



Request ID: 0001154921

UNCLASSIFIED  
TRANSMITTAL OF MATERIAL



Type: OMAL



Submitted: 20221209

|  |  |  |  |  |                             |
|--|--|--|--|--|-----------------------------|
| TO<br>MR. JOHN GREENEWALD, JR<br>27305 W. LIVE OAK RD<br>SUITE # 1203<br>CASTAIC, CA 91384 | FROM (RETURN ADDRESS)<br>DEPARTMENT OF DEFENSE<br>NATIONAL SECURITY AGENCY<br>9800 SAVAGE ROAD<br>FORT MEADE MARYLAND 20755-6000<br>ATTN: RAMSEY,VICKI LYNN<br>SUITE: 6881 |  | This transmittal may NOT be downgraded upon removal of the enclosure(s).<br>This transmittal may NOT be declassified upon removal of the enclosure(s). |  |                             |
|  | WRAPPED<br><input checked="" type="checkbox"/> U <input type="checkbox"/> S <input type="checkbox"/> D   |  | COMSEC<br><input type="checkbox"/> YES <input checked="" type="checkbox"/> NO  |  | SUBMITTED<br>20221209       |
|  | SHIPPING MODE<br>USPS - First Class  |  |  |  | PACKAGE CT<br><b>1 of 1</b> |

| LN# | UNCLASSIFIED TITLE/DESCRIPTION OF ITEM    | QTY | TOT COST | MFG SERIAL# | BARCODE | CLASS. OF ITEM |
|-----|---|-----|----------|-------------|---------|----------------|
| 1   | SERIAL: MDR-113393, DATED 9 DECEMBER 2022 | 1   | 0        |             |         | UNCLASSIFIED   |

|                 |            |            |                                 |          |
|-----------------|------------|------------|---------------------------------|----------|
| DESIG<br>CPOENP | ACCT<br>NO | TYPE<br>NA | PAS STATEMENT<br>Not Applicable | APPROVAL |
|-----------------|------------|------------|---------------------------------|----------|

SPECIAL HANDLING INSTRUCTIONS (UNCLASSIFIED)

|   |                                  |             |                        |
|---|----------------------------------|-------------|------------------------|
| REQUESTED BY<br>RAMSEY,VICKI LYNN (VLRAMSE) | SIGNATURE<br><i>Vicki Ramsey</i> | ORG<br>P133 | PHONE<br>(667)812-8002 |
|---|----------------------------------|-------------|------------------------|

UNCLASSIFIED  
DO NOT STAMP RECEIPT PORTION WITH CLASSIFICATION



Request ID: 0001154921

RECEIPT  
(Please sign and return immediately. Avoid tracer action)



Type: OMAL

|  |  |   |               |
|--|--|---|---------------|
| RETURN TO<br>DEPARTMENT OF DEFENSE<br>NATIONAL SECURITY AGENCY<br>9800 SAVAGE ROAD<br>FORT MEADE MARYLAND 20755-6000<br>ATTN: RAMSEY,VICKI LYNN<br>SUITE: 6881 | FROM<br>MR. JOHN GREENEWALD, JR<br>27305 W. LIVE OAK RD<br>SUITE # 1203<br>CASTAIC, CA 91384 | Receipt is hereby acknowledged for the material or documents listed under this Request ID |               |
|  |  | SID (Typed or Printed)  | DATE RECEIVED |
|  |  | NAME (Typed or Printed)   |               |
|  |  | SIGNATURES  |               |



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
FORT GEORGE G. MEADE, MARYLAND 20755-6000



Serial: MDR-113393  
9 December 2022

John Greenwald, Jr.  
27305 W. Live Oak Rd.  
Suite #1203  
Castaic, Ca. 91384

Dear Mr. Greenwald:

This responds to your request of 27 November 2021 to have FISA Amendments Act of 2008 Section 702, Summary Document, December 23, 2008 reviewed for declassification. The material has been reviewed under the Mandatory Declassification Review (MDR) requirements of Executive Order (E.O.) 13526 and is enclosed. We have determined that some of the information in the material requires protection.

Some portions deleted from the document were found to be currently and properly classified in accordance with E.O. 13526. The information denied meets the criteria for classification as set forth in Section 1.4 and remains classified SECRET as provided in Section 1.2 of E.O. 13526.

Section 3.5 (c) of E.O. 13526, allows for the protection afforded to information under the provisions of law. Therefore, the names of NSA/CSS employees and information that would reveal NSA/CSS functions and activities have been protected in accordance with Section 6, Public Law 86-36 (50 U.S. Code 3605, formerly 50 U.S. Code 402 note).

