~~SECRET//NOFORN~~

GeoEye
Elevating Insight

2325 Dulles Corner Blvd
Herndon, VA 20171

703.480.7500
703.480.8173 fax

January 9, 2013

Interagency Security Classification Appeals Panel
Attn: Executive Secretary/Mr. William Carpenter
C/O Information Security Oversight Office
700 Pennsylvania Avenue, NW Room 500
Washington, DC 20408

Subject: (U) Appeal of Classification Challenge; Enhanced View Contract HM0210-10-C-003/GeoEye

Reference: (a) (U) EO 13526 Section 1.8
(b) (U) 32 CFR Section 2001.14
(c) (U) Public Law 111-258 (The Over-Classification Act)

Attachments: (1) (U) NGA Letter dated 20 Nov 2012; same subject (document is S//NF)
(2) (U) GeoEye memorandum dated 23 Aug 2012; same subject (document is S//NF)
(3) (U) NGA GEOINT Classification Guide Annex: Commercial EO Imagery Security Classification Guide, V 1.0 dated 8 March 2010 (document is S//NF)
(4) (U) NGA GEOINT Classification Guide Annex: U.S. Based Commercial EO Imagery (NSGM SC 9215) undated/unsigned update to v1.1 below (document is S//NF)
(5) (U) NGA Classification Guide v1.1 dated 25 Mar 2008 (document is S//NF)
(6) (U) GeoEye Power Point Slides: C&A Discussions Topics dated 23 Apr 2012 (Protect as S//NF pending ISACP decision." GeoEye marked slide 9 as U//FOUO/PROPIN but NGA ruled is S//NF)
(7) (U) Slide 9 - Implementation Architecture View Slide (illustration purposes only) (notional detail depicted in purple to signify classification of slide as S//NF)
(8) (U) Email correspondence between GeoEye and NGA (email package is S//NF)

Attachment Summary

| | | |
|---|---|---|
| Attachment (1) | (U) | NGA final ruling on GeoEye's classification challenge; |
| Attachment (2) | (U) | GeoEye's classification challenge submission to NGA; |
| Attachments (3-5) | (U) | NGA classification guidance for the commercial imagery program; |
| Attachment (6) | (U) | PowerPoint brief. NGA ruled slide #9 classified S//NF based on SCG AIS table item numbers 11 and 17, which GEOEYE disputes; |
| Attachment (7) | (U) | Notionally classified copy of attachment (6), slide #9, with fictitious information added that would raise the sensitivity level to S//NF per NGA classification guidance (Attachment is classified for illustrative purposes only. It demonstrates our understanding of the details that would be embedded in the slide per line items 11 and 17 of NGA AIS table which are classified). |
| Attachment (8) | (U) | Email communications between GeoEye and NGA on this issue |

Classified By: Paul Mattocks, GEOEYE Director of Security
Derived From: NGA GEOINT CG NSGM SC 9215 & NGA Commercial Imagery Guide v1.0 Mar 2008
Declassify On: 20371231

GeoEye
Elevating Insight

2325 Dulles Corner Blvd
Herndon, VA 20171

703.480.7500
703.480.8173 fax

January 9, 2013

Dear Mr. Carpenter,

(U) Pursuant to references (a) and (b), GeoEye is respectfully appealing a final classification ruling that was rendered on November 20, 2012 by elements within the National Geospatial-Intelligence Agency (NGA). Attachment (1) refers. GeoEye submitted attachment (2) that reveals the details, analysis and a conclusion to NGA that the document is properly marked UNCLASSIFIED//FOUO//PROPIN. Accordingly, as an authorized holder of information, GeoEye is exercising its option to appeal the NGA decision to the Interagency Security Classification Appeals Panel (ISCAP) for final resolution. Attachments (3) through (8) are also provided as background information for this appeal.

(U) As a result of numerous unsuccessful attempts to resolve classification ambiguities regarding slide 9, GeoEye believes the NGA final decision is neither supported by the classification guidance issued by competent NGA authority, and that it conflicts with other classification decisions in the GEOINT commercial EO annex guides which clearly acknowledge the open/unclassified association between the commercial data providers (CDPs) and NGA. Additionally, the fact that commercial vendors and CDPs conduct secure operations with NGA and work with classified information has already been determined as unclassified, which provides the framework under which GEOEYE protects the NGA program equities.

(U) The following classification management observations are noted as a matter of record:

- (U) During 2011, GeoEye participated on a NGA/CDP security classification working group. The purpose was to update security classification guidance for commercial imagery. On our own initiative, GeoEye presented proposed classification citations to the agency that would aid in greater specificity and clarity for their new guide; we believe the expense of using our own resources was important to help avoid confusion and unnecessary costly clean-up of data spills that were deemed avoidable with clear guidance. GeoEye requested that the NGA EnhancedView Program Office provide draft security guidance but was denied on November 15, 2011. GeoEye received draft guidance in June 2012 and notified the agency's classification management office our intentions were to implement it unless otherwise directed, but was subsequently denied by the Contracting Officer on June 15, 2012. (email correspondence refers).

- (U) NGA did not provide a written response or acknowledge the challenge to GeoEye within 60 days as stipulated by references (a) and (b).

- (U) NGA's final ruling was issued in writing to GeoEye by other than an OCA and did not inform GeoEye of its appeals right to the ISCAP.

GeoEye
Elevating Insight

2325 Dulles Corner Blvd
Herndon, VA 20171

703.480.7500
703.480.8173 fax

- (U) NGA has since posted a new unsigned commercial imagery security classification guide on its internal website; the agency has not directed GeoEye to use the new guide at this time. The classification of the AIS table in the new guide has not changed and GeoEye concludes the classification of slide 9 is properly marked and keeping within the new guidance.

(U) In summary, GeoEye contends the sensitivity of slide 9 was adequately protected at the UNCLASSIFIED//FOUO/PROPIN level; does not contain information falling within the AIS table (line items 11 or 17), as stated by NGA; nor was the NGA Classification Management Office's decision to classify the slide supported by the official published commercial imagery security classification guidance under contract. GeoEye firmly believes that resolving classification ambiguities regarding architectural drawings and schematics is vital to protecting both U.S government and commercial data providers interests and most important, avoid over-classification of information pursuant to references (a), (b) and (c).

(U) Thank you for your consideration in reviewing this matter. My point of contact regarding this security classification appeal is [redacted] ~~GeoEye Director of Security. He may be reach by unclassified~~ email at [redacted] FOIA(b)(6)

Sincerely,

William Schuster
Chief Operating Officer

Copy to:
Director, National Geospatial Intelligence Agency

~~SECRET//NOFORN~~

S-2013-0186

## INFORMATION PAPER

SUBJECT: (U) GeoEye Classification Challenge Appeal of Decision to the Interagency Security Classification Appeals Panel (ISCAP)

(U//~~FOUO~~) **Purpose**. To provide an information paper to D/NGA on GeoEye's Classification Challenge and Appeal to the ISCAP in accordance with Executive Order (E.O.) 13526, 'Classified National Security Information', Section 5.3. *Interagency Security Classification Appeals Panel.*

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

1. (U//~~FOUO~~) **Content**. On 10 May 2012 NGA's Office of Security, Classification Management Branch [redacted] rendered a SECRET//NOFORN classification decision on an automated information systems (AIS) flow diagram contained in a briefing labeled by GeoEye as UNCLASSIFIED//FOUO//PROPIN. GeoEye disagrees with the decision and has appealed the decision to ISCAP, requesting concurrence with their original determination of UNCLASSIFIED//FOUO//PROPIN as a final resolution.

FOIA(b)(1) FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

2. (~~S//NF~~) **Background on NGA's final ruling on GeoEye Enhanced View AIS diagram.** [redacted]

FOIA(b)(1) NGA

[redacted]

~~SECRET//NOFORN~~

CL BY: [redacted]
DERIVED FROM: NGA SCG
DECL ON: 20371219

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

S-2013-0186

[redacted] FOIA(b)(1) NGA

3. ~~(S//NF)~~ **Potential impact that might result from the appeal of this classification challenge.**

[redacted] FOIA(b)(1) FOIA(b)(3) - 10 USC 424 - DIA NRO and NGA

[redacted] FOIA(b)(1) NGA

4. (U) Point of Contact.

[redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)

~~SECRET//NOFORN~~

GeoEye
Elevating Insight

2325 Dulles Corner Blvd
Herndon, VA 20171

703.480.7500
703.480.8173 fax

January 9, 2013

Interagency Security Classification Appeals Panel
Attn: Executive Secretary/Mr. William Carpenter
C/O Information Security Oversight Office
700 Pennsylvania Avenue, NW Room 500
Washington, DC 20408

Subject: (U) Appeal of Classification Challenge; Enhanced View Contract HM0210-10-C-003/GeoEye

Reference: (a) (U) EO 13526 Section 1.8
(b) (U) 32 CFR Section 2001.14
(c) (U) Public Law 111-258 (The Over-Classification Act)

Attachments: (1) (U) NGA Letter dated 20 Nov 2012; same subject (document is S//NF)
(2) (U) GeoEye memorandum dated 23 Aug 2012; same subject (document is S//NF)
(3) (U) NGA GEOINT Classification Guide Annex: Commercial EO Imagery Security Classification Guide, V 1.0 dated 8 March 2010 (document is S//NF)
(4) (U) NGA GEOINT Classification Guide Annex: U.S. Based Commercial EO Imagery (NSGM SC 9215) undated/unsigned update to v1.1 below (document is S//NF)
(5) (U) NGA Classification Guide v1.1 dated 25 Mar 2008 (document is S//NF)
(6) (U) GeoEye Power Point Slides: C&A Discussions Topics dated 23 Apr 2012 (Protect as S//NF pending ISACP decision." GeoEye marked slide 9 as U//FOUO/PROPIN but NGA ruled is S//NF)
(7) (U) Slide 9 - Implementation Architecture View Slide (illustration purposes only) (notional detail depicted in purple to signify classification of slide as S//NF)
(8) (U) Email correspondence between GeoEye and NGA (email package is S//NF)

Attachment Summary

| | | |
|---|---|---|
| Attachment (1) | (U) | NGA final ruling on GeoEye's classification challenge; |
| Attachment (2) | (U) | GeoEye's classification challenge submission to NGA; |
| Attachments (3-5) | (U) | NGA classification guidance for the commercial imagery program; |
| Attachment (6) | (U) | PowerPoint brief. NGA ruled slide #9 classified S//NF based on SCG AIS table item numbers 11 and 17, which GEOEYE disputes; |
| Attachment (7) | (U) | Notionally classified copy of attachment (6), slide #9, with fictitious information added that would raise the sensitivity level to S//NF per NGA classification guidance (Attachment is classified for illustrative purposes only. It demonstrates our understanding of the details that would be embedded in the slide per line items 11 and 17 of NGA AIS table which are classified). |
| Attachment (8) | (U) | Email communications between GeoEye and NGA on this issue |

Classified By: Paul Mattocks, GEOEYE Director of Security
Derived From: NGA GEOINT CG NSGM SC 9215 & NGA Commercial Imagery Guide v1.0 Mar 2008
Declassify On: 20371231

~~SECRET//NOFORN~~

**NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY**
S5, M/S N73-SU, 7500 GEOINT Drive
Springfield, Virginia 22150

20 November 2012

[redacted] FOIA(b)(6)

GeoEye Imagery Collection Systems, Inc
2325 Dulles Corner Boulevard
Herndon, Virginia 20171

Subject: RE: Classification Challenge; EnhancedView Contract HM0210-10-C-0003

Reference: (a) GeoEye's email dated 1 November 2012; Subject: Classification Challenge

(b) GeoEye's memorandum dated 23 August 2012; Subject: Security Classification Challenge

Mr. Donovan,

1. ~~(S//NF)~~ [redacted] FOIA(b)(1) NGA

2. ~~(S//NF)~~ [redacted] FOIA(b)(1) NGA

3. (U//~~FOUO~~) As a result of these findings, [redacted] is required to attend mandatory training on NGC-CBT 013413 Information Assurance and NGC-CBT 016094 Annual Security Refresher Training. Once the training is completed, please forward a copy of your training certificate to the NGA PMO no later than 26 November 2012. FOIA(b)(6)

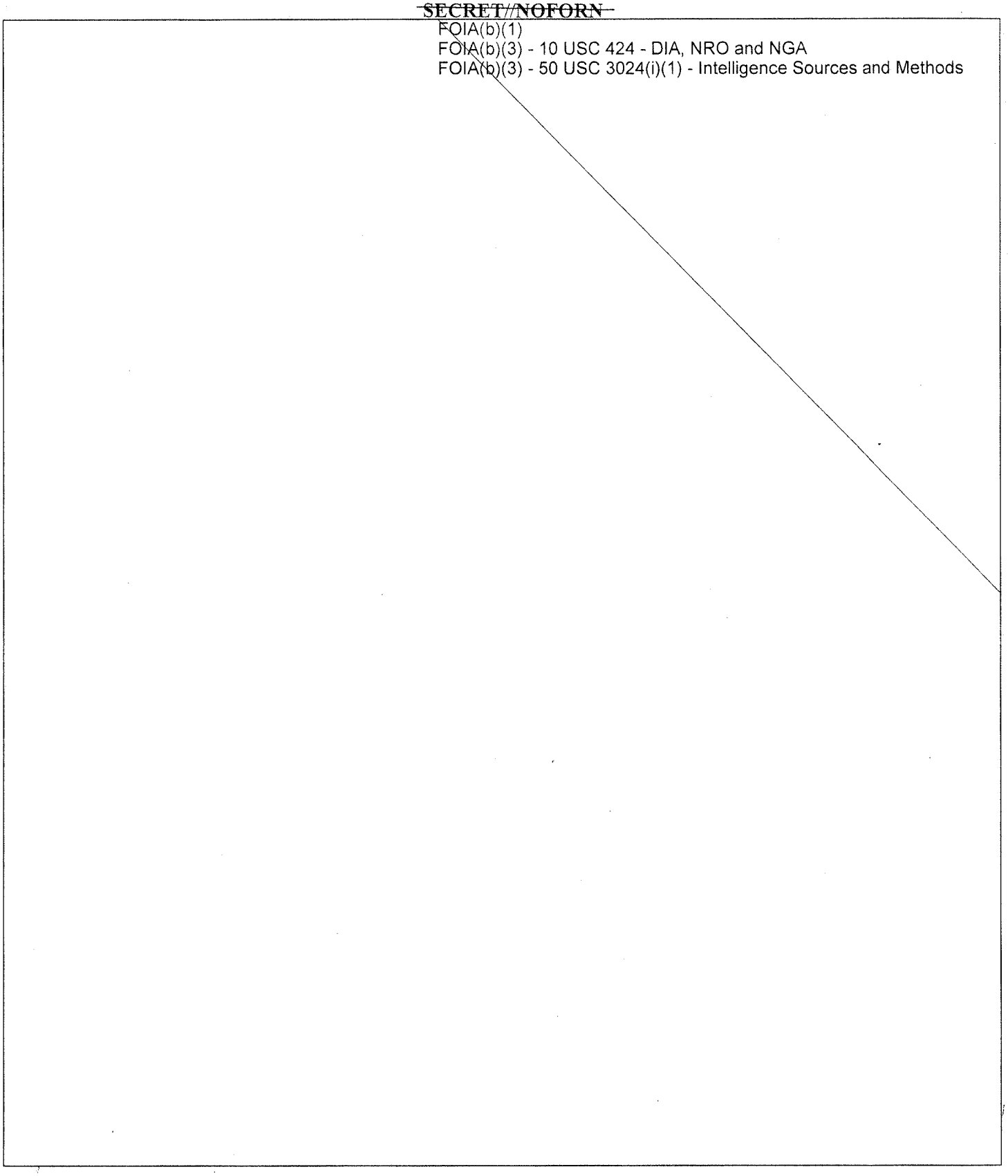
4. (U) If you have any questions or concerns, please contact the undersigned at [redacted]
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

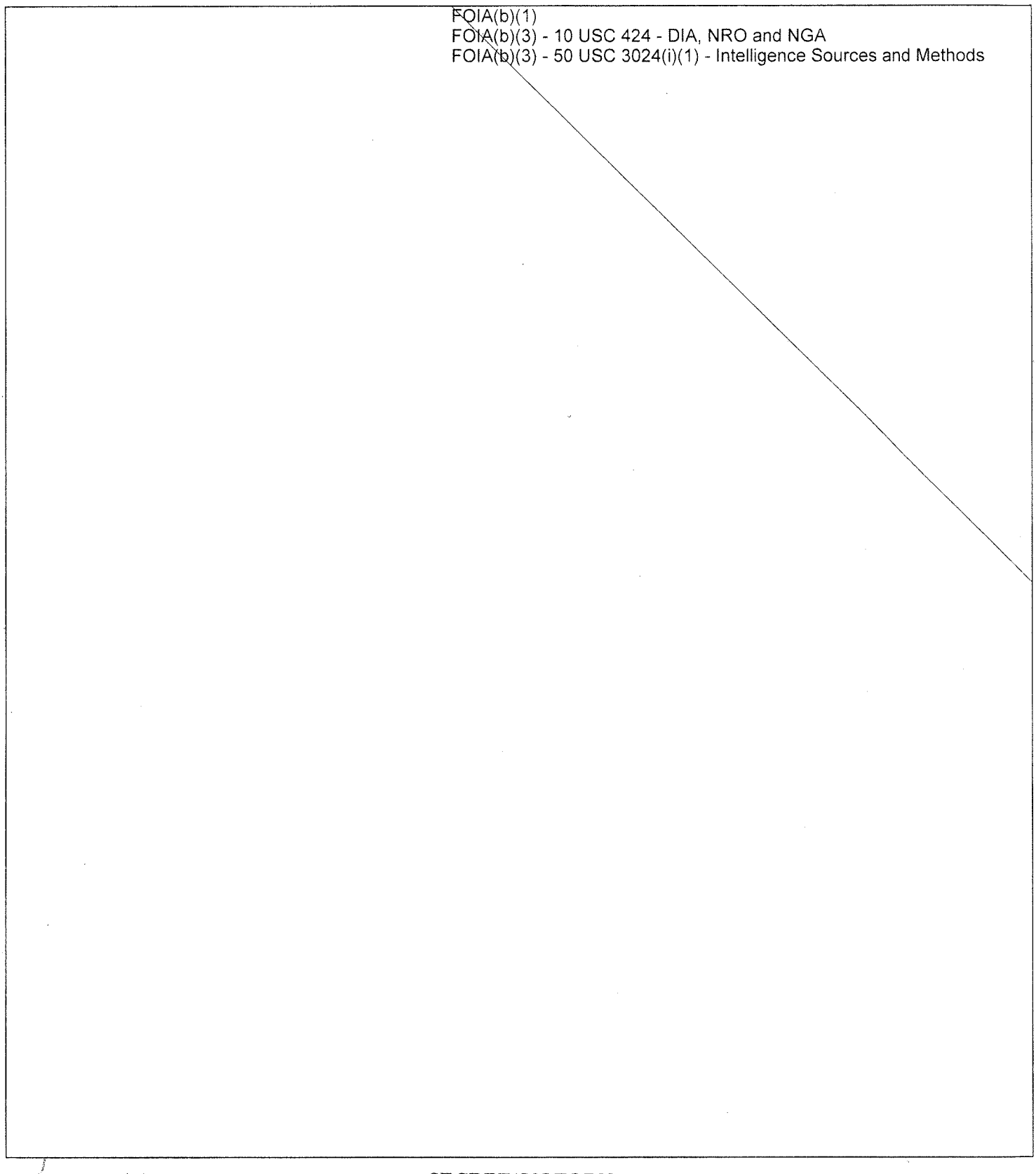
Classified By: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
Derived From: NGA SCG CON-08.1.1
Declassify On: 20371231

