2013

## MEMORANDUM FOR Trial Counsel

FROM: Sterling R. Thomas, Lt. Col, USAF, Defense Counsel for Mr. al Baluchi

SUBJECT: SUPPLEMENT TO DEFENSE REQUEST FOR DISCOVERY (DR-062A-AAA)

This discovery request supplements DR-062-AAA submitted on 10 Jun 2013 by: (1) updating the definitions of "IC" and "electronic surveillance information"; and (2) requesting all electronic surveillance information in the possession of the United States relating to detailed defense counsel's email addresses during the period 28 February 2011 to the present.

**Definitions:**

1. "IC" means the Central Intelligence Agency (CIA); National Security Agency (NSA); Defense Intelligence Agency (DIA); the offices within the Department of Defense for the collection of specialized national foreign intelligence through *surveillance* programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the Army, Navy, Air Force, and Marine Corps; the Federal Bureau of Investigation (FBI); the Department of the Treasury and the Department of Energy; the staff elements of the *Director of National Intelligence*; and all those otherwise identified in or designated pursuant to section 6.1(z) of Executive Order 13526, as amended; section 3(4) of the National Security Act of 1947, as amended; or section 3.5 of Executive Order 12333, as amended.

2. "Electronic surveillance information" means information relating to the monitoring, recording, gathering, or interception of telephonic, e-mail, text messaging, *social network services* and other electronic communications, including, without limitation, information, recordings, and records related to the communications' contents or substance; identities of participants; phone numbers and/or e-mail addresses of participants; locations of participants; and duration of communications.

3. "Detailed defense counsel's telephone numbers" [REDACTED]

4. "Detailed defense counsel's e-mail addresses" means sterling.thomas [REDACTED]  
sterling.thomas [REDACTED] sterling.thomas [REDACTED]  
[REDACTED] james.connell2 [REDACTED]

Defendant, by and through undersigned counsel pursuant to RMC 701, the Due Process Clause of the Fifth Amendment, the Confrontation Clause to the Sixth Amendment, and the Compulsory Process Clause of the Sixth Amendment to the United States Constitution, hereby requests that the government produce the following information:

**Request #1:**

All documents and information pertaining to IC policies and procedures governing the collection of electronic surveillance information on detailed defense counsel's telephone numbers and email addresses.

**Request #2:**

All electronic surveillance information in the possession of the United States, including, without limitation, the IC, relating to detailed defense counsel's telephone numbers and/or email addresses during the period 28 February 2011 to the present.

**Request #3:**

All documents and information pertaining to intelligence community members' special policies and procedures, if any, for gathering, recording, and storing electronic surveillance information derived from communications that originate with or are received by attorneys who are communicating in their professional capacities, including attorneys representing defendants in criminal cases and accused in military justice and military commission proceedings.

Very respectfully,

//s//

Sterling Thomas,  
Lieutenant Colonel,  
USAF  
Military Defense Counsel for Mr. al Baluchi

# Attachment E

~~TOP SECRET//COMINT//NOFORN//20320108~~

## 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

Section 1 - Applicability and Scope ~~(S)~~

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"). ~~(S)~~

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. ~~(S)~~

For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). ~~(S)~~

Section 2 - Definitions ~~(S)~~

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

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN//20310108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (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 government employee, or by the General Counsel, NSA, to have actual or apparent authority to bind the organization. ~~(S)~~
- (e) Foreign communication means a communication that has at least one communicant outside the United States. Other communications, including communications in which the sender or intended recipients are reasonably believed to be located in the United States, but the communication, in its totality, is received in the United States, are domestic communications. ~~(S//SI)~~
- (f) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing 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) Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication ~~(S//SI)~~ or multiple discrete communications ~~(S//SI)~~.
- (h) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. ~~(U)~~
- (i) 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)~~
- (j) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S//SI)~~
- (k) 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

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

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. Except as provided for in subsection 3(c)(2) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(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. ~~(U)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (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) Processing of Internet Transactions Acquired Through NSA Upstream Collection Techniques ~~(TS//SI)~~
- a. Notwithstanding any processing (e.g., decryption, translation) that may be required to render an Internet transaction intelligible to analysts, NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown. ~~(TS//SI)~~
1. Internet transactions that are identified and segregated pursuant to subsection 3(b)(5)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States. ~~(TS//SI)~~
- (a) Any information contained in a segregated Internet transaction [REDACTED] may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection 3(b)(5)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be destroyed upon recognition. ~~(TS//SI)~~
- (b) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance the other applicable provisions of these procedures. ~~(TS//SI)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (c) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(5)a.
2. Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance with the other applicable provisions of these procedures.
- b. NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~
1. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. ~~(TS//SI)~~
2. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~
- (a) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~
- (b) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be treated in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~
- (c) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

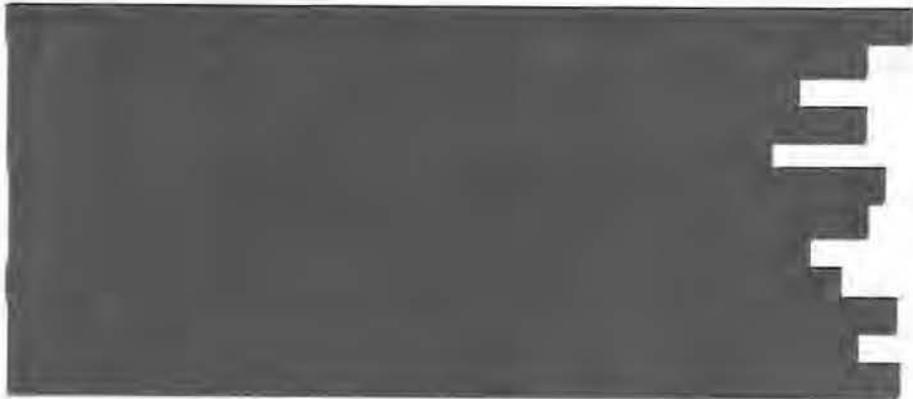
human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

~~(TS//SI)~~

3. An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(5)b.1. and 2. above.

~~(TS//SI)~~

4.



- (6) 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 be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph. ~~(S//SI)~~

- (7) 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)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~(c) Destruction of Raw Data ~~(C)~~

- (1) Telephony communications, Internet communications acquired by or with the assistance of the Federal Bureau of Investigation from Internet Service Providers, and other discrete forms of information (including that reduced to graphic or "hard copy" form such as facsimile, telex, computer data, or equipment emanations) that do not meet the retention standards set forth in these procedures 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 from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~
- (2) Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. All Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and processed only in accordance with the standards set forth in subsection 3(b)(5) of these procedures. ~~(TS//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

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

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 ~~(S)~~

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 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)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection 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 from the expiration date of the certification authorizing the collection 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)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~(b) Dissemination ~~(S)~~

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 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) 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;

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (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)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

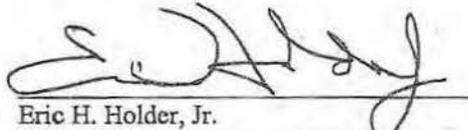
- (b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding 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)~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

- (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)~~

10-31-11  
Date

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

~~TOP SECRET//COMINT//NOFORN//20320108~~