Since your request for declassification has been denied you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS MDR Appeal Authority. **The appeal must be postmarked no later than 60 calendar days after the date of the denial letter.** The appeal shall be in writing addressed to the NSA/CSS MDR Appeal Authority (P133), National Security Agency, 9800 Savage Road, STE 6881, Fort George G. Meade, MD 20755-6881. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes the release of information is

Serial: MDR-113393

required. The NSA/CSS MDR Appeal Authority will endeavor to respond to the appeal within 60 working days after receipt of the appeal.

If you have questions regarding this action, please contact me at 301-688-7785.

Sincerely,


A handwritten signature in cursive script that reads "Jacqueline M. Amacher".

Jacqueline M. Amacher  
Chief  
Declassification Services

Encl(s):  
a/s

This document is made available through the declassification efforts  
and research of John Greenewald, Jr., creator of:

# The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)  
document clearinghouse in the world. The research efforts here are  
responsible for the declassification of hundreds of thousands of pages  
released by the U.S. Government & Military.

**Discover the Truth** at: <http://www.theblackvault.com>

Declassified and Approved for Release by NSA on 12-09-2022 pursuant to E.O. 13526,  
MDR Case # 113393

# FISA Amendments Act of 2008

## Section 702

### Summary Document

Prepared by the Office of General Counsel (OGC)  
Formatting, Section Titles, and the Outline in the left margin added by ADET

23 December 2008

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20320108

## Table of Contents:

|   |    |
|---|----|
| Introduction to FAA section 702.....  | 3  |
| Compel Providers.....   | 3  |
| FISC orders for US persons or persons located inside the United States .....      | 3  |
| Time sensitive targets and high volume of targets .....                           | 3  |
| The means used:.....  | 3  |
| Certification details .....   | 3  |
| Day to day Analysts' attention.....   | 4  |
| Certification [redacted].....   | 5  |
| DIRNSA's affidavit.....   | 5  |
| Targeting Procedures (Exhibit A) .....  | 6  |
| Part 1 – Location .....   | 6  |
| Part 2 – Detecting target location or status changes.....                         | 7  |
| Part 3 – Identifying the foreign power .....                                      | 7  |
| Part 4 – Oversight and reporting .....  | 7  |
| Minimization Procedures (Exhibit B) .....   | 8  |
| The definitions section .....   | 8  |
| Section 3 – Acquisition and processing .....                                      | 9  |
| Section 4 – Attorney-Client communications .....                                  | 9  |
| Section 5 – Domestic communications .....   | 9  |
| Section 6 – Foreign communications of US persons .....                            | 10 |
| Section 7 – Foreign communications of US persons .....                            | 11 |
| Section 8 – FAA and collaboration with other governments .....                    | 14 |
| [redacted].....   | 12 |
| FAA Certification [redacted].....   | 13 |
| DIRNSA's affidavit.....   | 13 |
| Targeting Procedures (Exhibit A) .....  | 13 |
| Minimization Procedures (Exhibit B) .....   | 13 |
| The [redacted] that are the subject of Certification [redacted] (Exhibit F) ..... | 13 |
| FAA Certification [redacted].....   | 14 |
| DIRNSA's affidavit.....   | 14 |
| Targeting Procedures (Exhibit A) .....  | 14 |
| Minimization Procedures (Exhibit B) .....   | 15 |
| FAA Certification [redacted].....   | 16 |
| FAA Certification [redacted].....   | 17 |

EO 1.4.(c)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
PL 86-36/50 USC 3605

## I. Introduction to FAA section 702

1. Compel Providers
  - a. Non-US persons
  - b. Outside the United States
  - c. FAA 702 = an exception
2. Court Orders
  - a. FISA section F1-F4 did not change
  - b. Non-US persons & persons inside the United States need a FISC order
  - c. FISC orders need a probable cause case.
3. FAA 702 – for:
  - a. fast targeting and
  - b. a high volume of targets
4. The means:
  - a. AG/DNI certifications (certs) approved by FISC
  - b. Directives to providers
5. Certs
  - a. DNI & AG approve
  - b. At NSA – DIRNSA approves

## Introduction to FAA section 702

### **Compel Providers**

As described in the briefing accompanying this training, in July 2008, Congress enacted the “Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008” (FAA.) One of the primary purposes in enacting the FAA was the creation of a new way for the US Government to compel providers of electronic communications services to assist the Government in acquiring foreign intelligence information concerning **non-US persons located outside the United States**. This process is described in Section 702 of FAA. Almost all of the 1978 law remained intact, and Section 702 of FAA is best understood as an exception to FISA for such targets.

### **FISC orders for US persons or persons located inside the United States**

The definitions of “electronic surveillance” in FISA were not changed, so any collection that uses methods that fall within them and is directed at anyone inside the United States or at US persons abroad still requires a court order. The Government must give the court probable cause to believe that each target is a foreign power or agent of a foreign power before the court will issue an order compelling a communications service provider to assist with the targeting.