~~SECRET//NOFORN~~

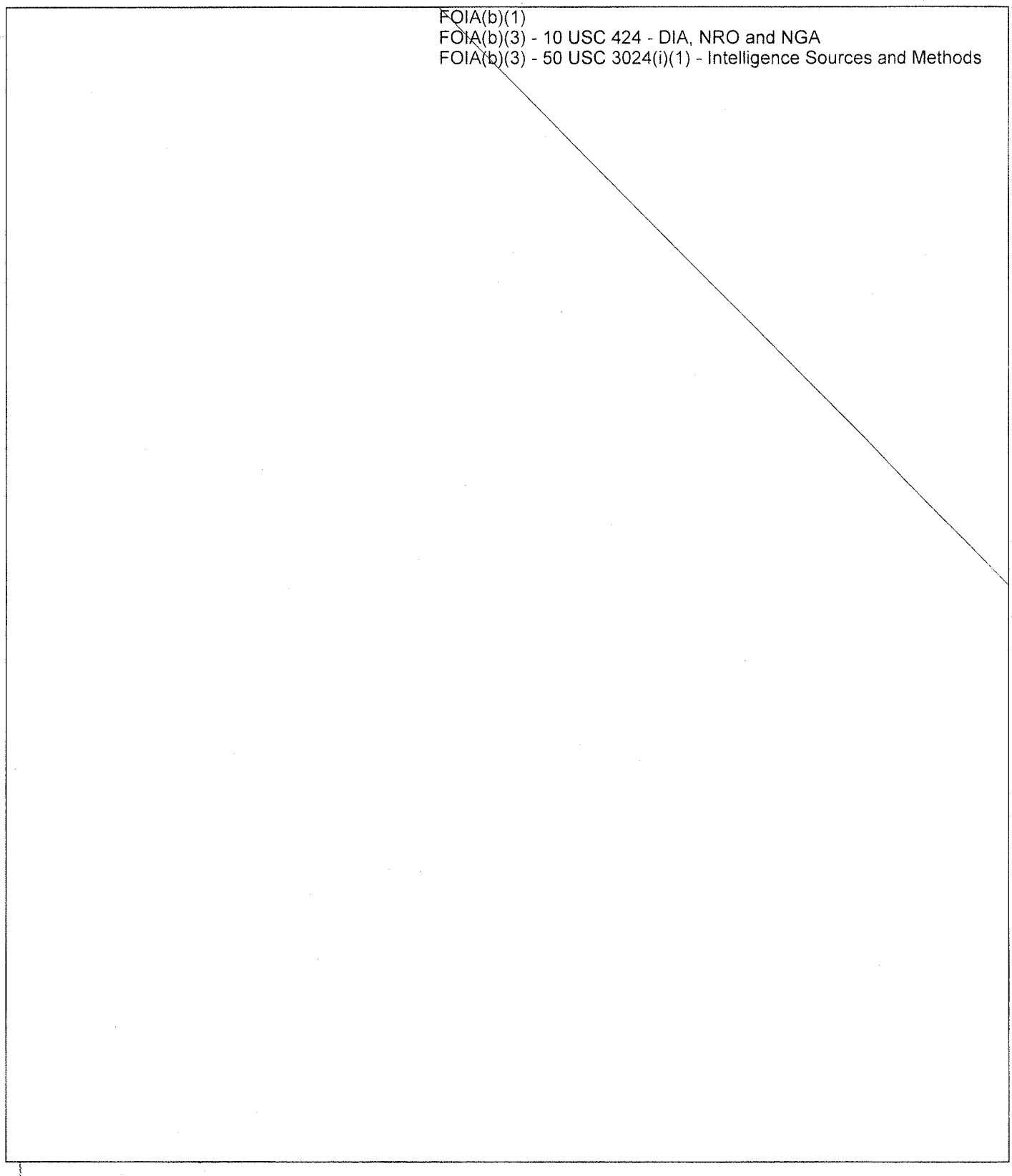
NW#:67776
DocId:34498398

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

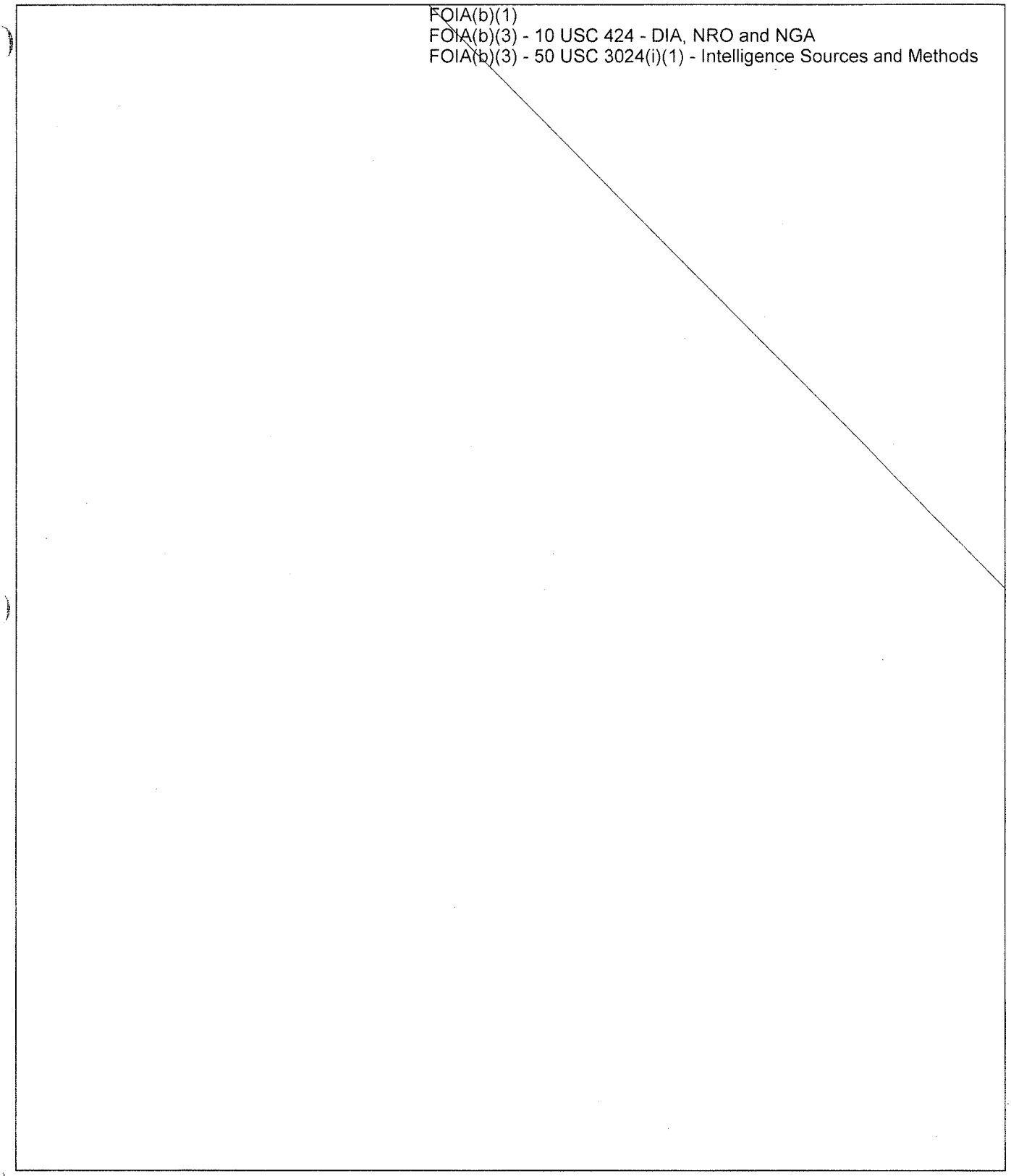




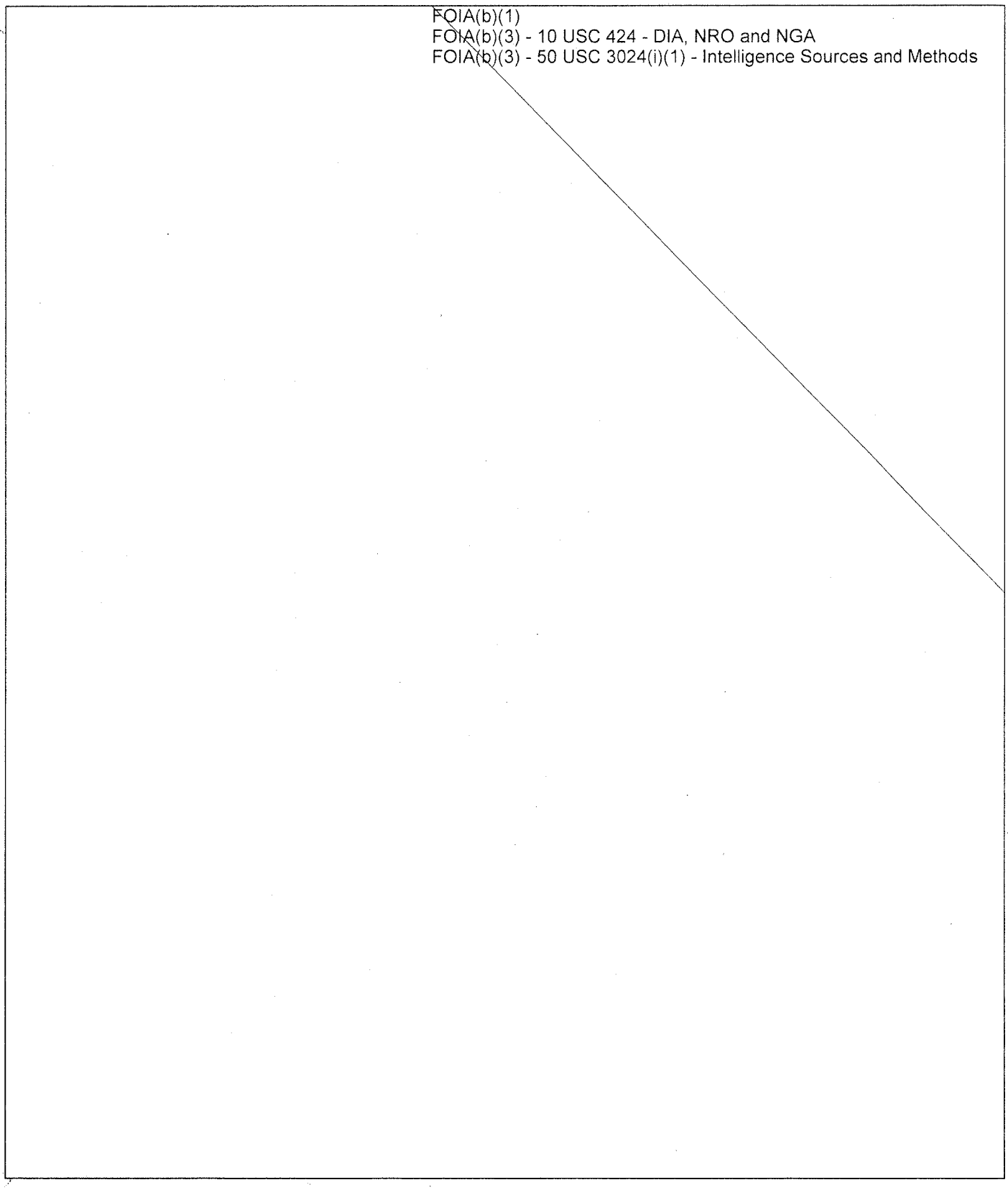
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

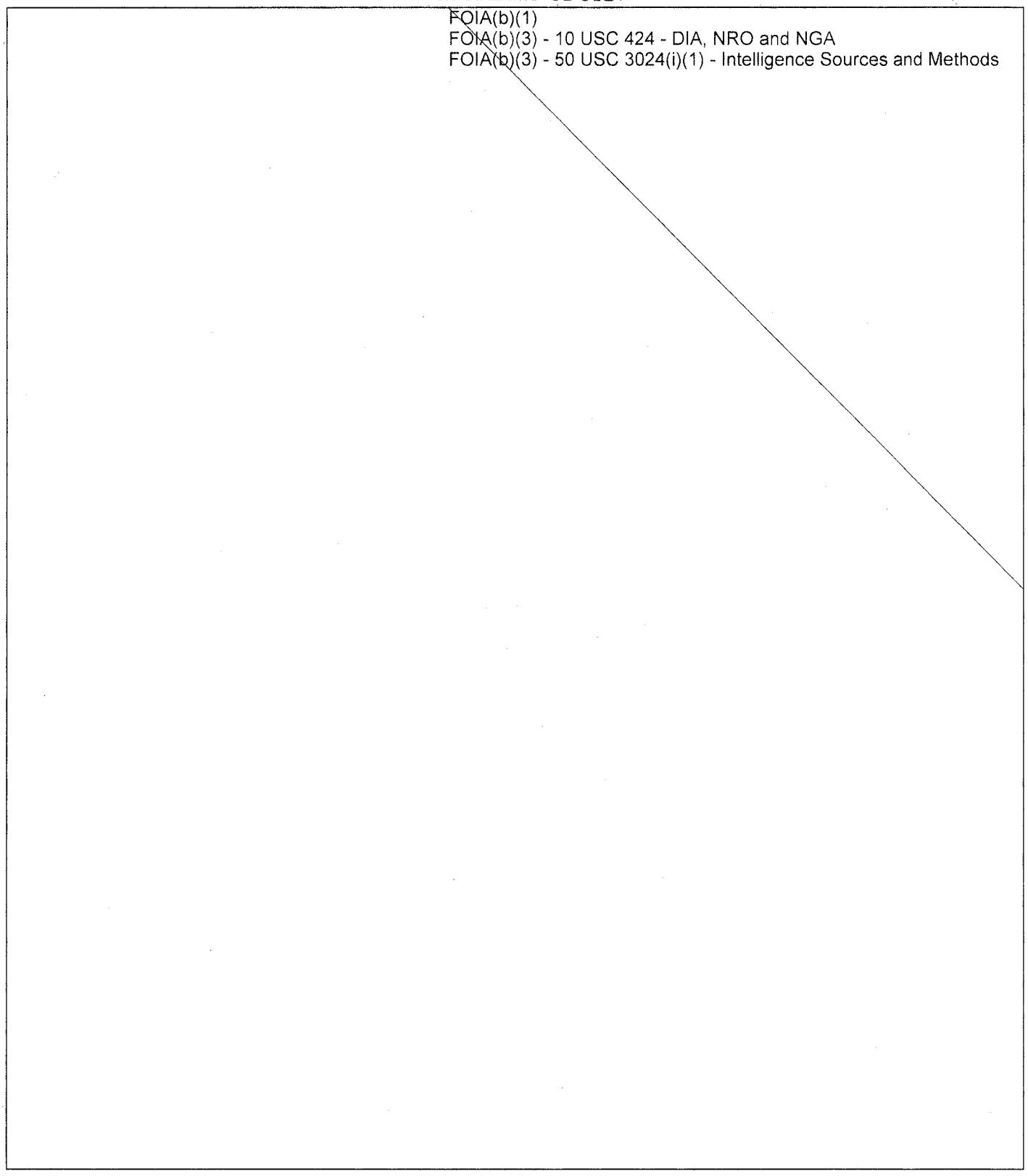


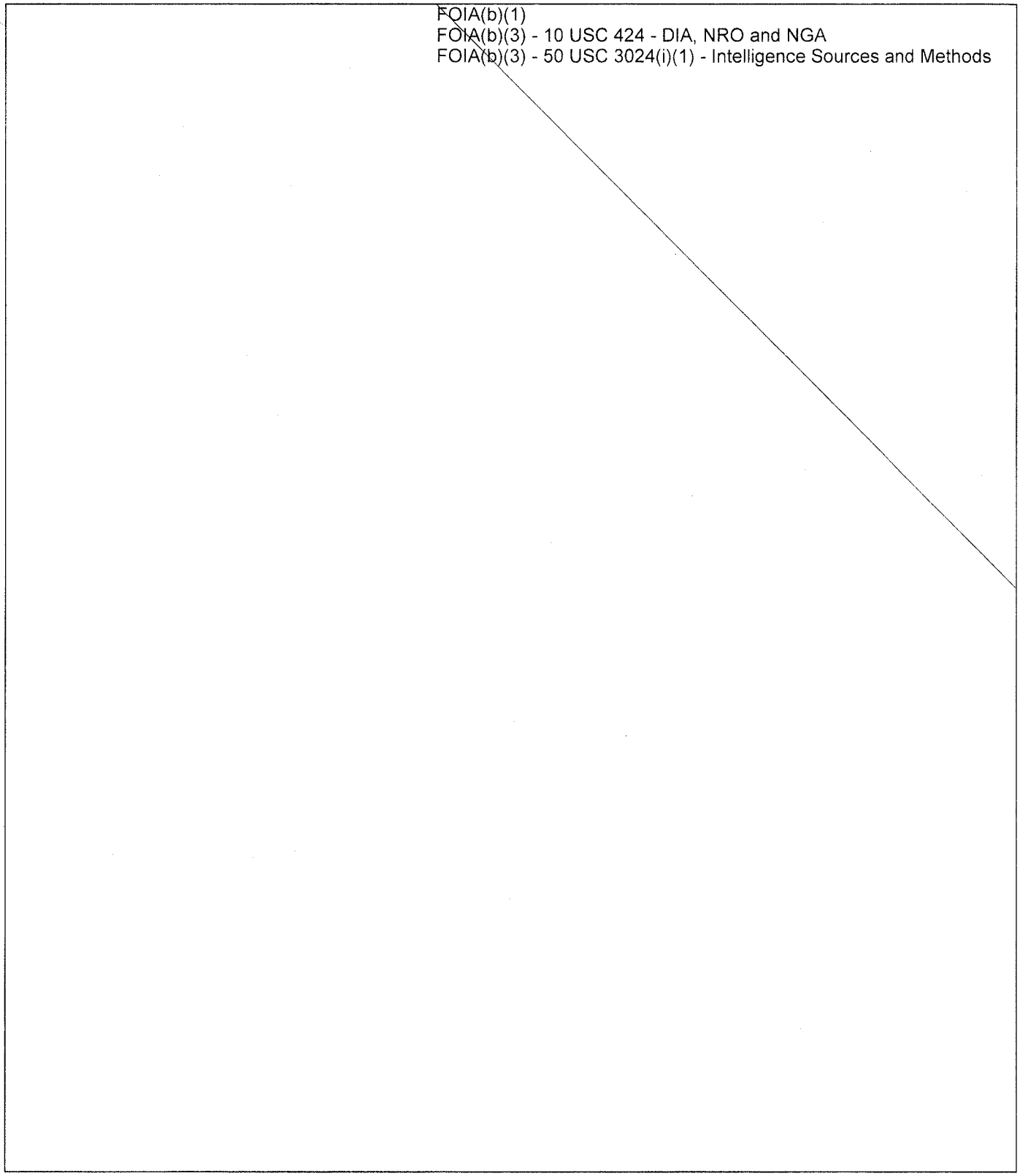
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