### **Time sensitive targets and high volume of targets**

Under section 702 of FAA, however, the Government may compel the same type of assistance in a way that is much more time-sensitive and more suitable for collection directed at a higher volume of targets.

### **The means used:**

The means used by the Government to compel this assistance is in the form of “certifications” issued jointly by the Attorney General and the Director of National Intelligence that are approved by the Foreign Intelligence Surveillance Court (FISC) and “directives” to the providers ordering them to assist the government.

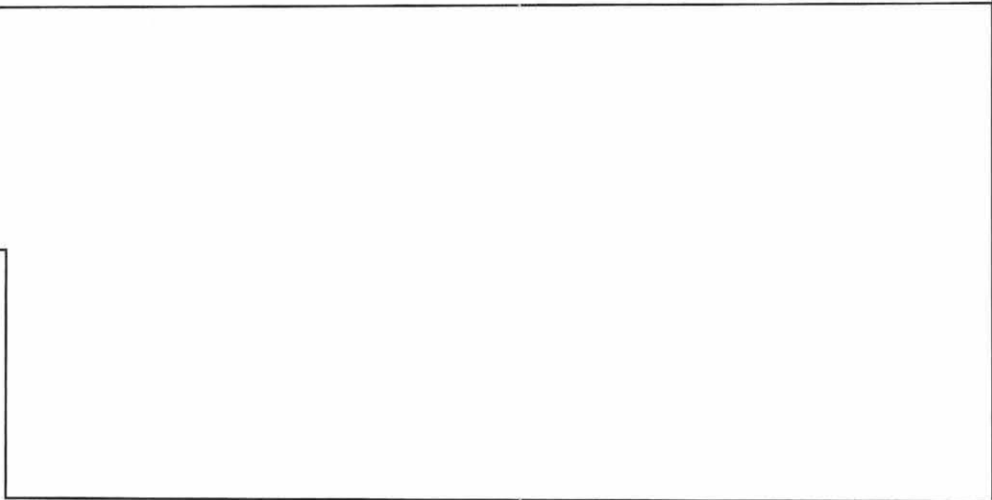
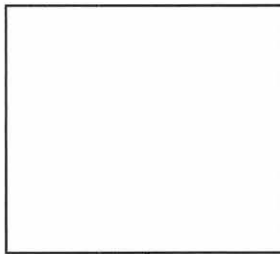
### **Certification details**

In a “certification”, the DNI and AG certify that specific requirements of the law have been met, and describe how this has been done. When the collection is being done by NSA, DIRNSA also makes representations to support the certification. If the court determines that the statutory requirements for a certification have been met, it issues an order to this effect, and the collection may begin.

I. Introduction to FAA section 702 cont'd

c.

d. AG/DNI have issued topical certs



Although Section 702 of the FAA provides a framework of requirements for issuance of a certification, it does not say how that framework must be used. To date, the AG and DNI have issued certifications that are topically based:

EO 1.4.(c)  
PL 86-36/50 USC 3605

6. Analysts concern:

a. Authorized targets (Exhibit F)

**Day to day Analysts' attention**

b. Foreignness procedures (Exhibit A)

c. Minimization procedures (Exhibit B)

d. Trained to know when a target fits the cert

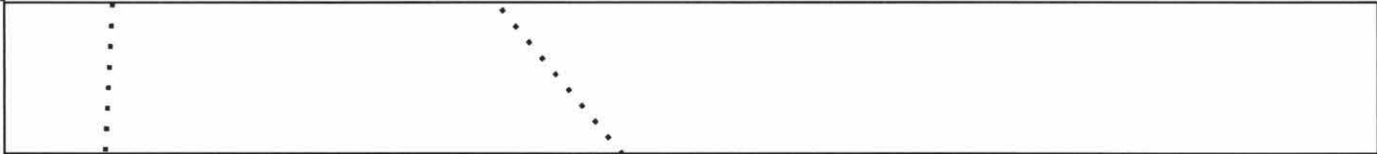
As described in the briefing, on a day-to-day basis, most analysts will need to be particularly concerned with:

- the portions of the certifications that describe which foreign intelligence targets have been authorized for collection in general terms by the Attorney General and DNI (typically, "Exhibit F" to a certification),
- the procedures for determining that there is a reasonable belief that a particular target is a non-US person located outside the United States (typically "Exhibit A" to a certification) and
- the minimization procedures that govern handling of US person (USP) information acquired in the course of collection directed at non-US persons reasonably believed to be located outside the US who fit within the terms of the authorization (typically "Exhibit B" to a certification.)

Thus, at the end of this training, NSA personnel should know how to find out whether a proposed target fits within the terms of a certification,



know where to find the rules for targeting, and know where to find the rules for handling the US person information they acquire. Because the certifications and the associated rules are subject to change, understanding where to find NSA's responsibilities and restrictions is every bit as important as becoming familiar with the specifics of their terms at the current time.



1. DIRNSA's Affidavit

**DIRNSA's affidavit**

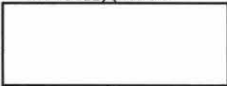


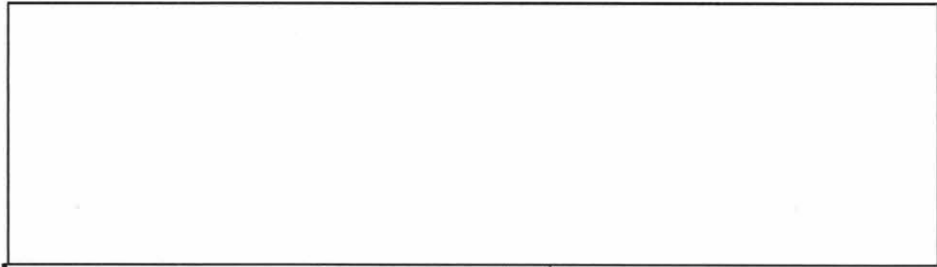
DIRNSA's affidavit to  states the following:

- a. Non-US person
- b. Outside of the United States
- c. Using US electronic communications carriers

NSA has adopted procedures that are reasonably designed to ensure that all targeting is directed at non-US persons reasonably believed to be outside the United States ("Exhibit A", described below)

This collection will be accomplished by a variety of means at switches and other parts of the infrastructure of companies that provide electronic communications services to people abroad from within the United States.

- d. Purpose
  - i. Foreign intelligence
  - ii. 



- e. Minimize US person info

When NSA personnel come across information concerning US persons, they will follow minimization procedures attached to the certification ("Exhibit B", described below)

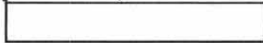
- f. CIA/FBI sharing

NSA may disseminate to CIA unevaluated data that comes from collection pursuant to this certification and that CIA requests in order to carry out its clandestine espionage and counterintelligence activities abroad.

NSA may also disseminate to FBI, at FBI's request, unevaluated data that comes from collection pursuant to this certification.

EO 1.4.(c)  
PL 86-36/50 USC 3605

**2. Targeting Procedures  
(Exhibit A)**



**Targeting Procedures (Exhibit A)**

These procedures address one of the central requirements of the FAA: determination that the targeting is limited to non-United States persons outside the United States. It does so in four parts.

a. Part I – Location

- i. Located outside of the United States
- ii. Totality of circumstances

**Part 1 – Location**

Part 1 discusses how NSA will make a determination that a person being targeted is located outside the United States. It notes that the determination is made in light of the totality of the circumstances.

1. Lead information

NSA analysts look at lead information they have received on the target; they conduct research in NSA databases available reports and collateral information, and they conduct technical analyses of the email addresses or other facilities to be targeted. They can use information from any one or a combination of these categories of information to determine that the potential target is outside the United States. Part 1 addresses each of these categories in greater detail, with examples of how they are applied to targeting of phone numbers and email addresses.

2. Seeking info “about” a target – requires filters

It also notes that when NSA is seeking to acquire communications about the target that are not to or from the target, it will employ IP filters or similar technology to ensure that the collection is directed at a party to communications reasonably believed to be outside the United States.

3. Presumption of status based on location

Part 1 also provides similar guidance on assessment of a potential target’s status as a non-US person. It notes that information on a potential target’s location is frequently useful in determining his status as well. It notes that in the absence of specific information regarding a potential target’s status, if a person is reasonably believed to be located outside the United States, he will also be presumed to be a non-US person, unless/until he can be positively identified as a US person or the nature or circumstances of his communication give rise to a reasonable belief to the contrary.

4. Target possesses and is likely to communicate foreign intelligence

Because one of the things certified by the AG and DNI is that the purpose of the collection is to gather foreign intelligence, part 1 also addresses how NSA will assess whether the target possesses and/or is likely to communicate information of foreign intelligence value concerning a foreign power or foreign territory. NSA can not target someone merely because he is located outside the US; there has to be some reason to believe that the targeting will acquire foreign intelligence. This requirement, and most of the factors listed in this

2. Targeting Procedures  
*cont'd*

[Redacted]

b. Part II – Location change detection

i. Detect if a target enters the United States

ii. Or if the target is a US person

c. Part III – identify the foreign power

d. Part IV – Oversight

i. O&C/OGC

ii. DOJ/ODNI

section are intuitive to NSA analysts, and include information that indicates the target has communicated with someone associated with a foreign power or territory, information in public directories that link a phone number to someone associated with a foreign power or foreign territory.