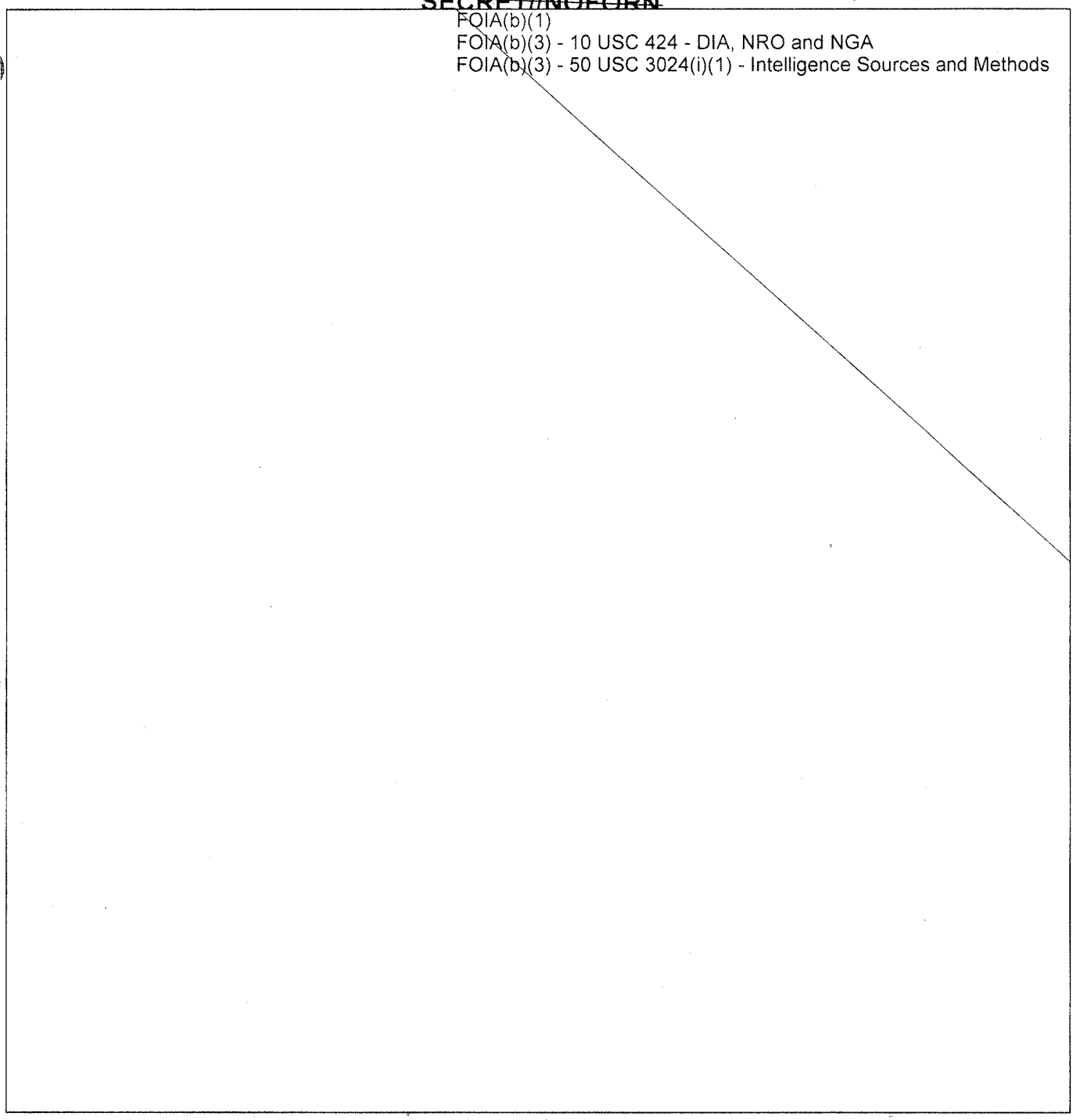






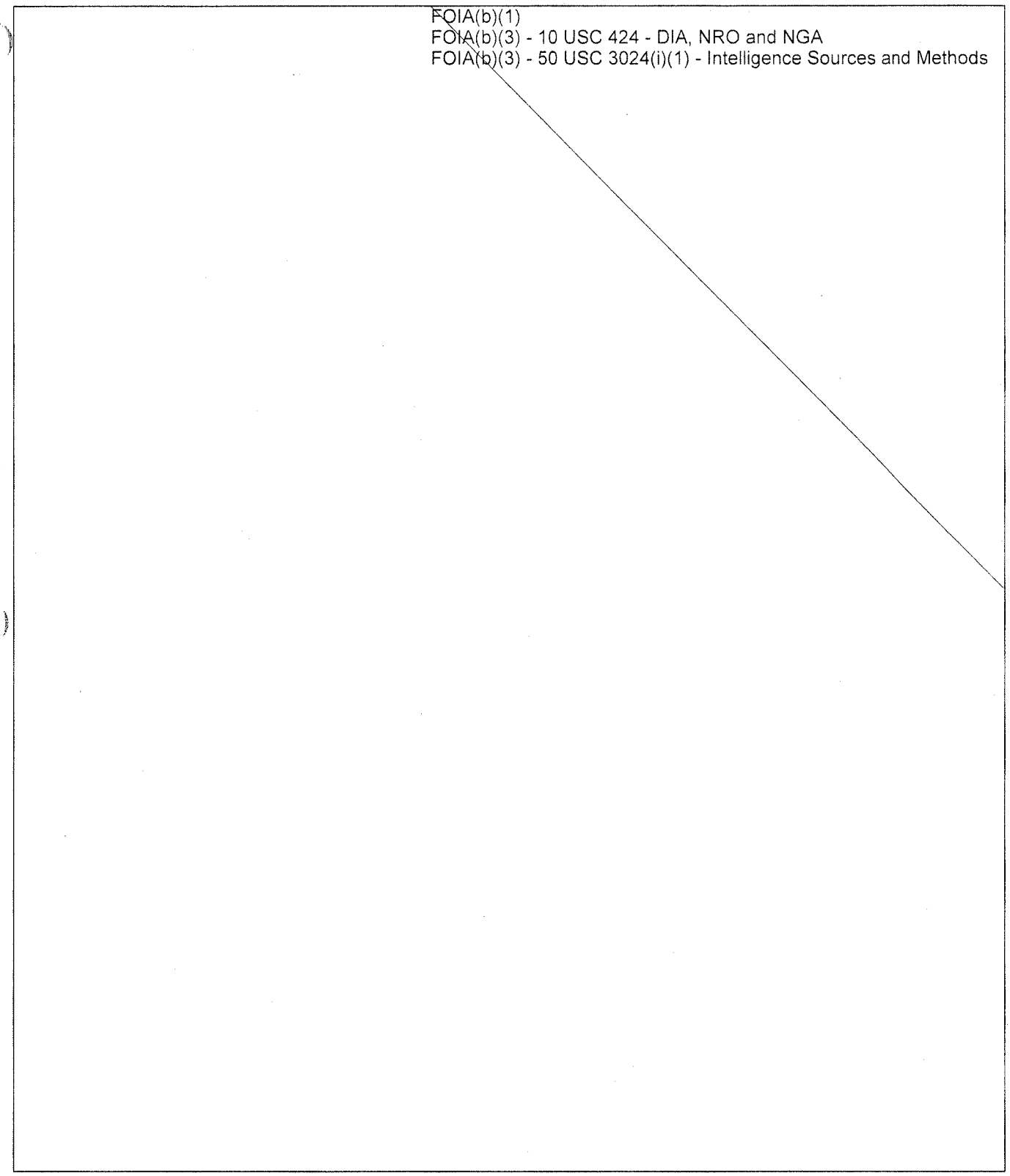
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

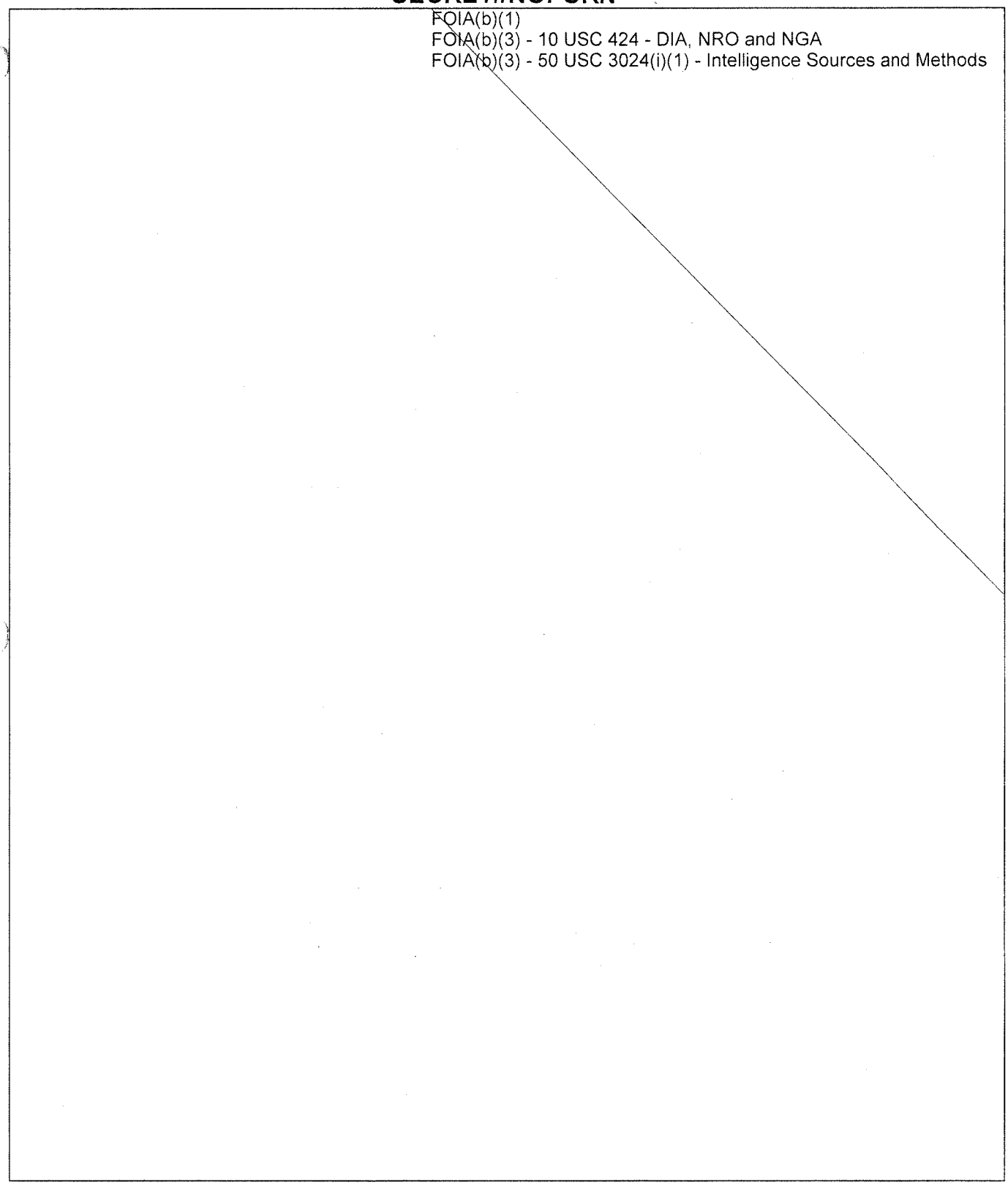
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



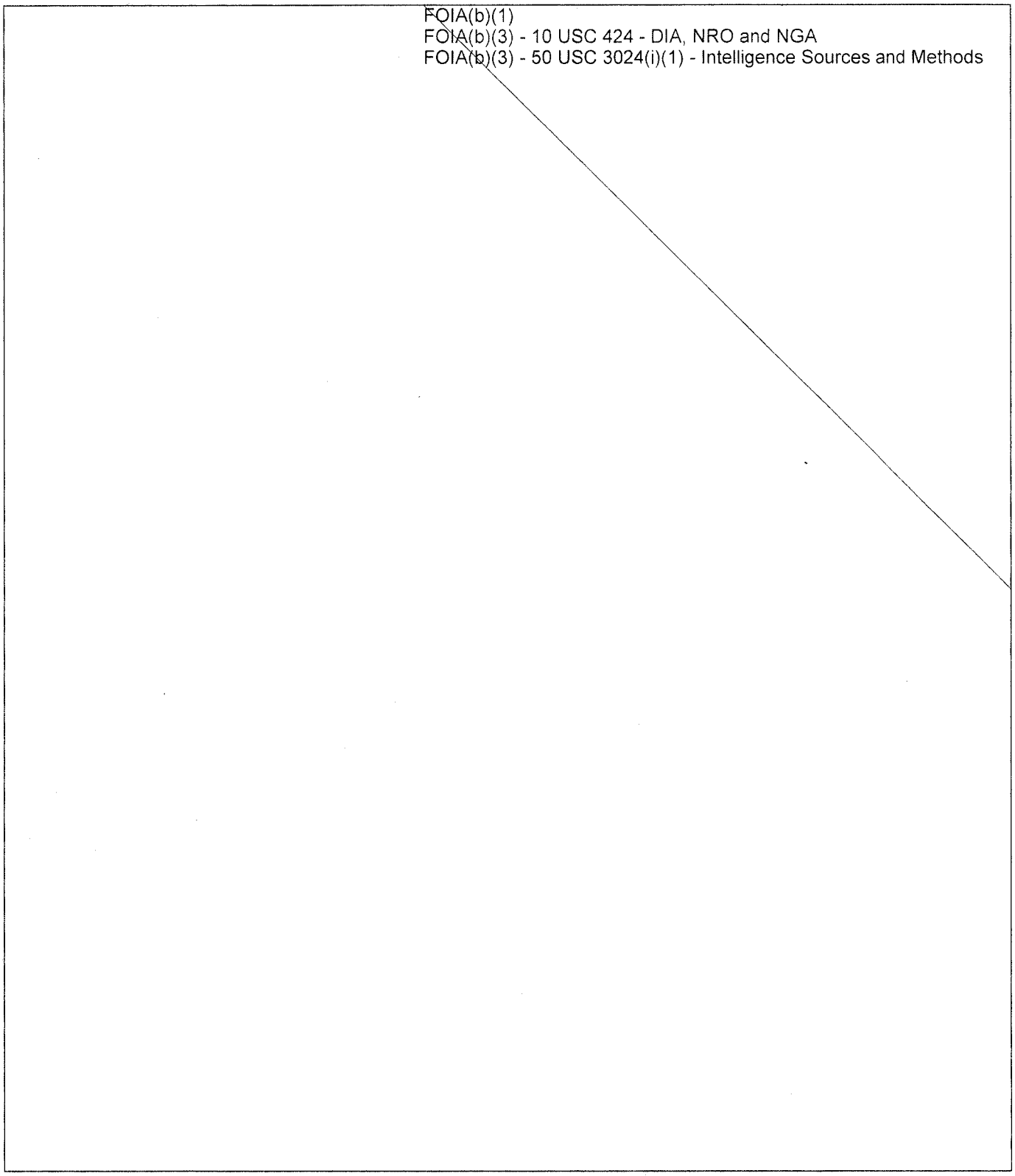
Geospatial-Intelligence Agency
Reason: 1.4(a)(c)(e)(g)
Declassify On: 20371016

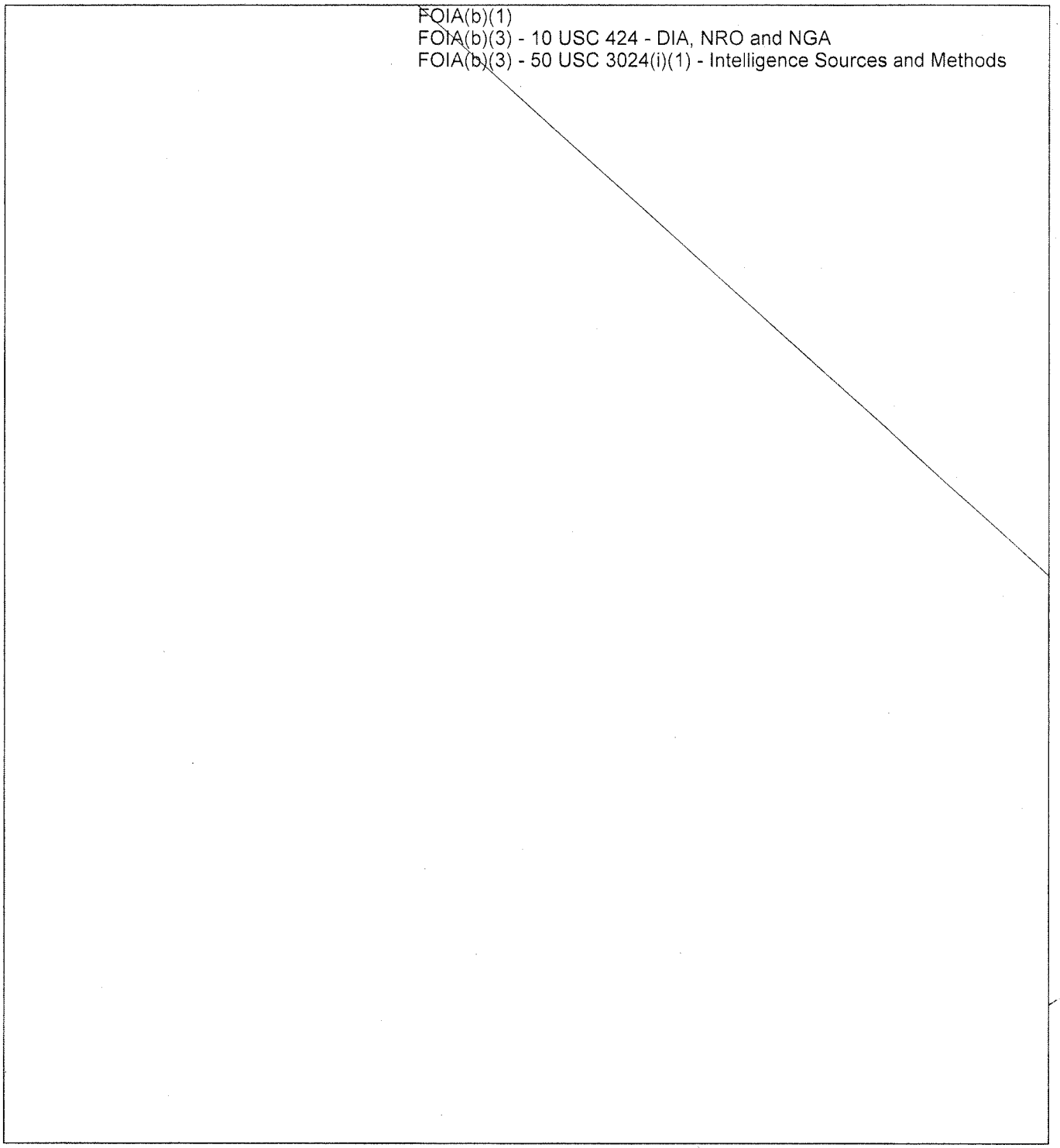
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)



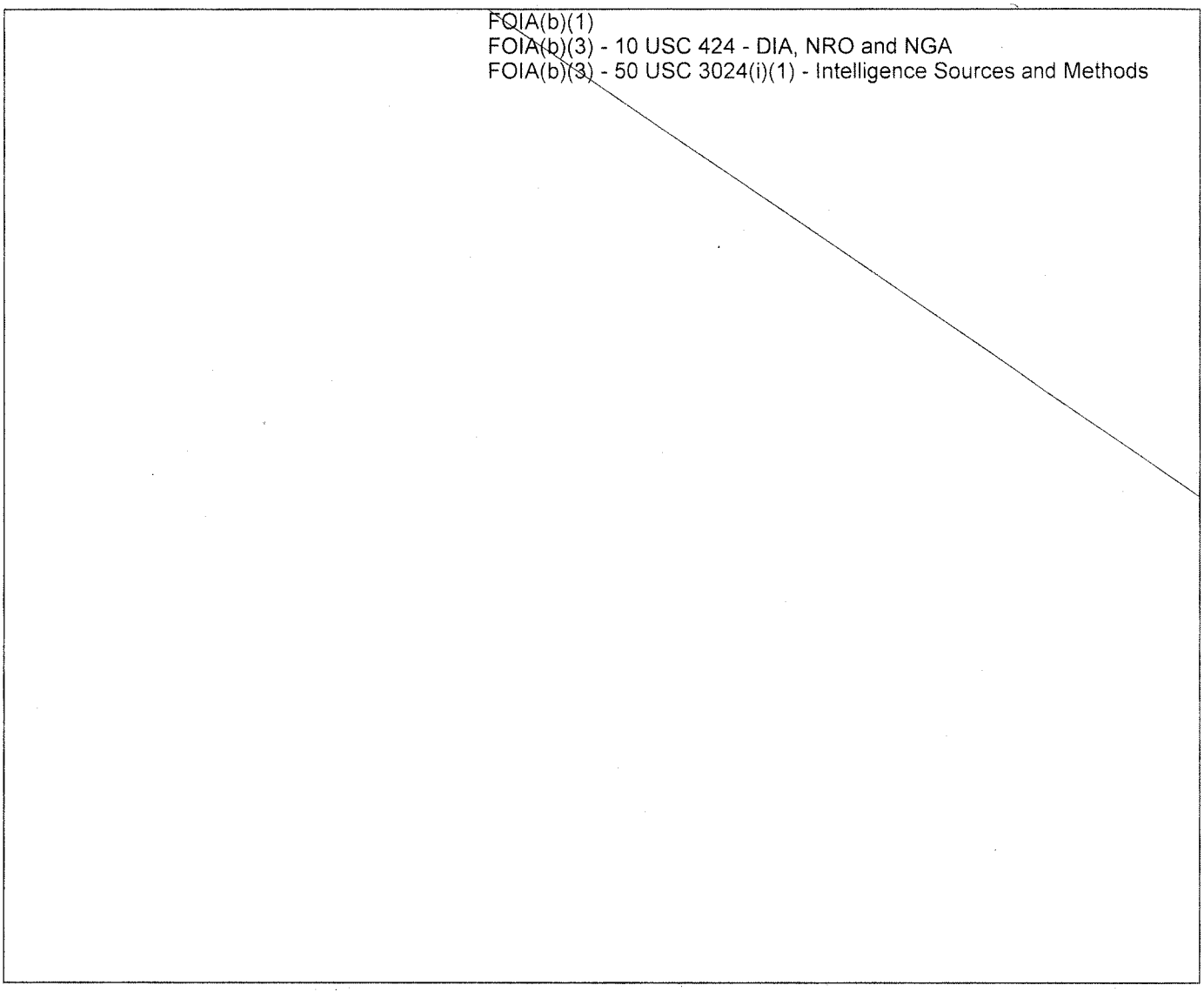


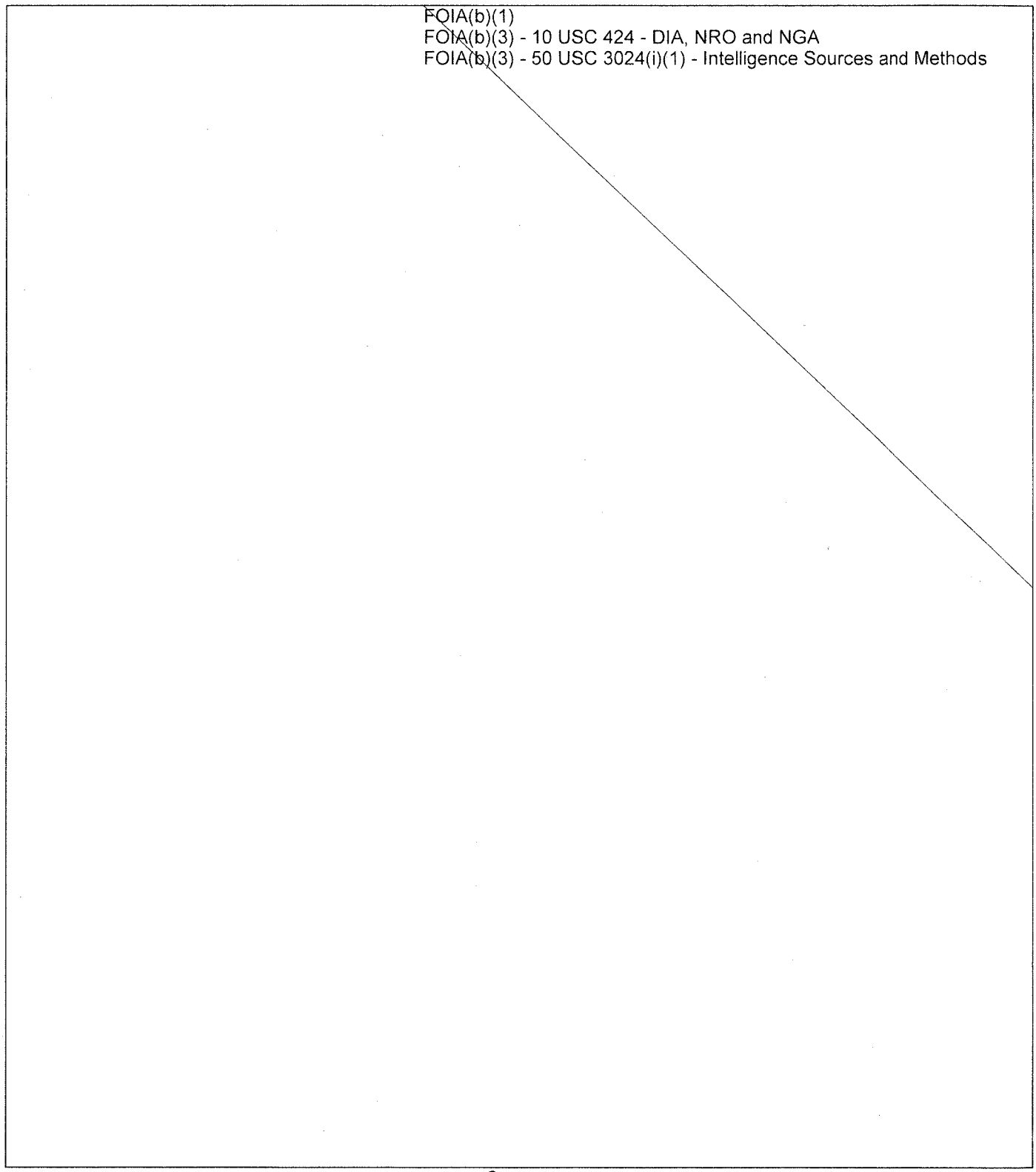
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

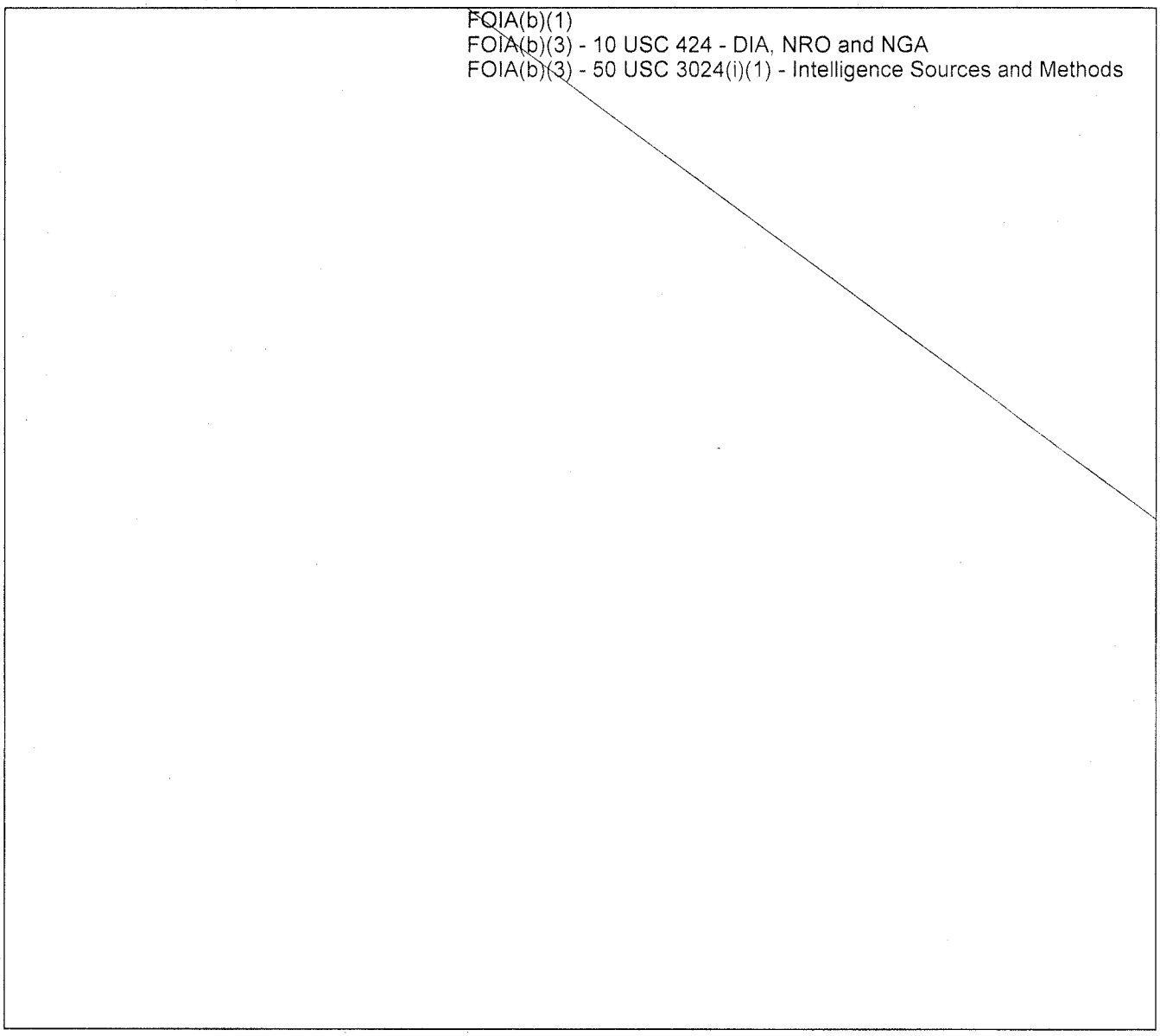


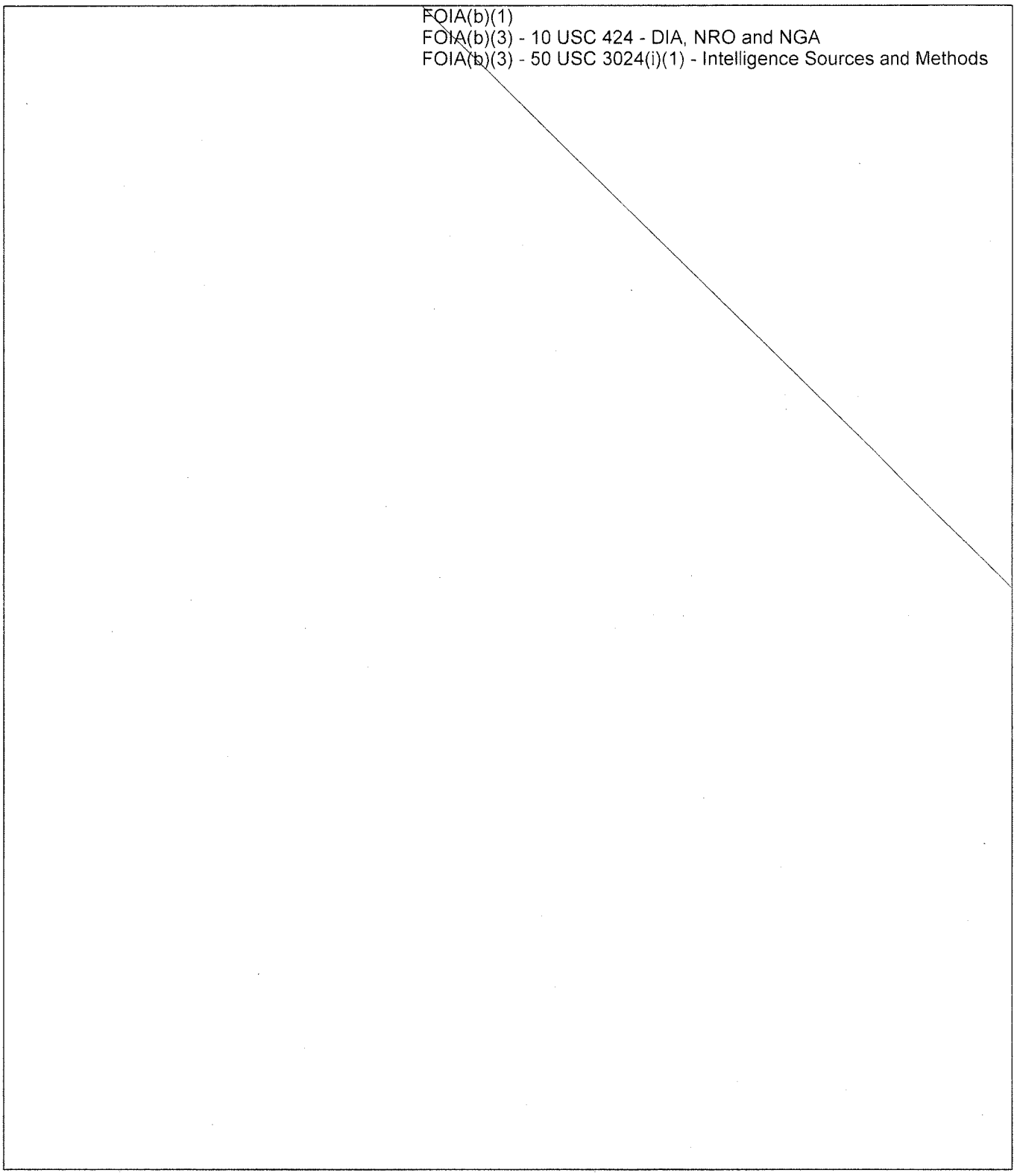


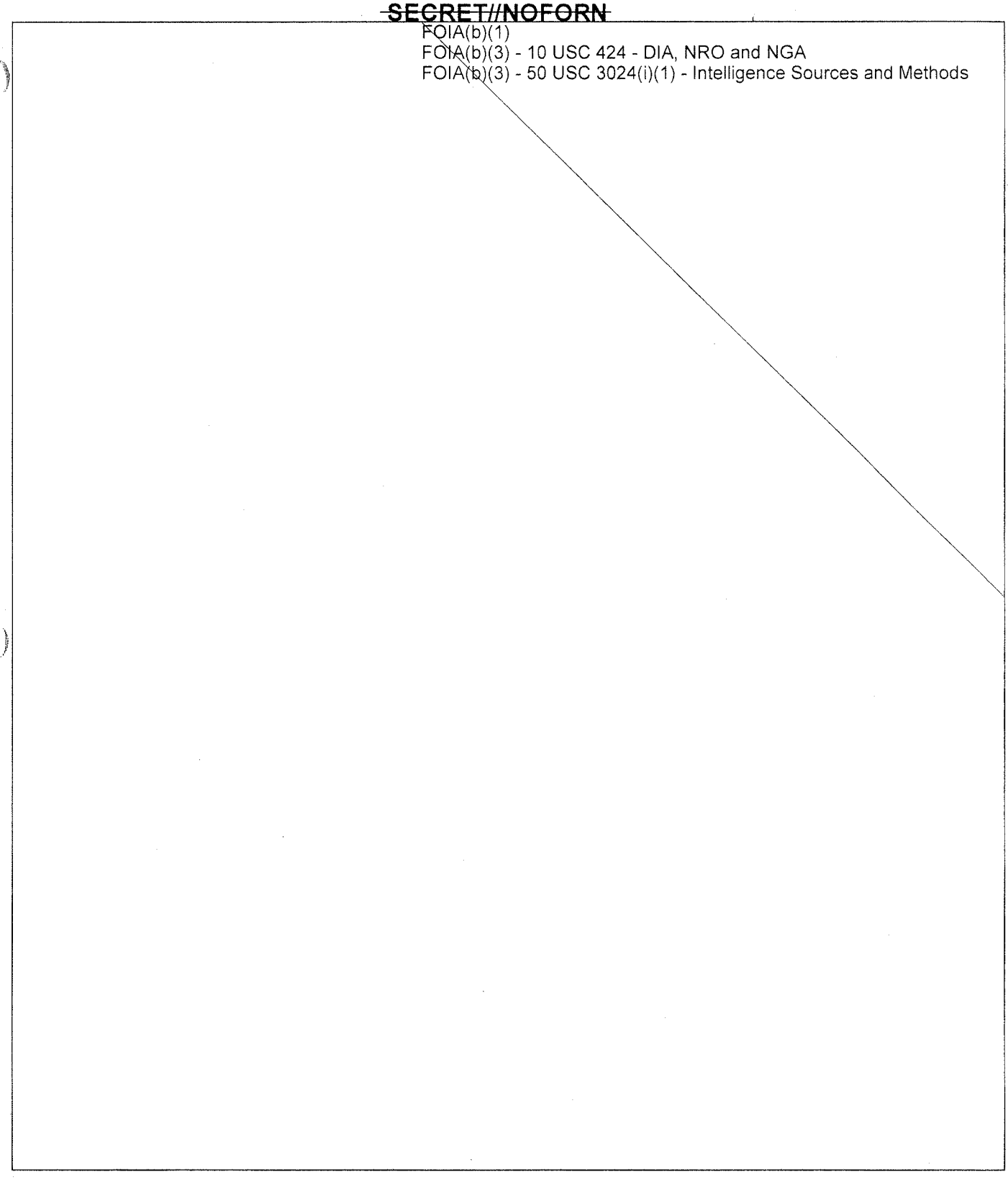

17



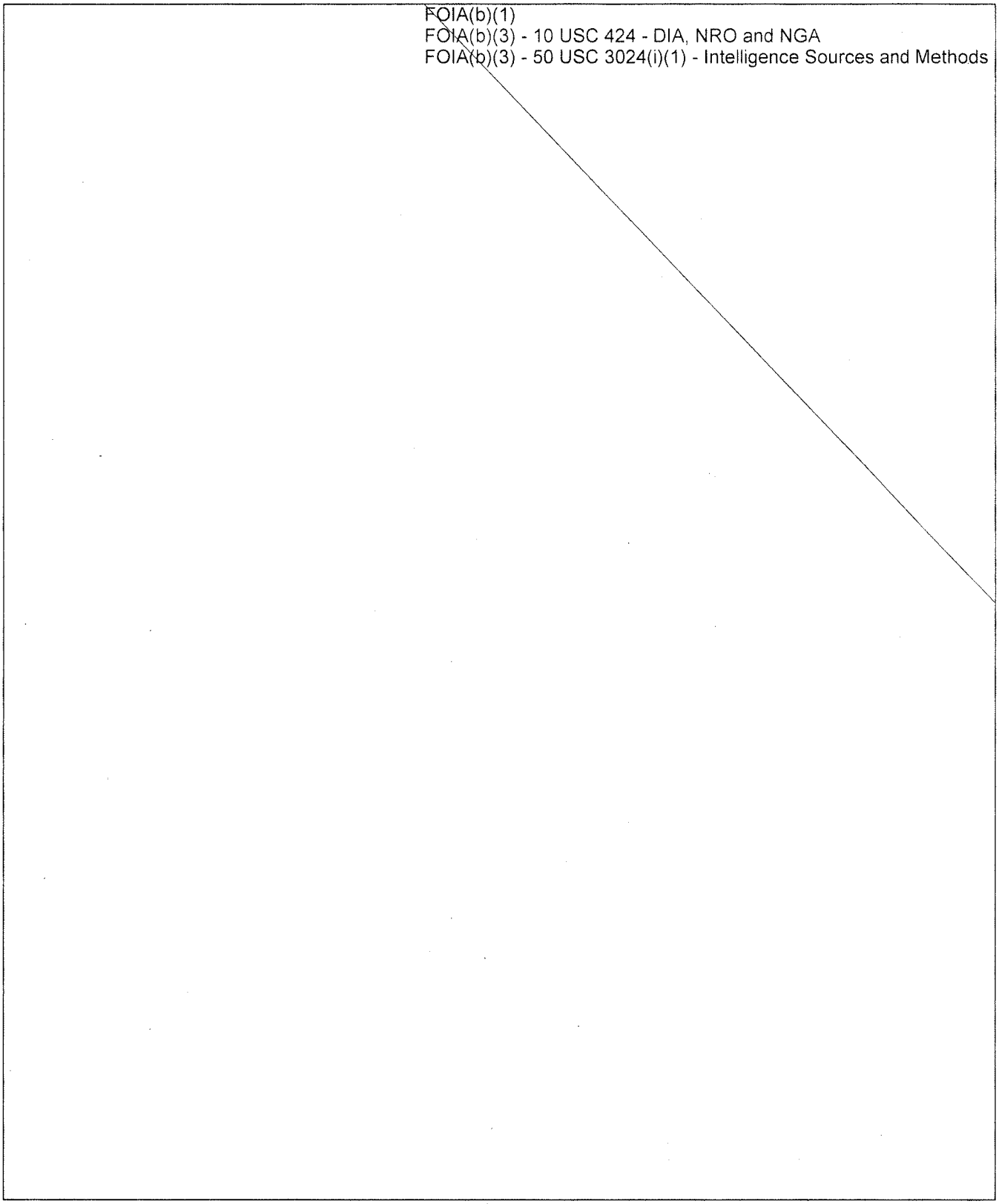


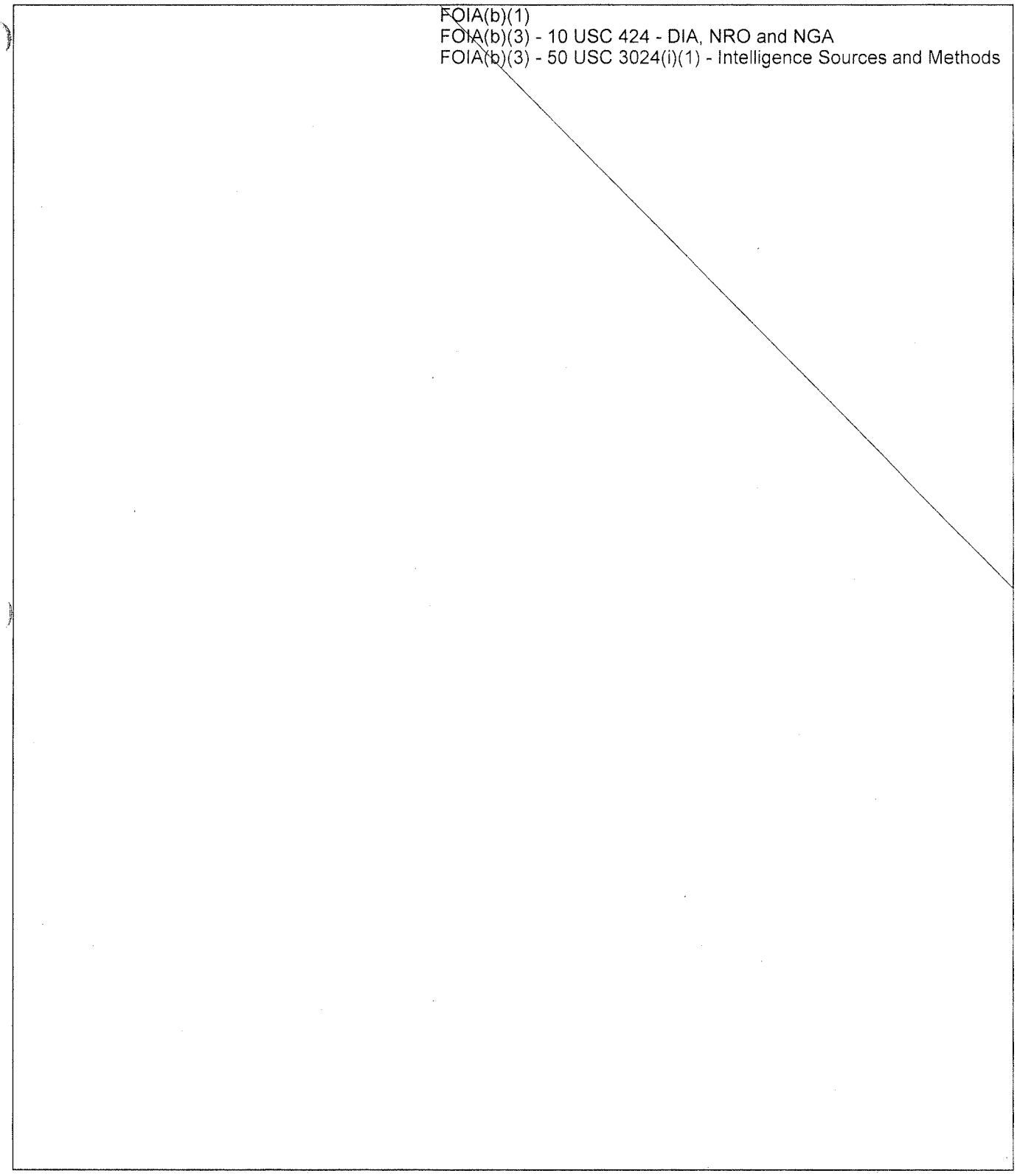




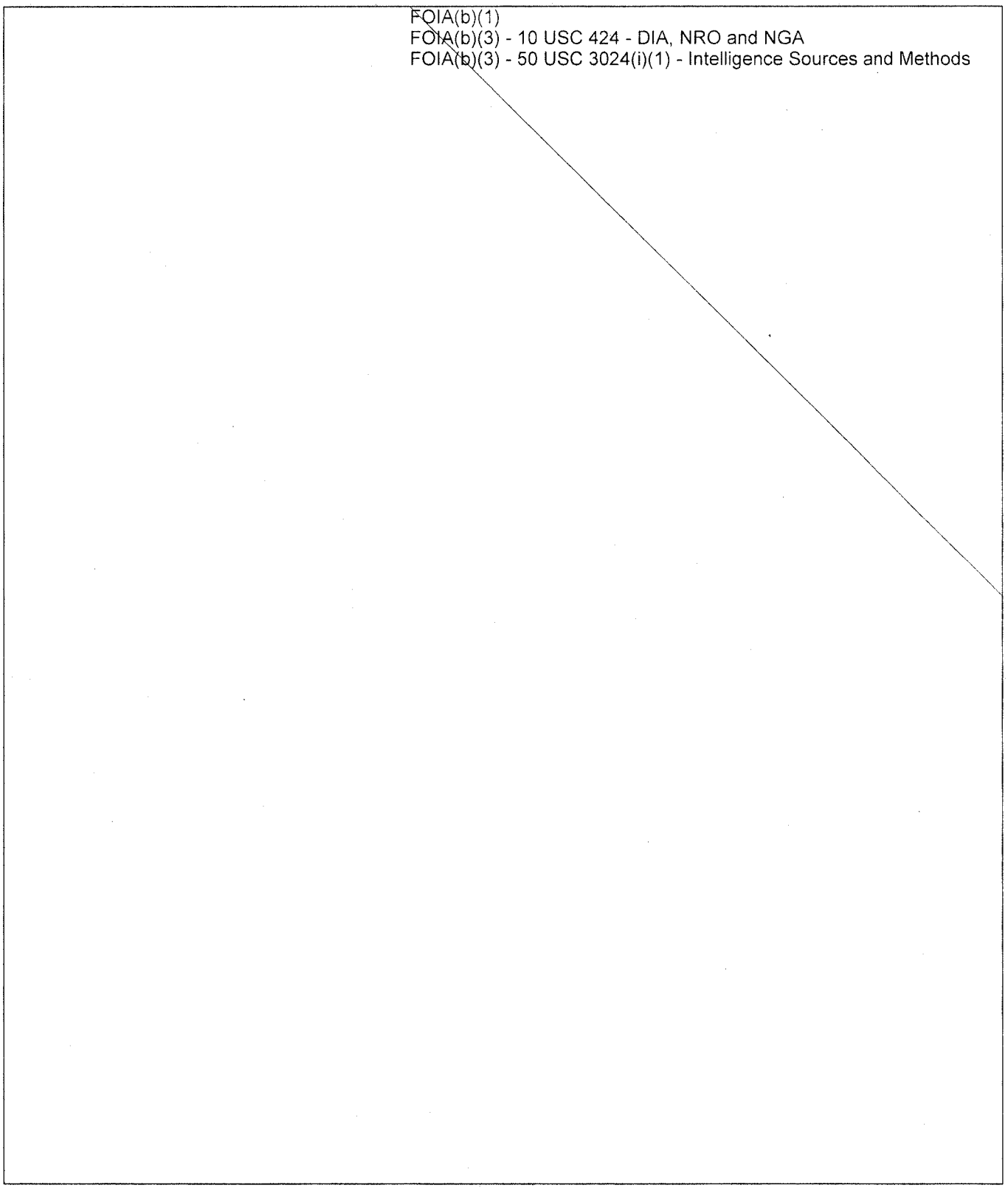


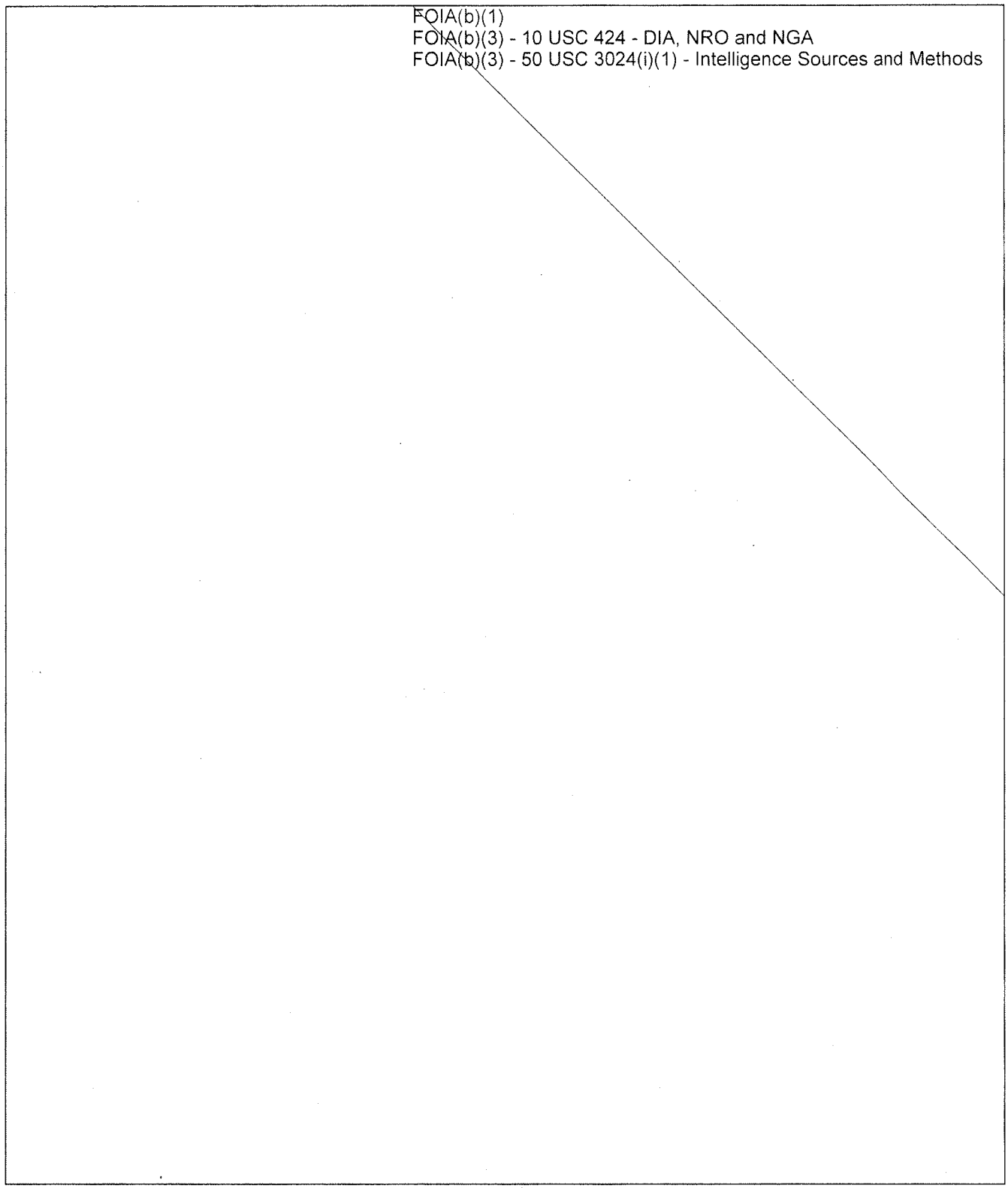