**Part 2 – Detecting target location or status changes**

Part 2 describes steps that will be taken by NSA after targeting has begun to ensure that it detects when a target has entered the United States, despite a reasonable belief to the contrary when targeting was initiated. These steps are designed to prevent NSA from collecting domestic communications as well as any targeting of persons who are inside the United States.

[Redacted]

but in many cases, it will be the content of a communication that indicates that a target has entered the United States. If NSA determines that a target has entered the United States or that a target thought to be a non-US person is in fact a US person, it must terminate collection without delay and take additional steps described in Part 4 below.

**Part 3 – Identifying the foreign power**

Part 3 states that before collection can begin, analysts must document one or more citations to the information that led them to believe that a target was located outside the United States. They must also identify the foreign power or foreign territory about which they expect to obtain foreign intelligence so that people conducting oversight of NSA's collection can see how the Agency is meeting the requirements established by the AG and DNI in their certification.

**Part 4 – Oversight and reporting**

Part 4 describes oversight and compliance responsibilities associated with collection done pursuant to [Redacted]. The SID office of Oversight and Compliance (O&C), together with the OGC, is required to develop training on the rules associated with FAA collection. O&C must also ensure that raw traffic from FAA collection is labeled and stored only in authorized repositories and accessible only to those who have had such training. O&C is also required to conduct periodic spot checks to ensure that NSA is meeting its responsibilities with regard to targeting, dissemination and other activities associated with FAA collection.

The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) also conduct independent oversight of NSA's activities, with reviews at least once every 60 days.

EO 1.4.(c)  
PL 86-36/50 USC 3605

PL 86-36/50 USC 3605

2. Targeting Procedures  
cont'd - [redacted]

iii. Reporting incidents to ODNI CLPO, DOJ, and ODNI OJC for:

- 1. Intentional violations
- 2. Mistakes

NSA must report to DOJ, the ODNI Office of General Counsel and the to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance with targeting procedures that result in intentional targeting of persons reasonably believe to be located in the United States or the intentional acquisition of domestic communications. These reports must be made within 5 days of NSA learning of the incident. Any information acquired by intentionally targeting a US person or a person nor reasonably believed to be outside the United States at the time of targeting has to be purged from NSA databases.

Part 4 also repeats the requirement that if NSA targets someone in the reasonable belief that he is a non-United States person outside the United States and later finds out that the target is inside the United States or is in fact a US person (no matter where he is located), it must cease the targeting without delay. Any information gathered prior to determining that the target was a US person or located inside the United States has to be handled in accordance with the relevant minimization procedures (Exhibit B, discussed below.) In addition, NSA must report the incident to DOJ, the ODNI Office of General Counsel and the ODNI Civil Liberties Officer within 5 days.

EO 1.4.(c)  
PL 86-36/50 USC 3605

3. Minimization Procedures (Exhibit B)

- a. Govern info concerning US persons obtained while targeting non-US persons

**Minimization Procedures (Exhibit B)**

The minimization procedures [redacted] are modeled on NSA's Standard Minimization Procedures (Annex A to USSID 18), but contain some significant differences. It is important to keep in mind that they govern the processing/retention/dissemination of information concerning US persons that is collected in the course of targeting non-United States persons reasonably believed to be outside the United States. Any restrictions on the handling of data that does not concern US persons come from another source (e.g., concerns about the potential risk to sources and methods.) All of the requirements in the procedures will not be repeated verbatim here, but NSA personnel working with FAA data should review their terms closely.

- b. Definitions

**The definitions section** is the first substantive portion of the procedures and should be reviewed carefully for obvious reasons. Restrictions on the handling of information concerning "US persons" can not be properly applied unless one understands what

3. Minimization Procedures  
cont'd

falls within the definition of "US person." The same is true for "foreign communication" and similar terms.

EO 1.4.(c)  
PL 86-36/50 USC 3605

c. Section 3 -  
Acquisition

**Section 3 – Acquisition and processing**

Highlights of section 3, which addresses acquisition and processing in general, include the following:

- i. Inadvertent communications retained 5 yrs
  - inadvertently acquired communications of or concerning US persons can be retained no longer than 5 years (unless the Signals Intelligence Director authorizes a longer retention period in accordance with Section 5)
- ii. No US person names in querying
  - computer selection terms used for scanning collected data to identify communications for analysis shall not include US person names or identifiers
- iii. Stop targeting of US location or US status is identified
  - if NSA is targeting someone in the reasonable belief that he is a non-US person outside the United States and subsequently learns that either of these beliefs is incorrect, it must terminate the targeting without delay. Any communications collected through such targeting, prior to the determination that the person's status or location was incorrect, must be handled in accordance with the procedures governing "domestic communications", discussed in Section 5)

d. Section 4 –  
Attorney- Client

**Section 4 – Attorney-Client communications**

Section 4 states that privileged attorney-client communications must be handled with particular care. Any proposed dissemination of information from privileged attorney-client communications must be reviewed by the NSA OGC

e. Section 5 –  
Domestic  
Communications

**Section 5 – Domestic communications**

Section 5 governs the handling of domestic communications. Generally, domestic communications shall be promptly destroyed. However, DIRNSA can authorize an exception to this requirement if he determines, in writing, that the communications in question fall within one of 4 specified categories:

- i. Normally Destroy
- ii. Waiver if:
  - 1. foreign intelligence
    - domestic communications reasonably believed to contain significant foreign intelligence shall be disseminated to the FBI,

3. Minimization Procedures

conf'd



ii. Waiver if: cont'd

2. Evidence of a crime

3. Technical database information

4. Threat of serious harm to life or property

iii. The ordinary storage limit of raw data is 5 years

for possible further dissemination in accordance with its minimization procedures

- domestic communications that do not contain foreign intelligence information but are reasonably believed to contain evidence of a crime may be referred to the NSA OGC for possible further dissemination in accordance with procedures established within the Executive Branch
- domestic communications that do not contain foreign intelligence or evidence of a crime, but contain technical database information or information necessary to understand or assess a communications security vulnerability may be disseminated to the FBI and other elements of the US Government
- the communication contains information pertaining to a threat of serious harm to life or property

Section 5 also states that ordinarily the maximum amount of time that unencrypted domestic communications may be retained in technical databases is 5 years, unless the Signals Intelligence Director determines in writing that retention for a longer period is required to respond to authorized foreign intelligence requirements. Notwithstanding any of these limitations, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact.

f. Section 6 - Foreign communications of US persons

**Section 6 – Foreign communications of US persons**

i. The ordinary storage limit of raw data is 5 years

Section 6 governs the handling of foreign communications of or concerning US persons. Unencrypted foreign communications can be retained for up to 5 years, while they are being evaluated, unless the Signals Intelligence Director determines in writing that a longer retention period is required. They can also be retained if dissemination of the communications would be permissible with the US person information included or if they contain evidence of a crime.

ii. Ordinarily mask US person identities

Ordinarily, reports based on foreign communications of or concerning US persons are supposed to be disseminated in a manner that masks the US person identities. However, US

3. Minimization Procedures  
*conf'd*



person identity information may be disseminated to recipients requiring it for the performance of their official duties if the identity is necessary to understand or assess foreign intelligence information or otherwise fits within the criteria outlined in Section 6 (b).

g. Section 7 - Foreign communications of non-US persons

**Section 7 – Foreign communications of Non-US persons**

Section 7 states that information from foreign communications concerning non-United States persons can be disseminated in accordance with NSA's normal rules for handling intercept.

h. Section 8 – FAA and collaboration

**Section 8 – FAA and collaboration with other governments**

Section 8 provides the rules for handling information collected pursuant to Section 702 of FAA in the context of collaboration with foreign governments. It is distinct from the dissemination of reporting to foreign governments, which is governed by Section 6. NSA can share or exchange foreign communications with the governments of Australia, Canada, the United Kingdom and New Zealand, but only with their written assurance that they will use the communications subject to the limits on retention and dissemination within the procedures. Domestic communications may not be shared with them, and ordinarily, NSA analysts must remove US person identifiers that are not necessary to understand or assess the foreign intelligence contained within foreign plain text communications.

1. This is not sharing reports
2. NSA can share raw data with Second Party partners
3. NSA may not share Domestic Communications and ordinarily minimize data
4. Encrypted communications may be shared unminimized with limitations

Encrypted communications may also be shared, as may communications for which the Second Parties' linguistic or technical assistance is required. However, there are significant limitations on what the Second Parties can do with such unevaluated communications and NSA has additional responsibilities with regard to ensuring that the material is handled properly.

4. Target list (Exhibit F)

[Redacted]

[Redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

[Redacted] the **DNI and AG** state that the foreign intelligence information to be acquired pursuant to the certification [Redacted] as defined in specific parts of FISA. They also state that the entities listed in Exhibit F fit within these definitions. This means that NSA can target individuals reasonably believed to be non-US persons located outside the United States to acquire information concerning these entities. If NSA wants to target an individual who is reasonably believed to be a non-United States person located outside the United States in order to obtain information [Redacted] that fits within these definitions, but which is not on the list it may do so.