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



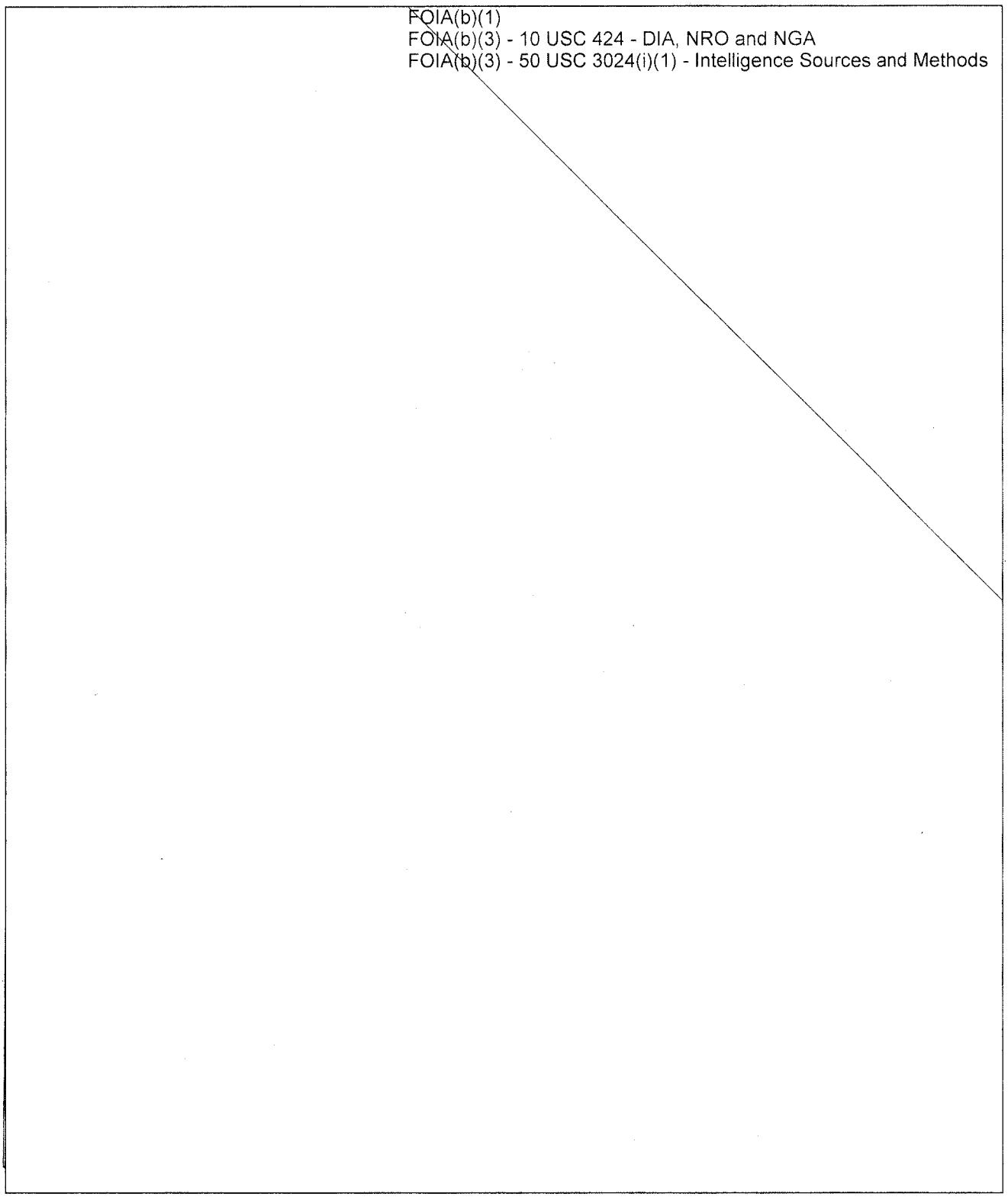


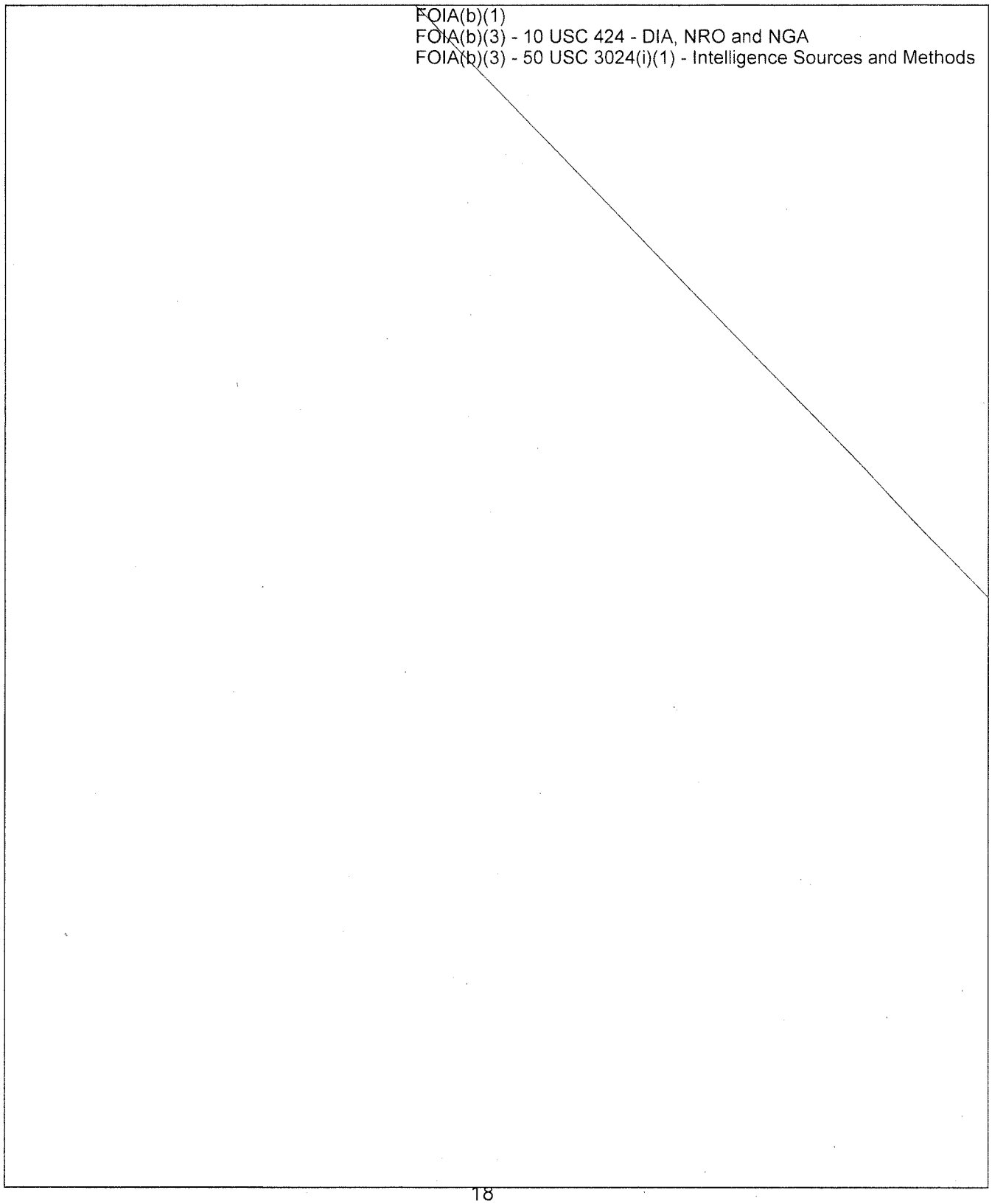
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



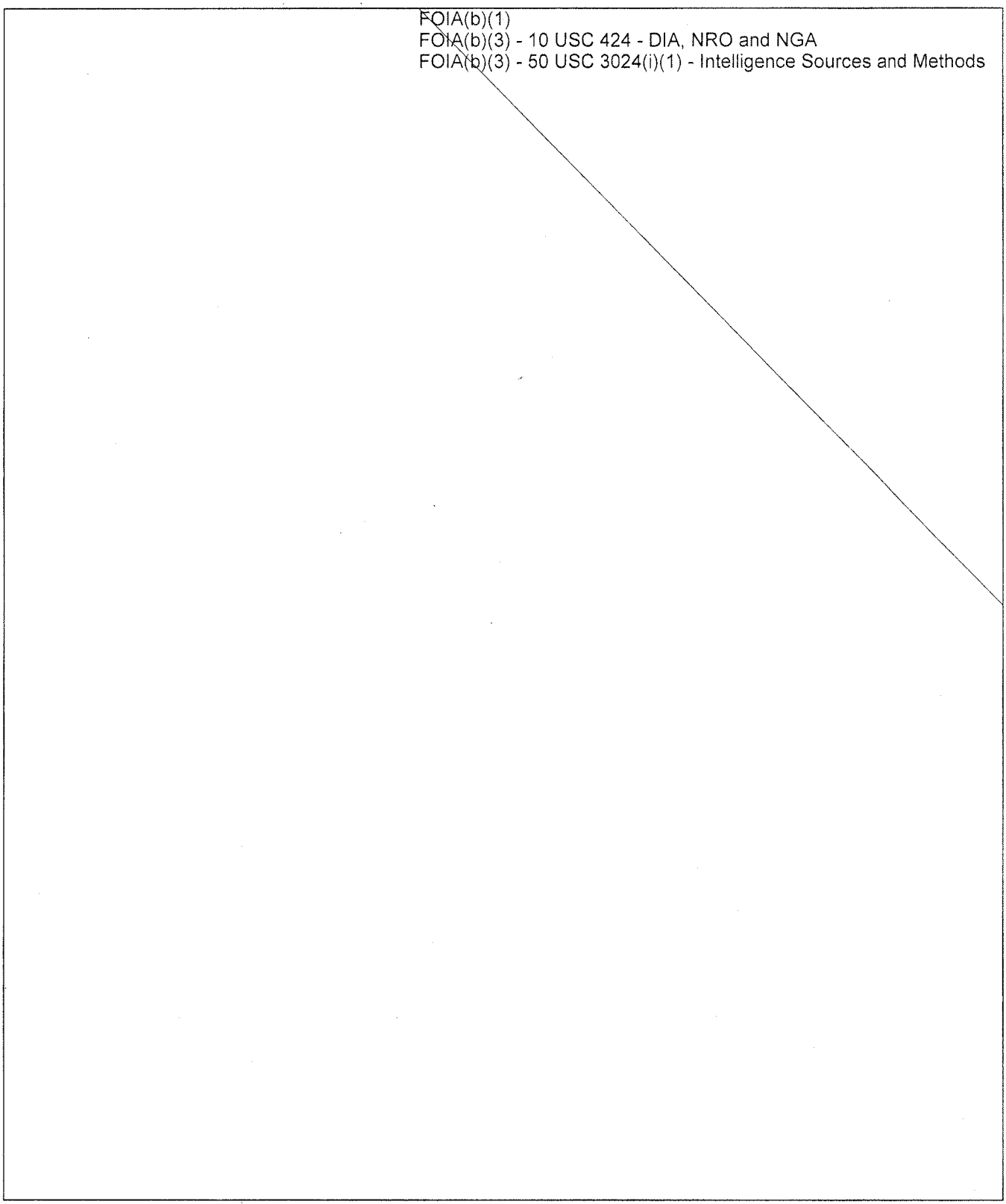


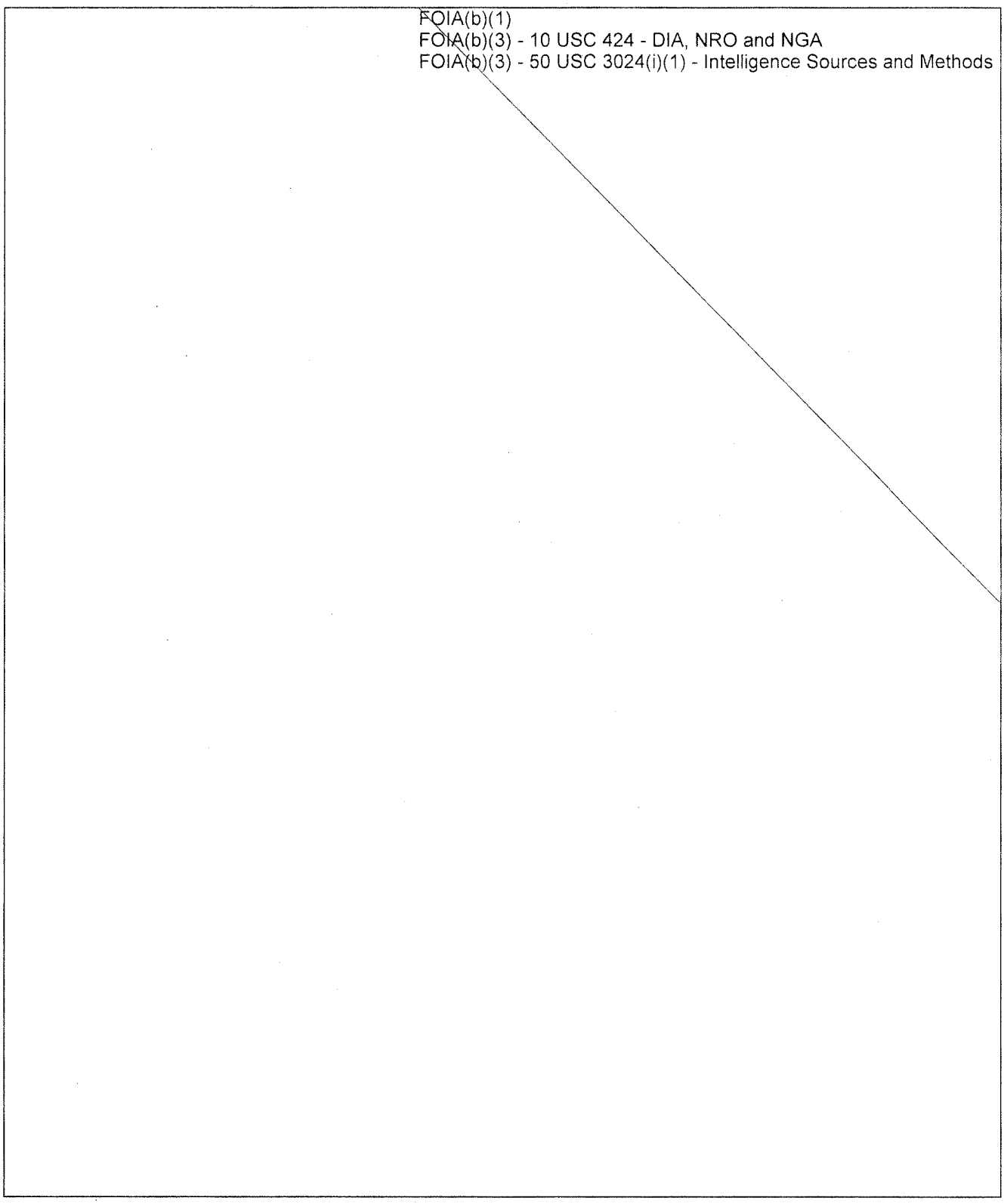
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods





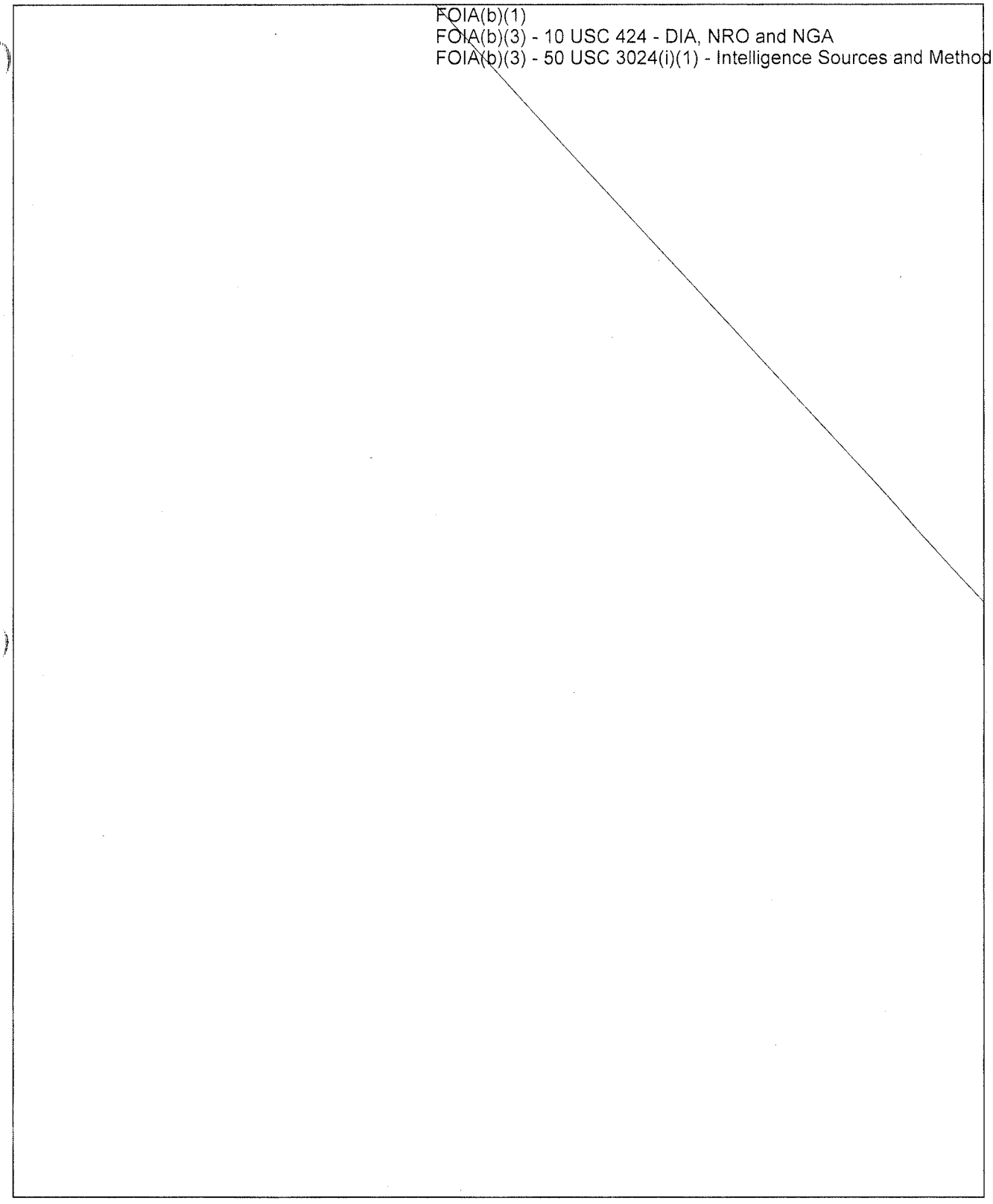
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

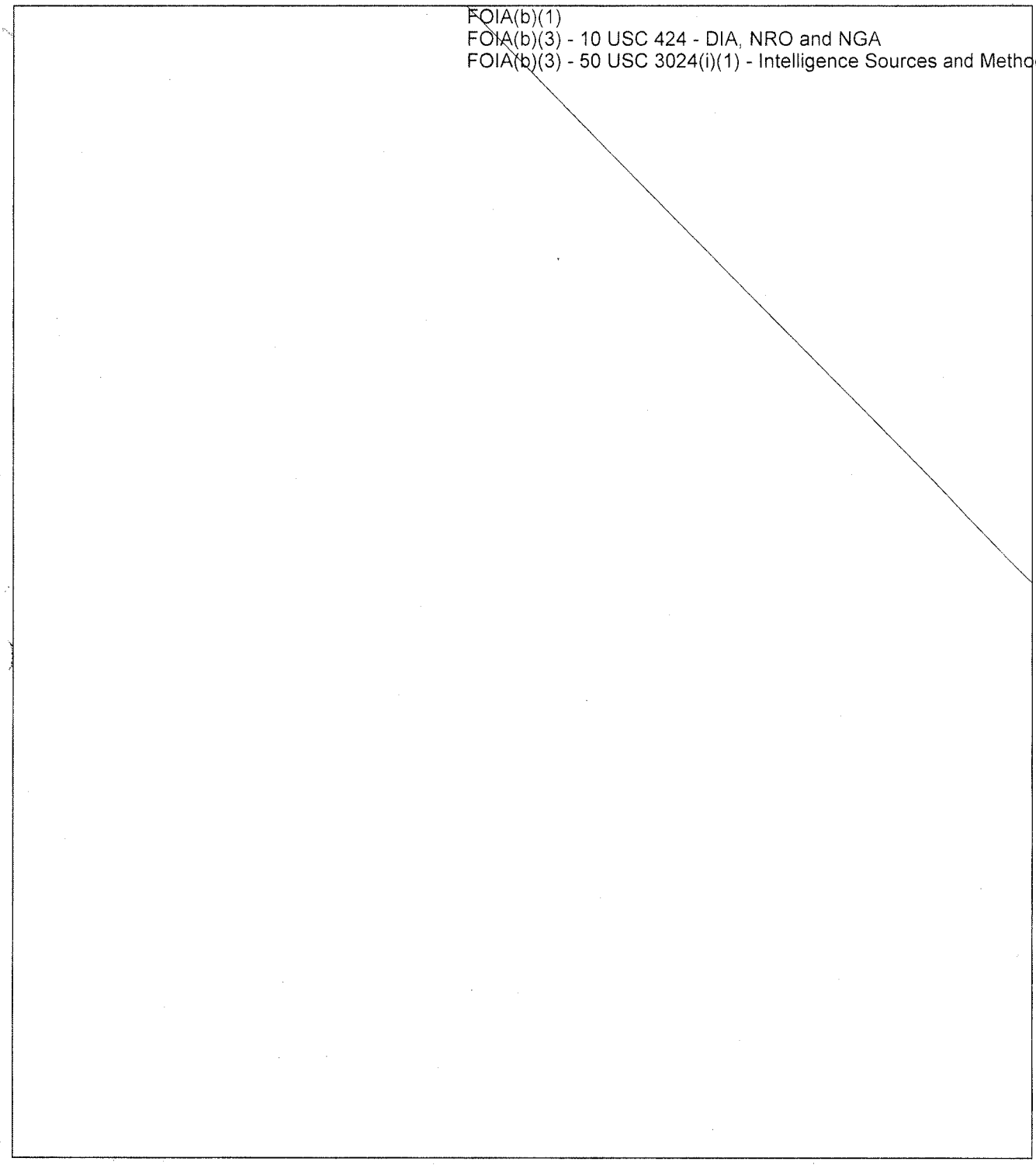


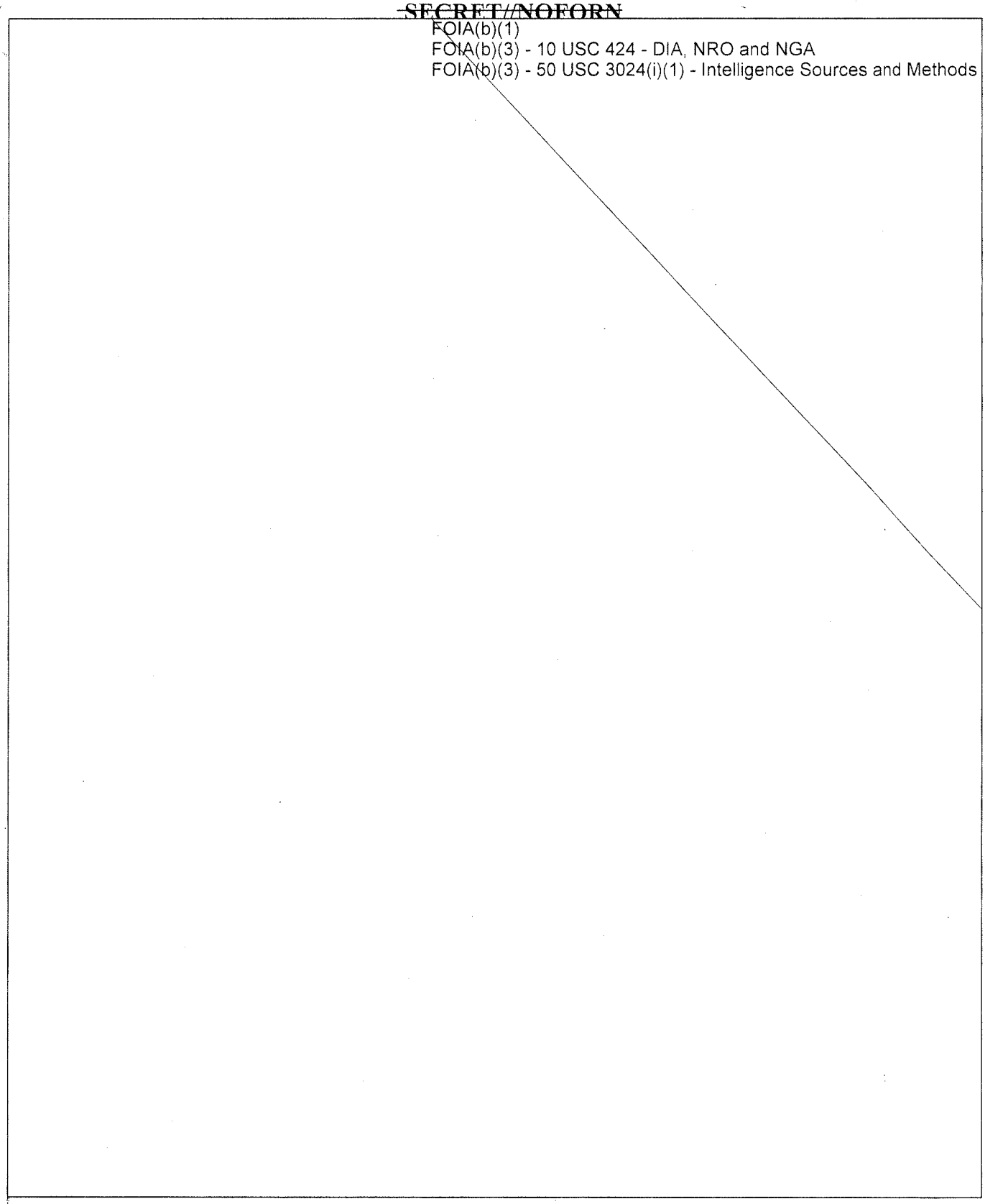


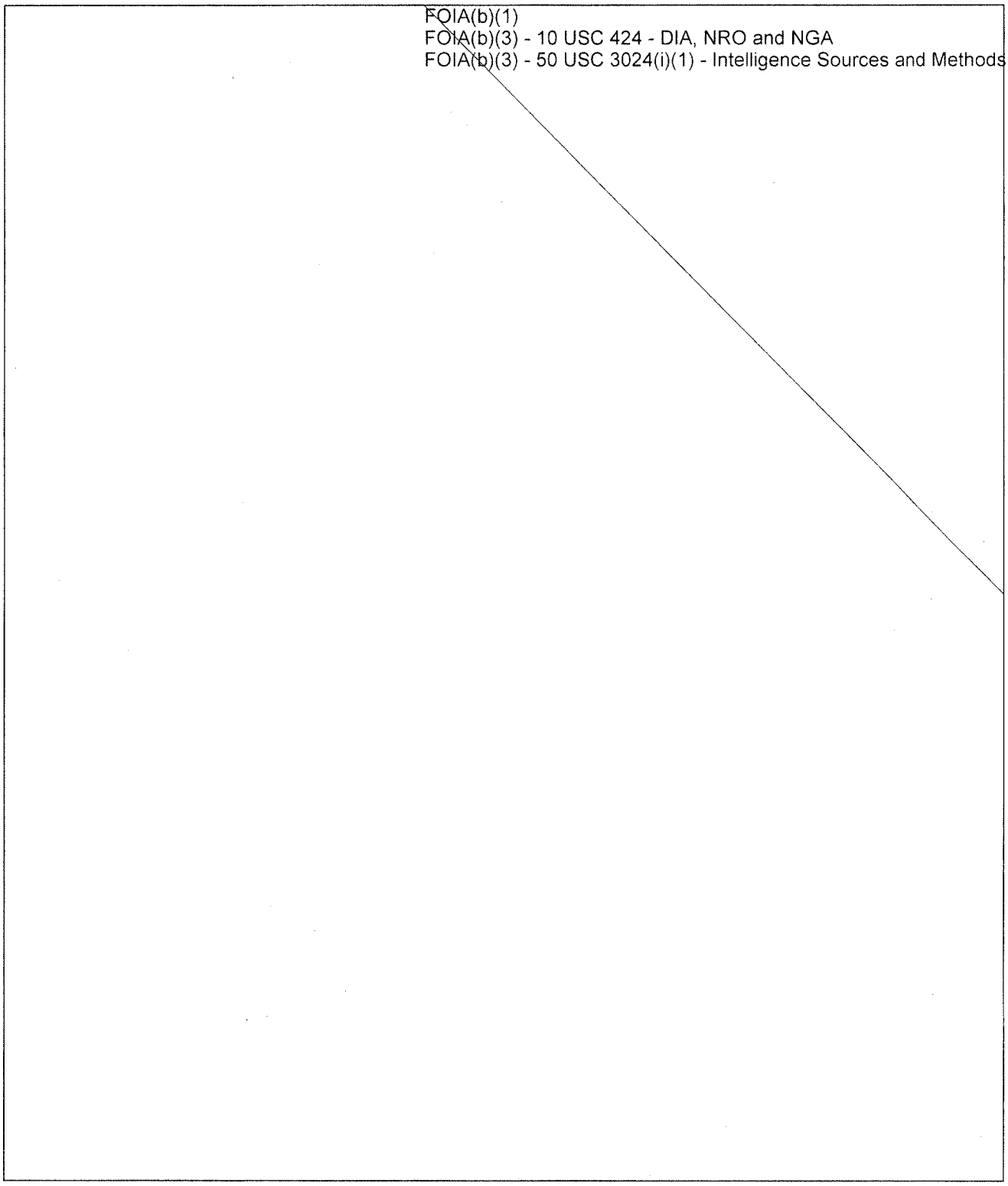
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

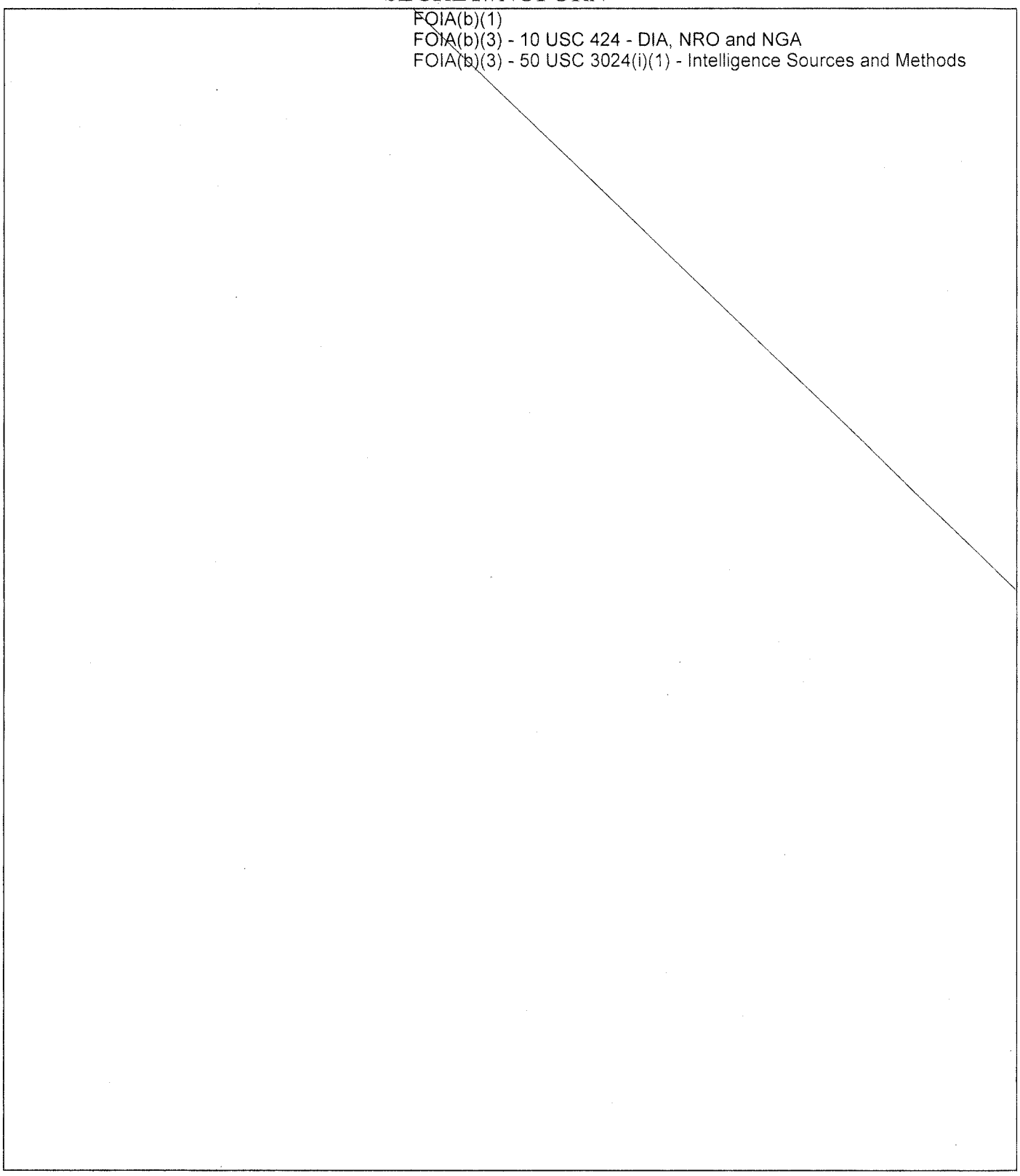
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

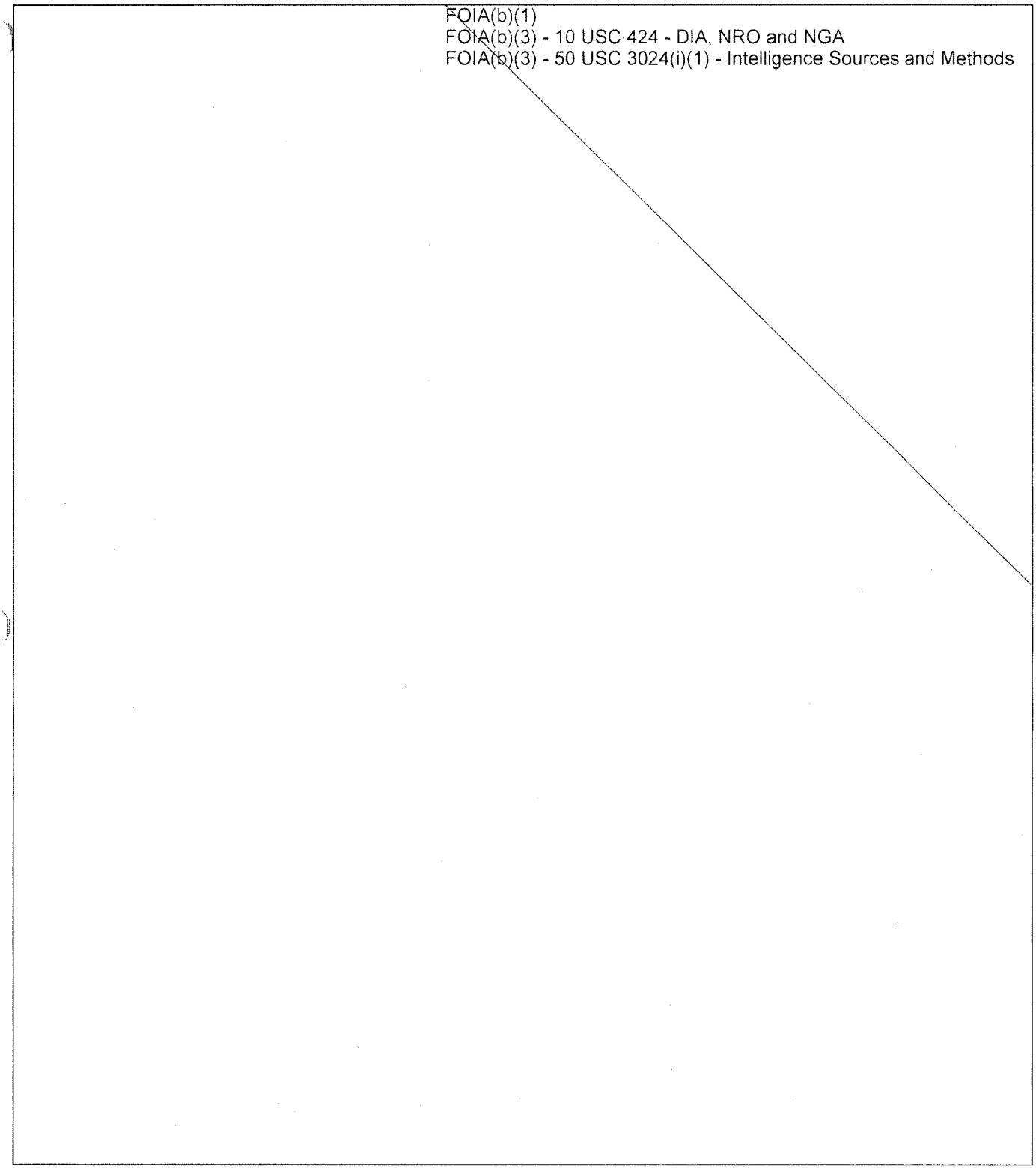


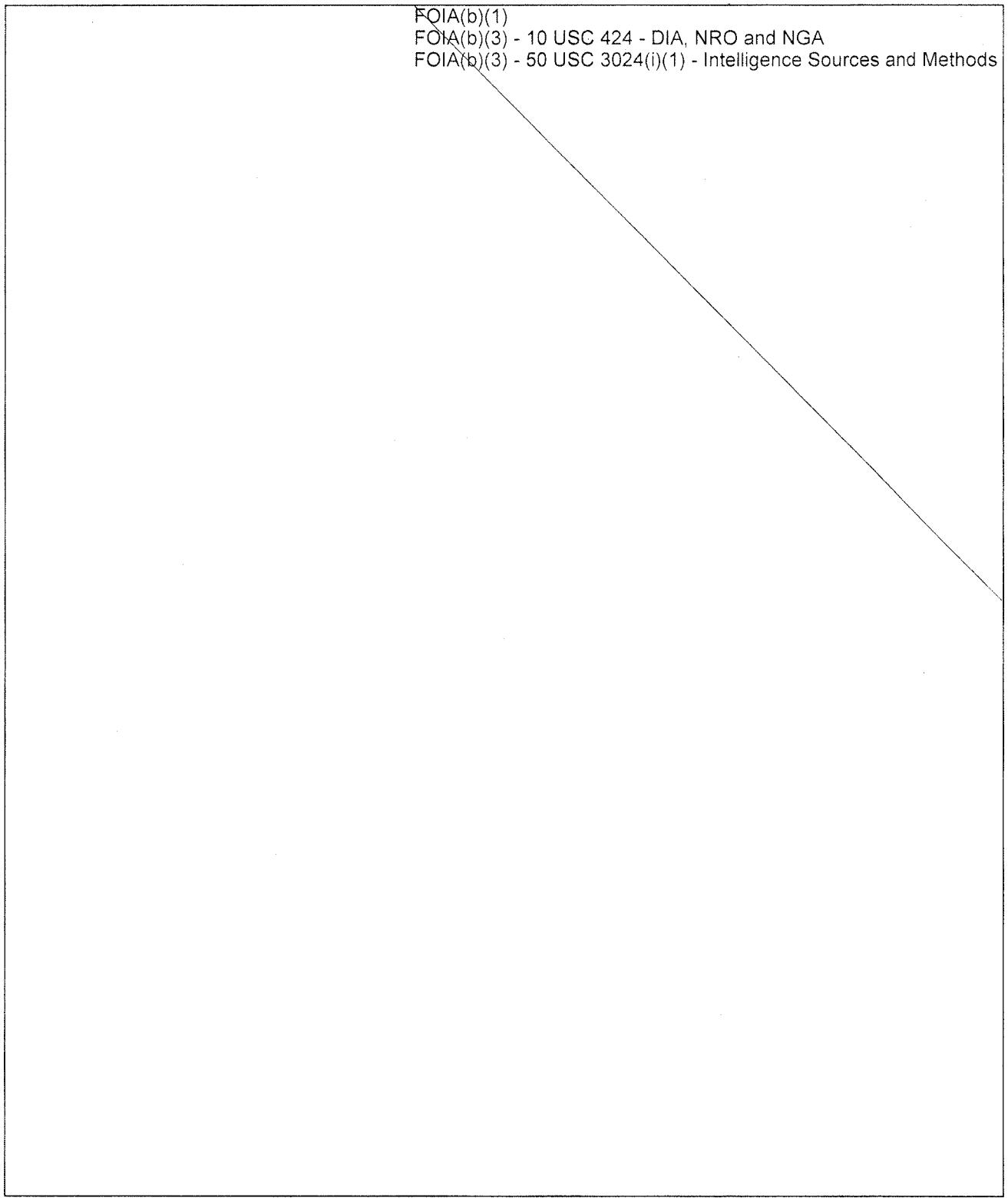


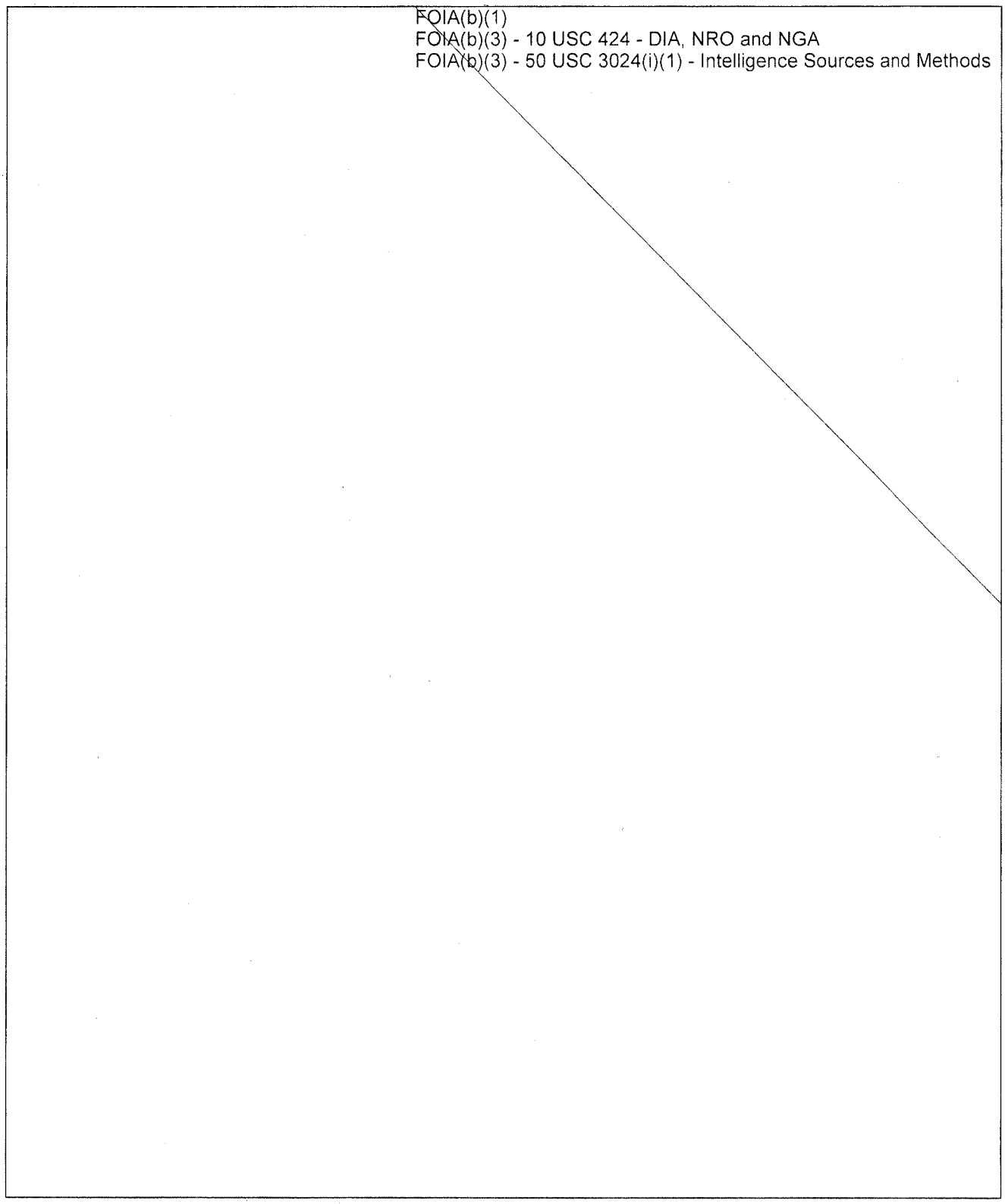




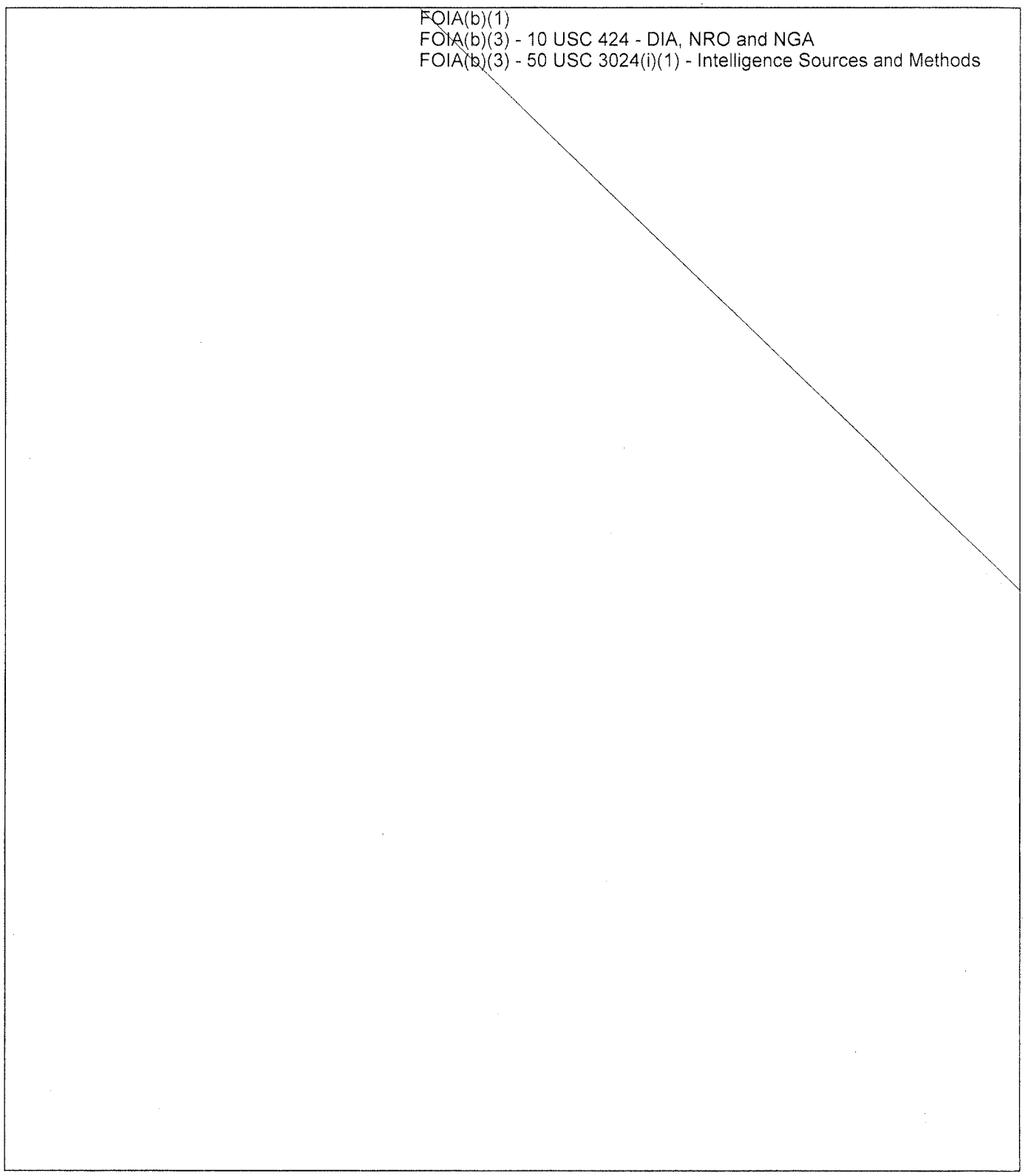


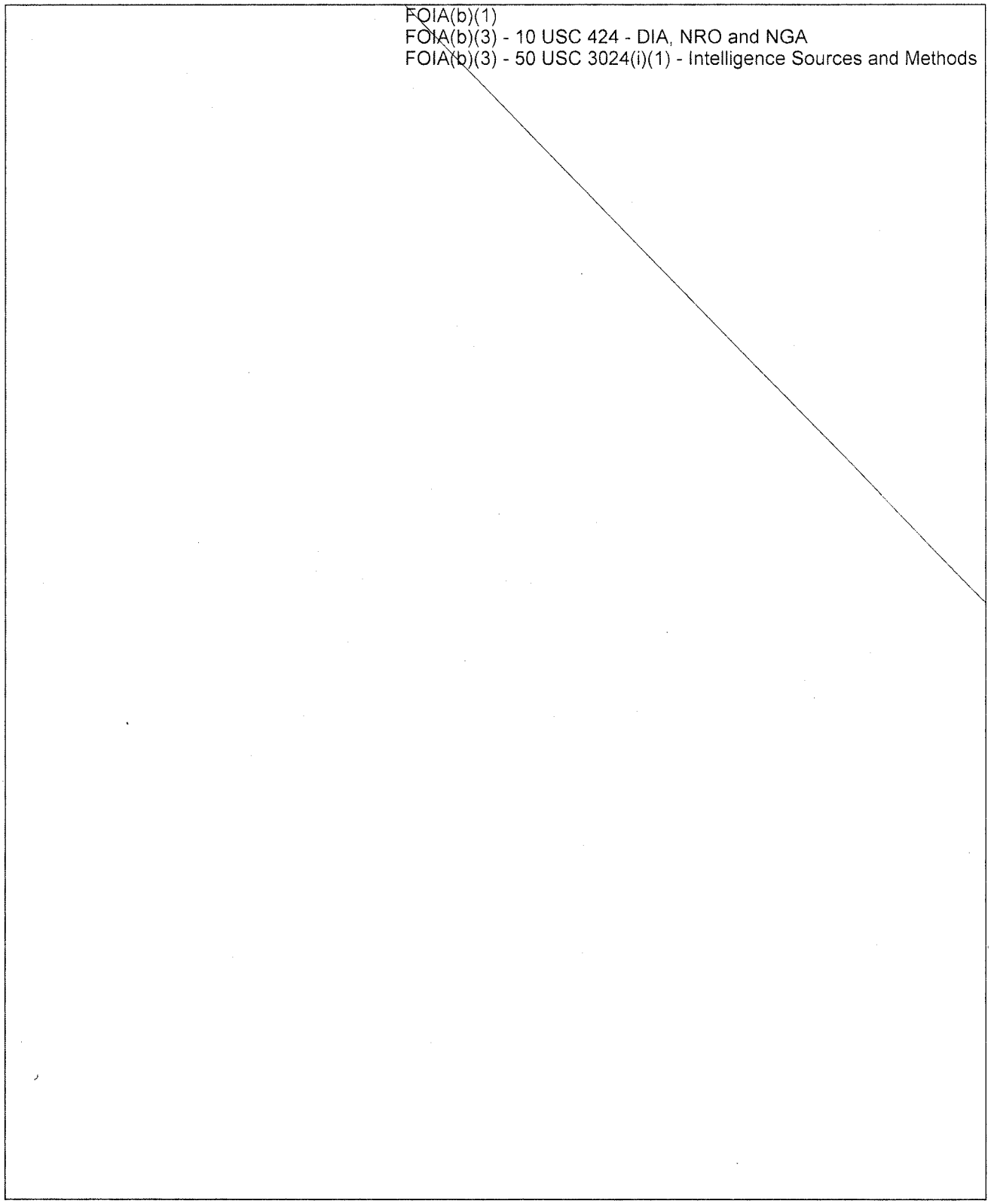


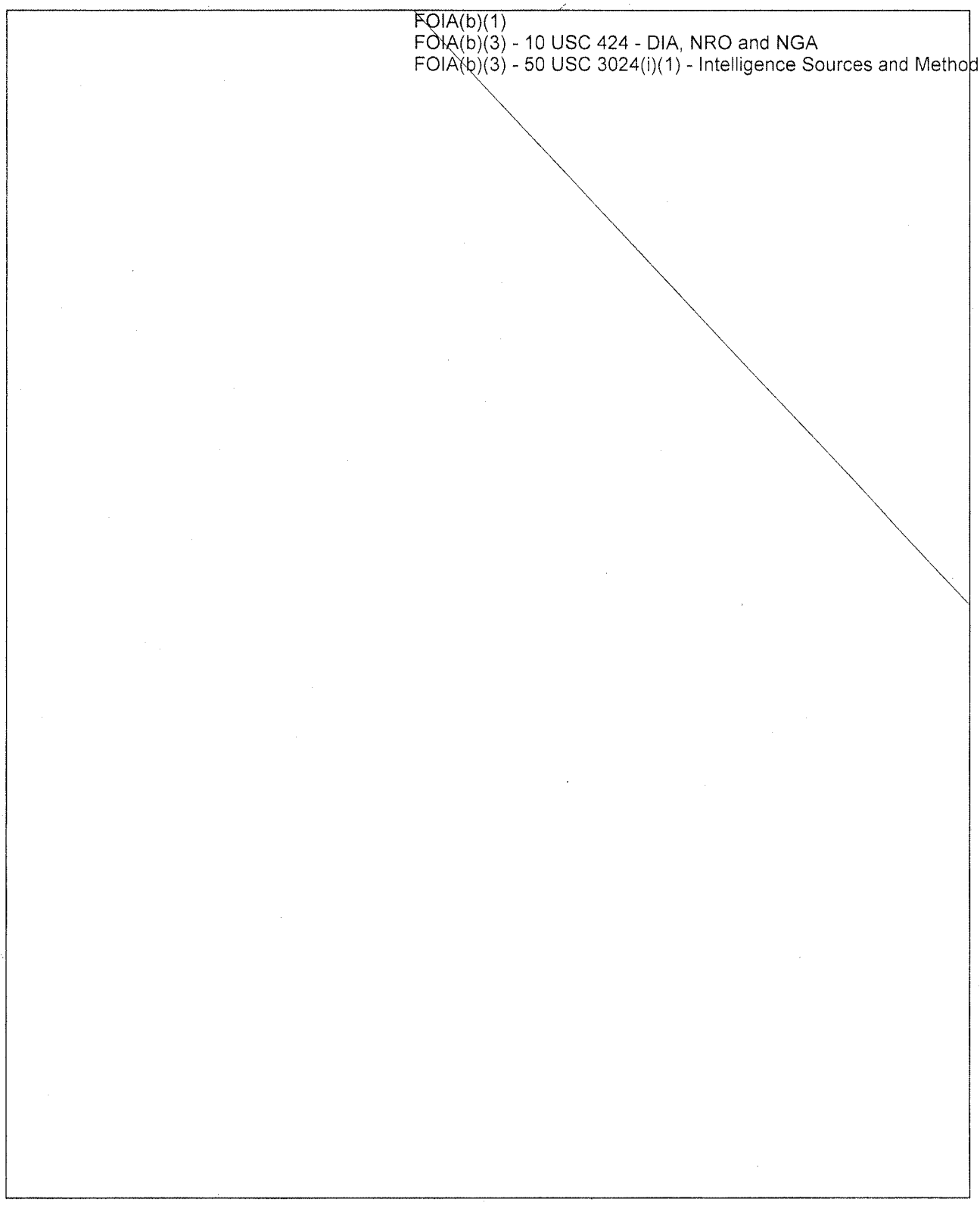

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



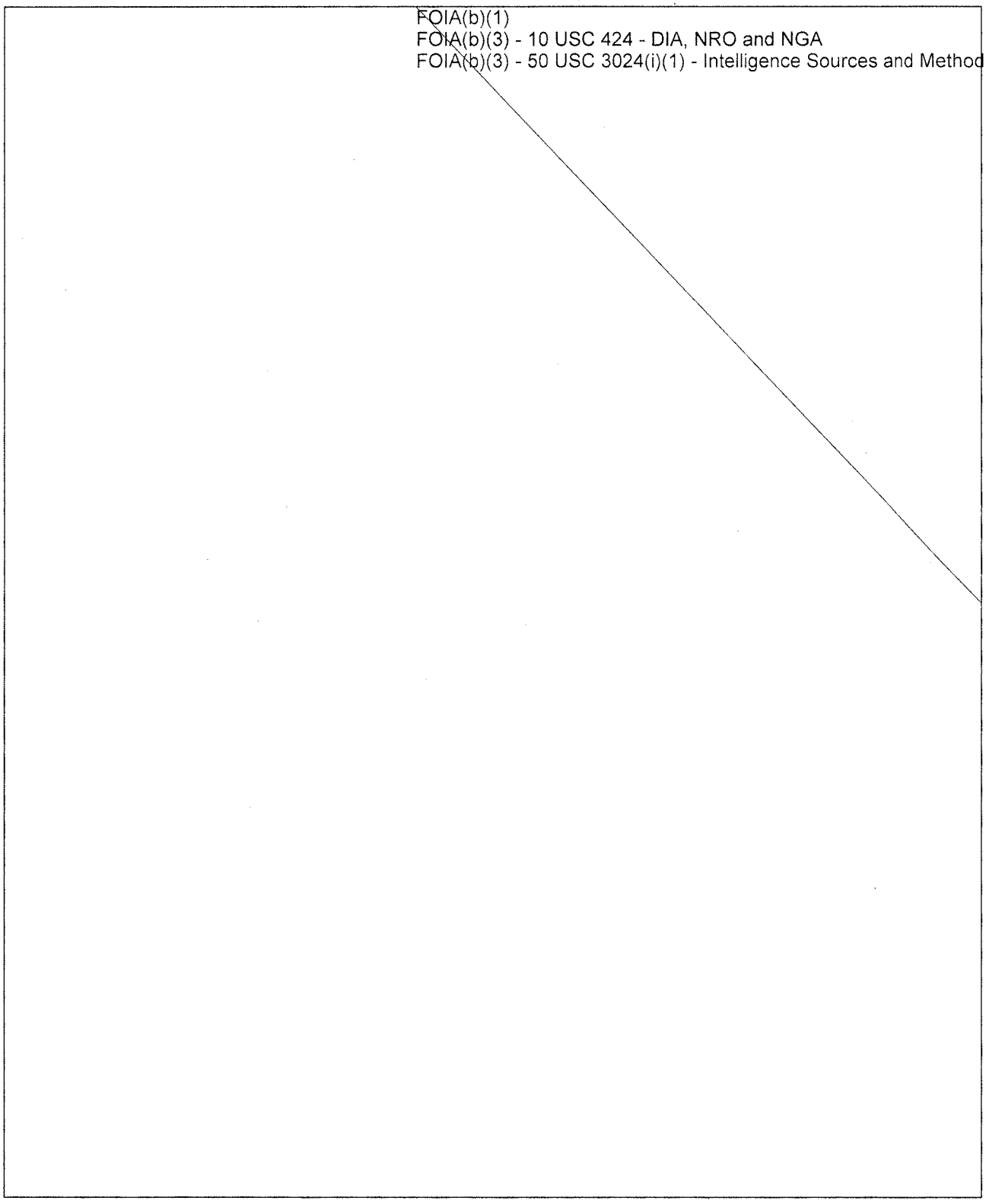
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