[Redacted]



PL 86-36/50 USC 3605

**FAA Certification**

(Targeting Directed at

1. DIRNSA's Affidavit

**DIRNSA's affidavit**

The only difference from [redacted] is the TARGET SET

The only difference between this affidavit and the affidavit for [redacted] is that it reflects that the certification concerns a different set of targets. The collection in this case will seek to acquire foreign intelligence information concerning [redacted]

2. Targeting Procedures (Exhibit A)

**Targeting Procedures (Exhibit A)**

These procedures are the same [redacted]

3. Minimization Procedures (Exhibit B)

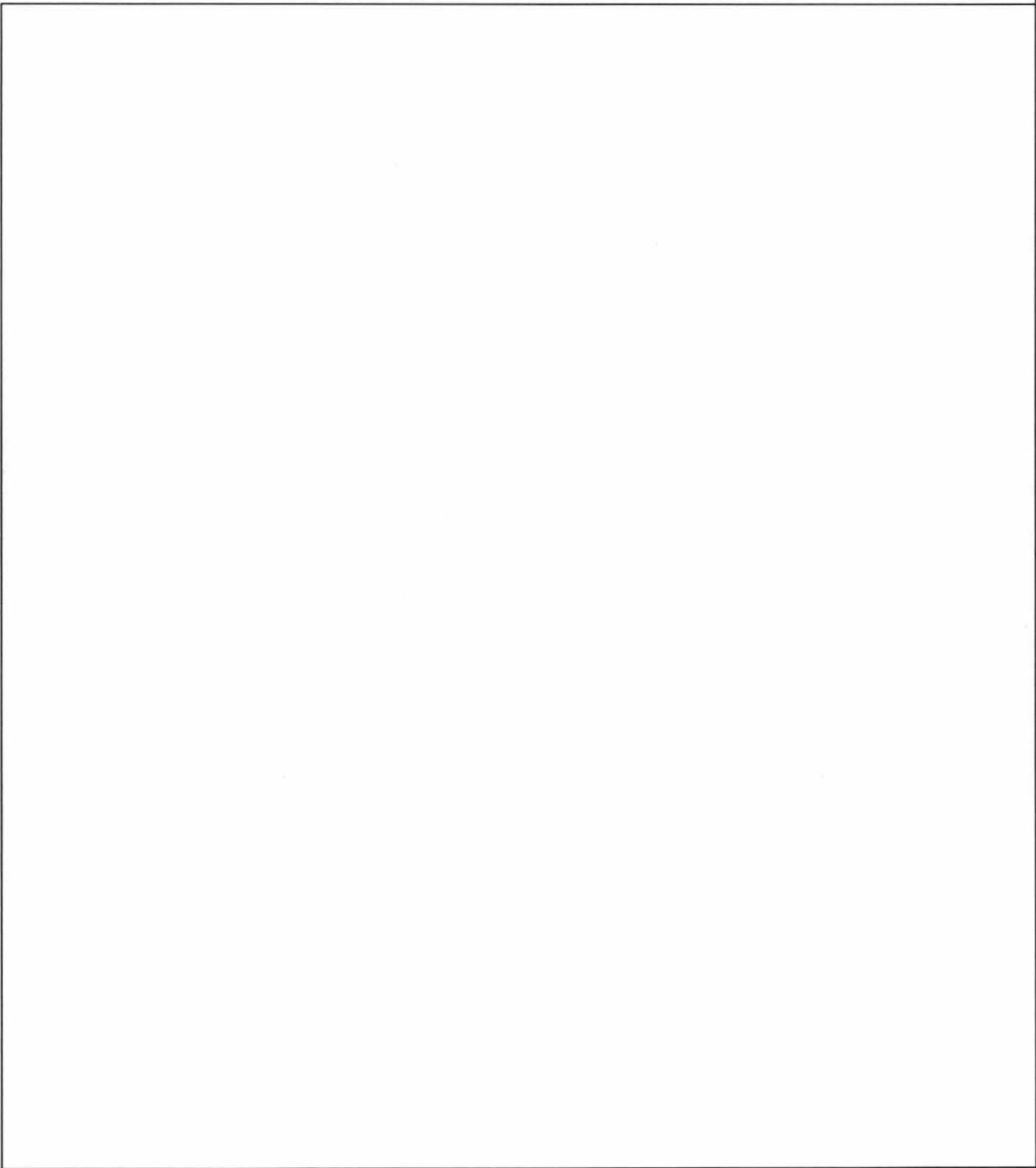
**Minimization Procedures (Exhibit B)**

These procedures are the same [redacted]

4. Target List (Exhibit F)

The only difference from [redacted] is the TARGET SET

EO 1.4.(c)  
PL 86-36/50 USC 3605



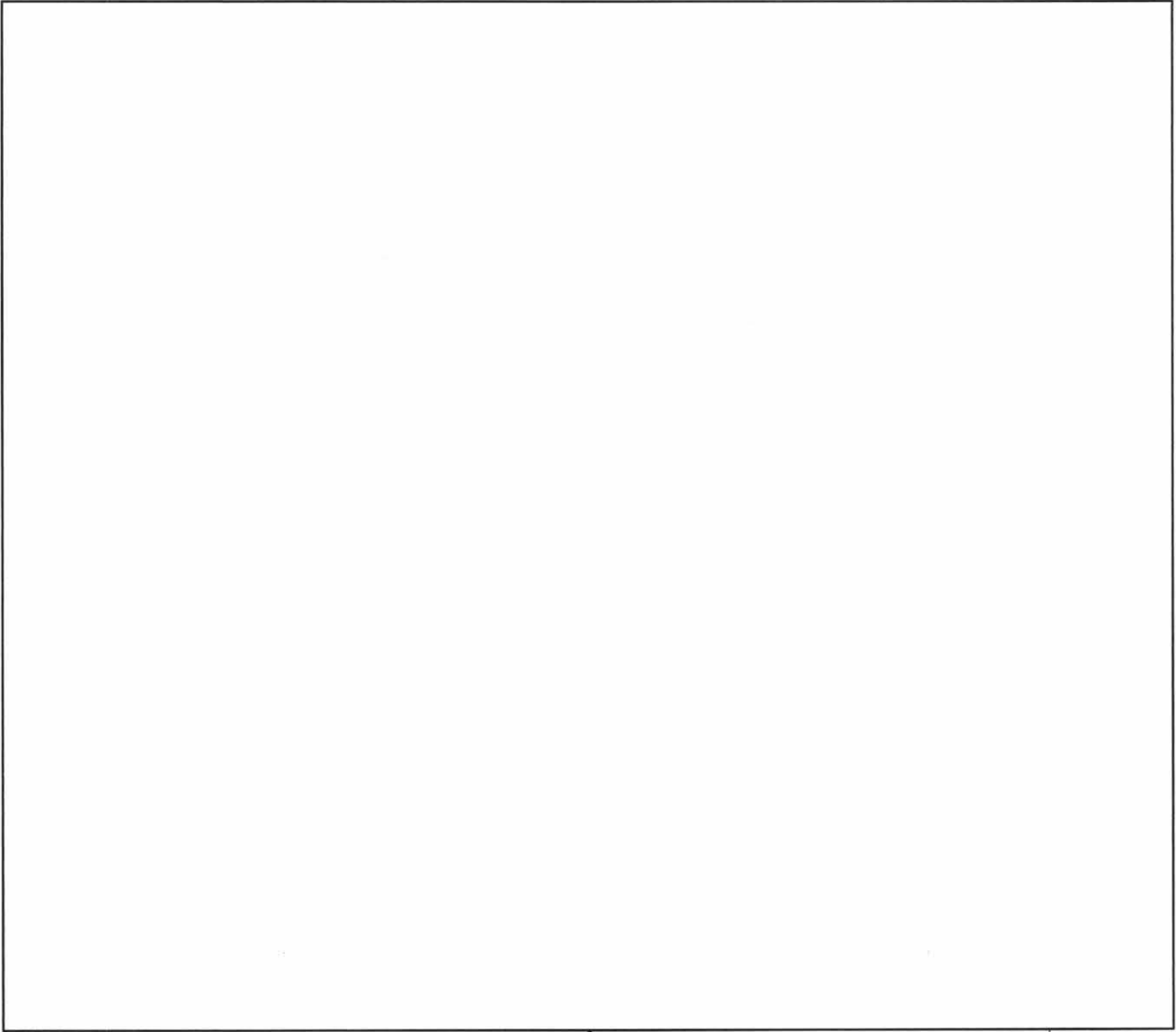
3. Minimization Procedures  
(Exhibit B)

**Minimization Procedures (Exhibit B)** :

Focus on Section 8

- 1. NSA may dissemination instruction
  
- 2. Expanded NSA capability to obtain technical and linguistic assistance

These procedures differ in two relatively minor ways from the minimization procedures [redacted] Both of these differences appear in section 8. First, they make it clear that NSA may disseminate intelligence reports that contain properly minimized US person information to foreign governments, and that any dissemination of US person information to a foreign government must be done in a manner consistent with subsections 6(b) and 7 of the minimization procedures... essentially the same rules that govern dissemination of US person information to other federal agencies. Because NSA always interpreted this portion of the minimization procedures in this manner, this "clarification" has no meaningful practical consequences. Second, they expand NSA's capability to obtain technical and linguistic assistance from foreign governments beyond the Second Parties. The conditions and limitations under which such assistance may be sought/provided remain unchanged, but as long as they are met, NSA may obtain the assistance from other foreign governments as well.



EO 1.4.(c)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
PL 86-36/50 USC 3605