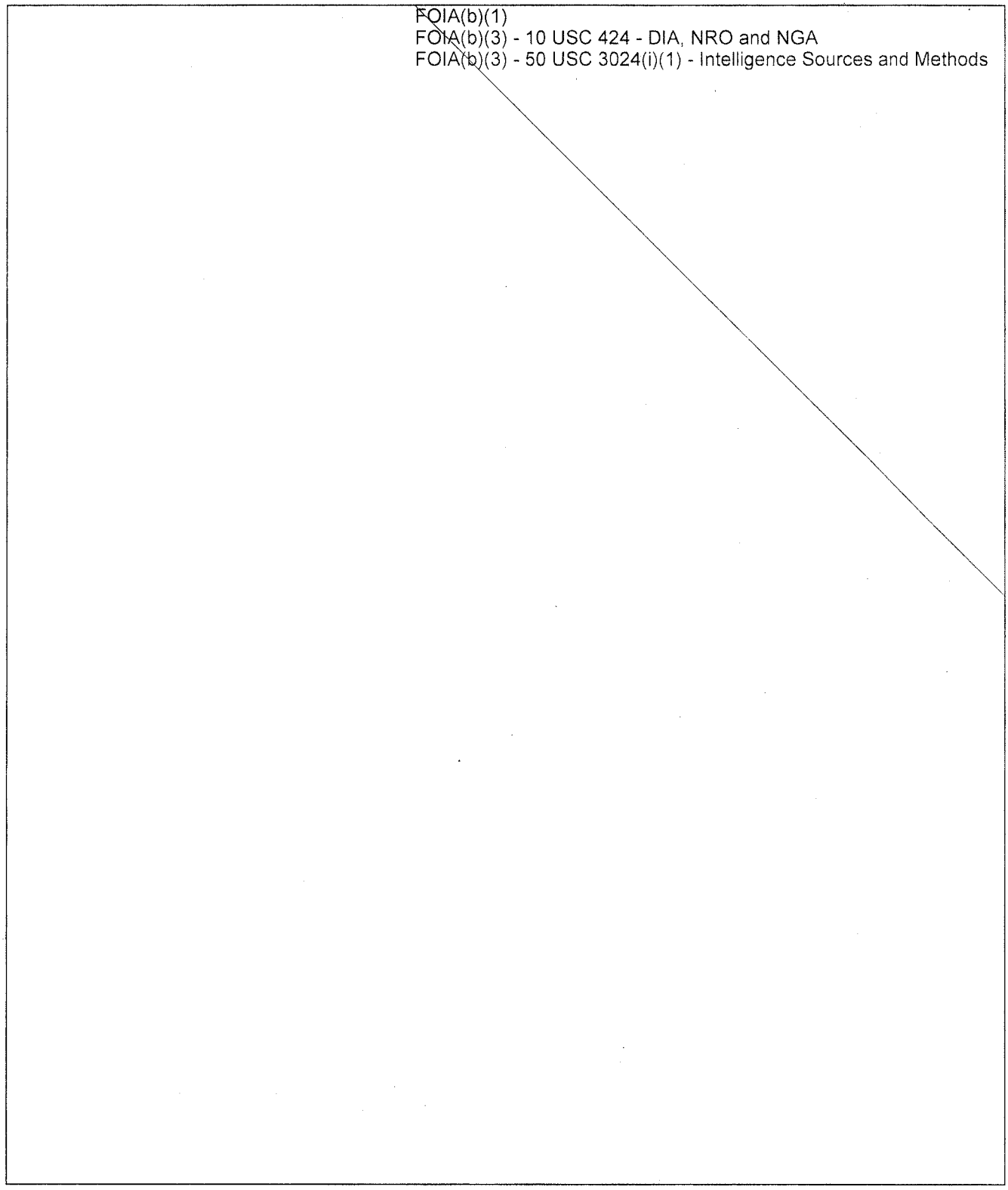


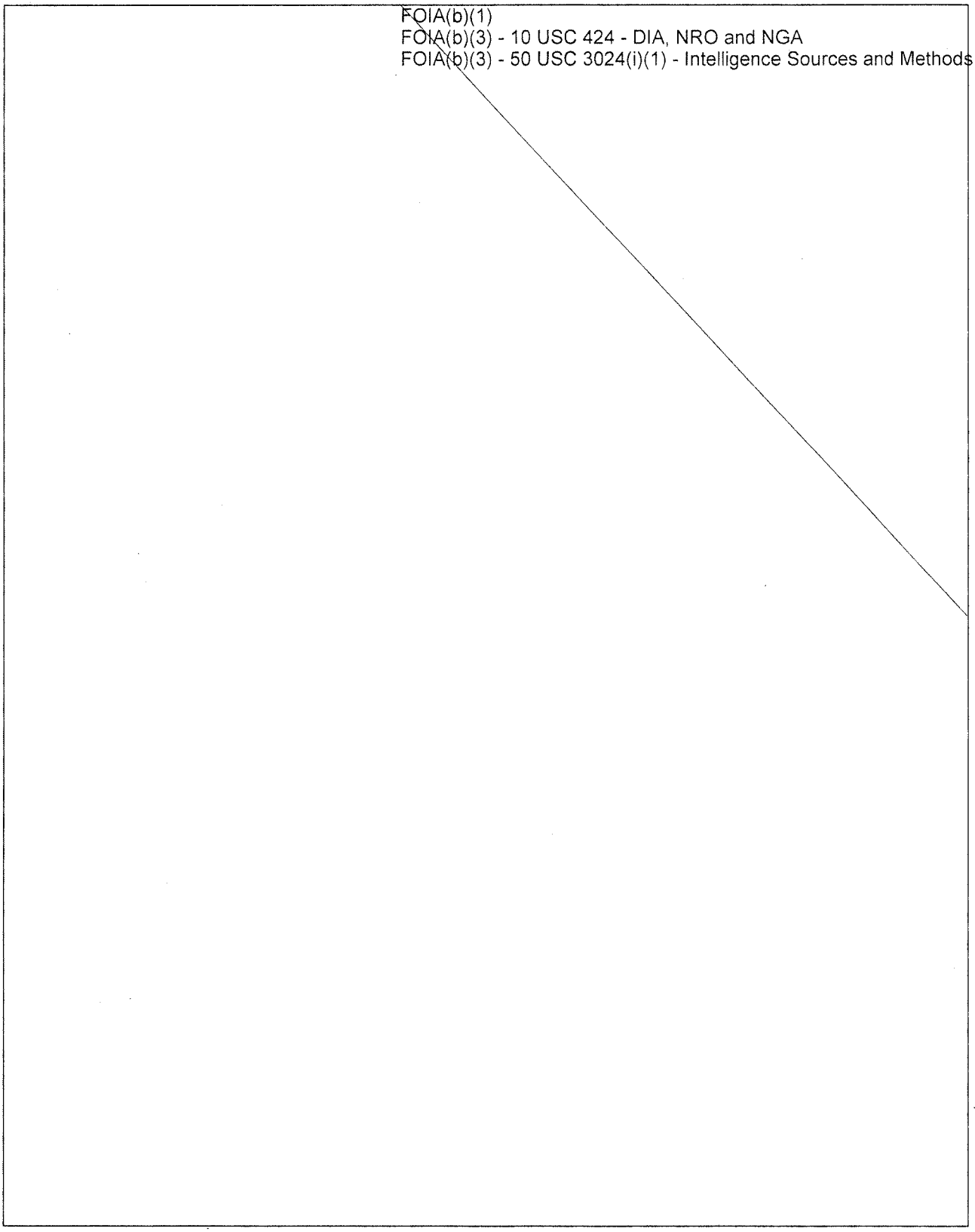


FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

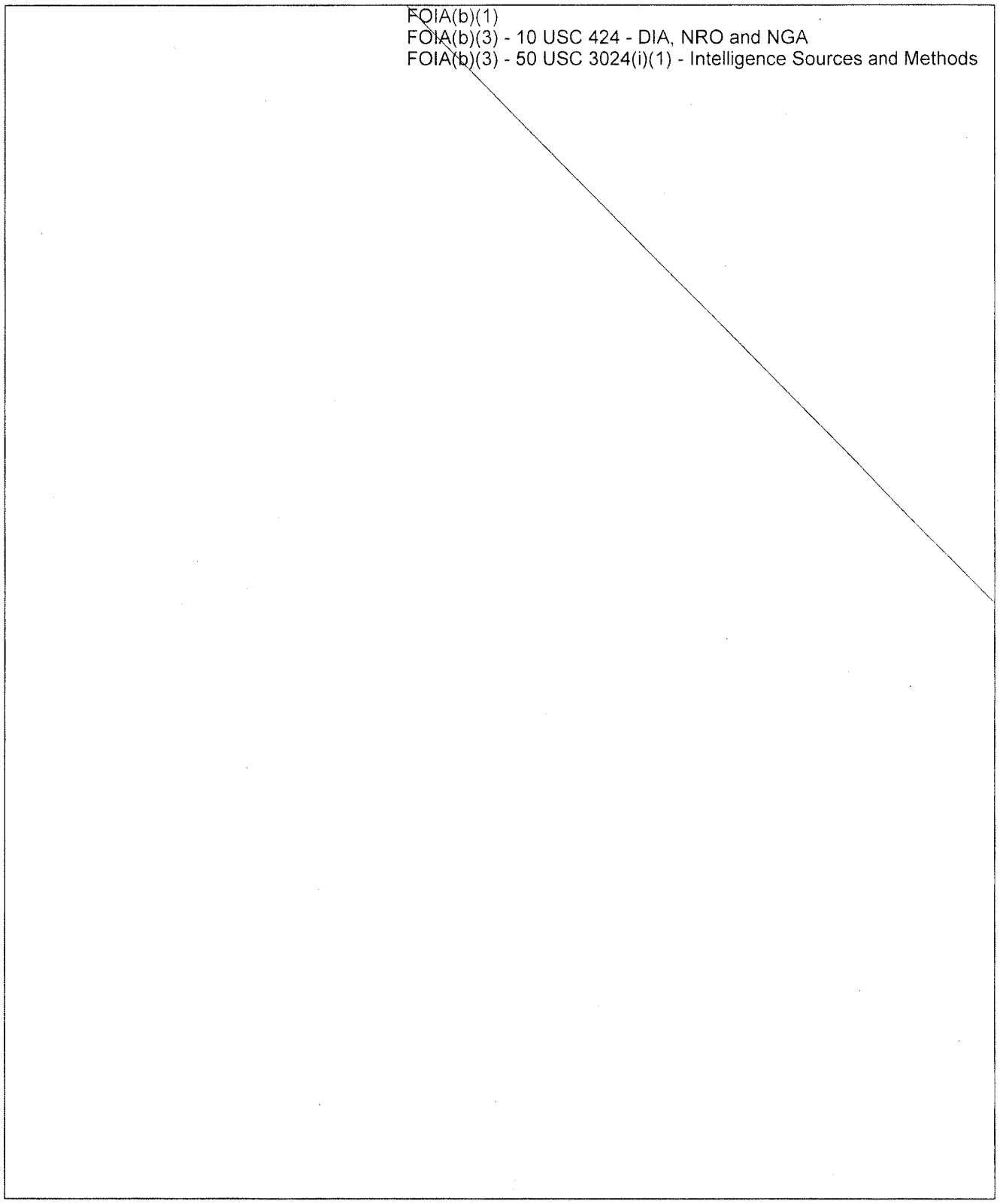


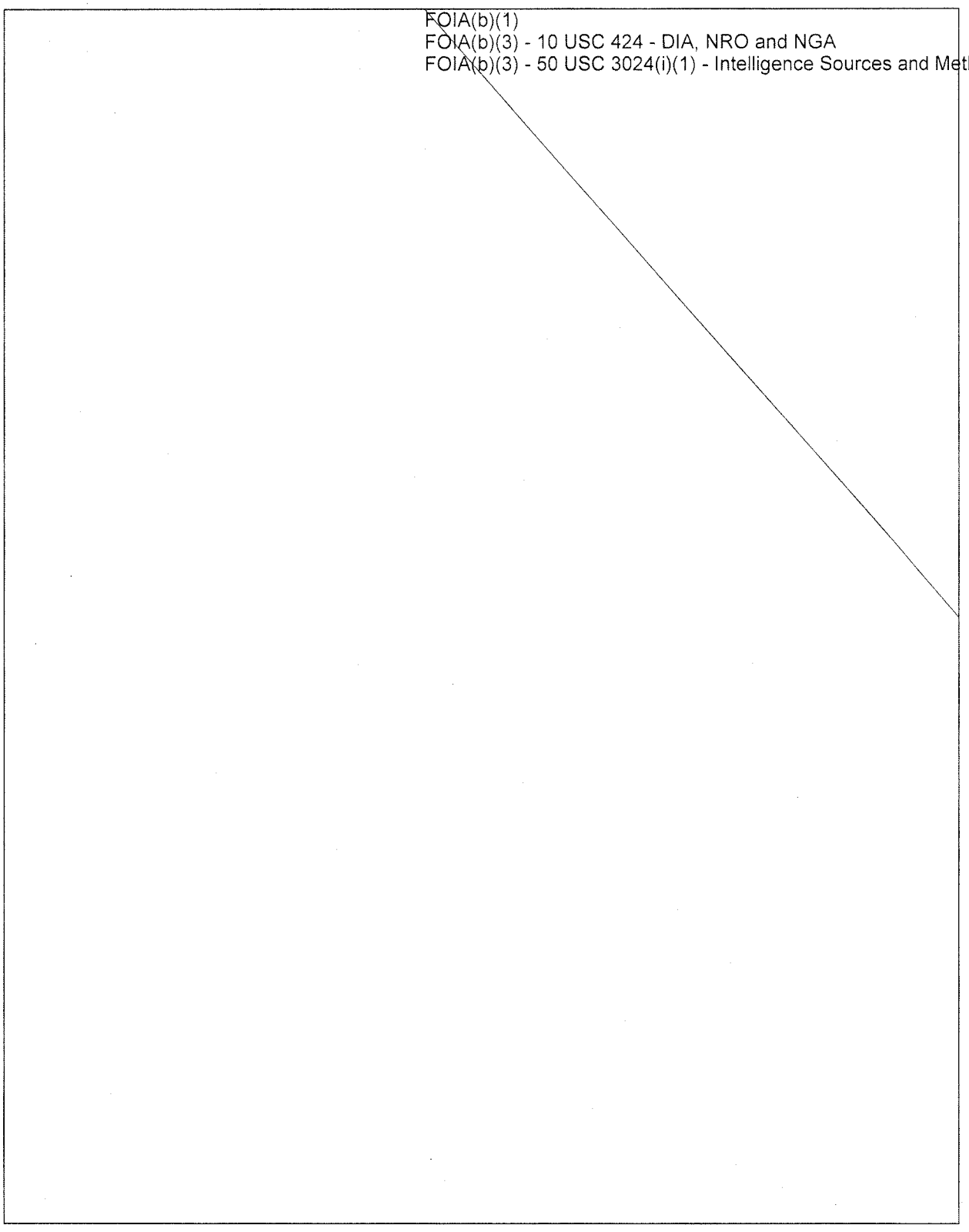
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



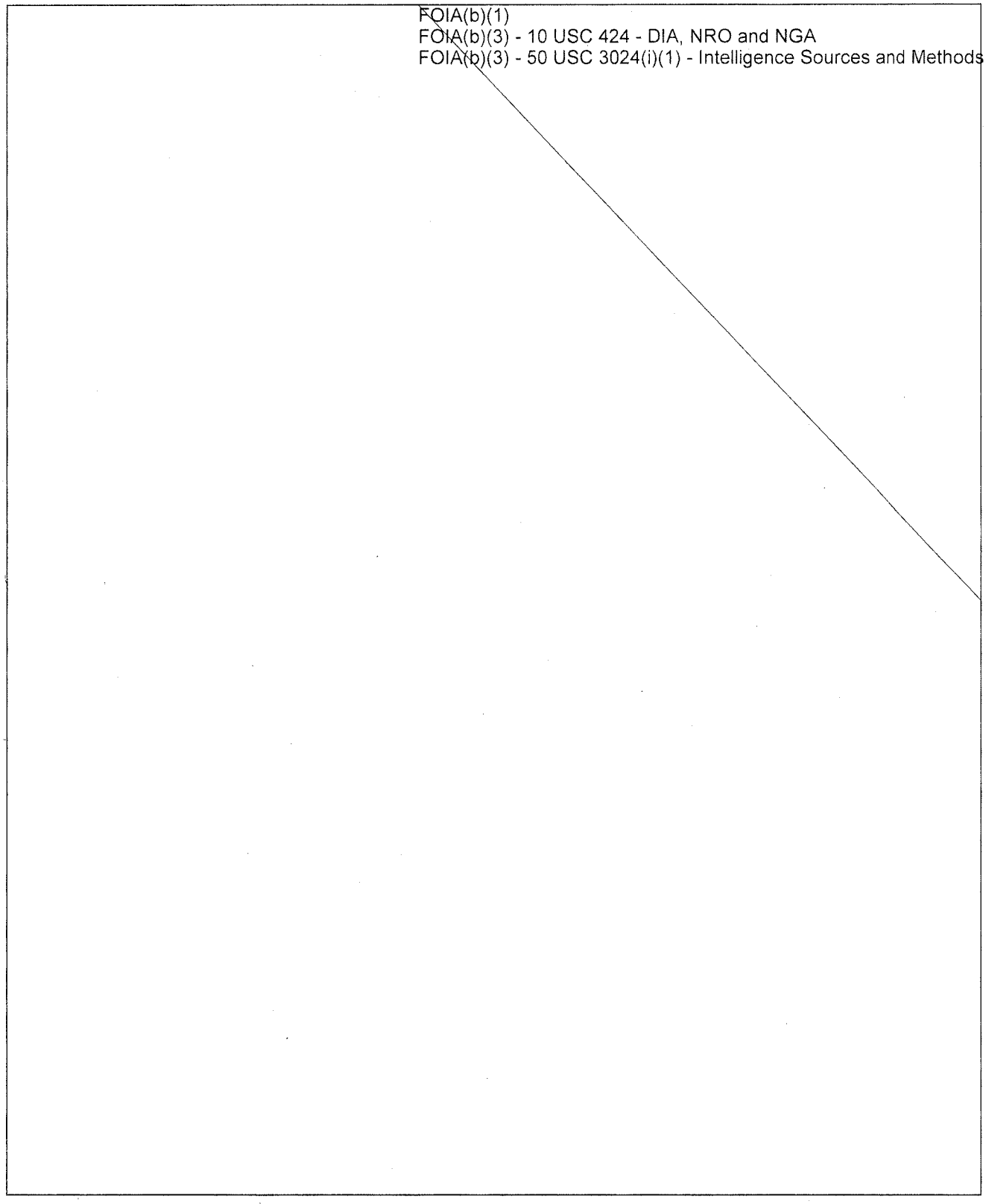


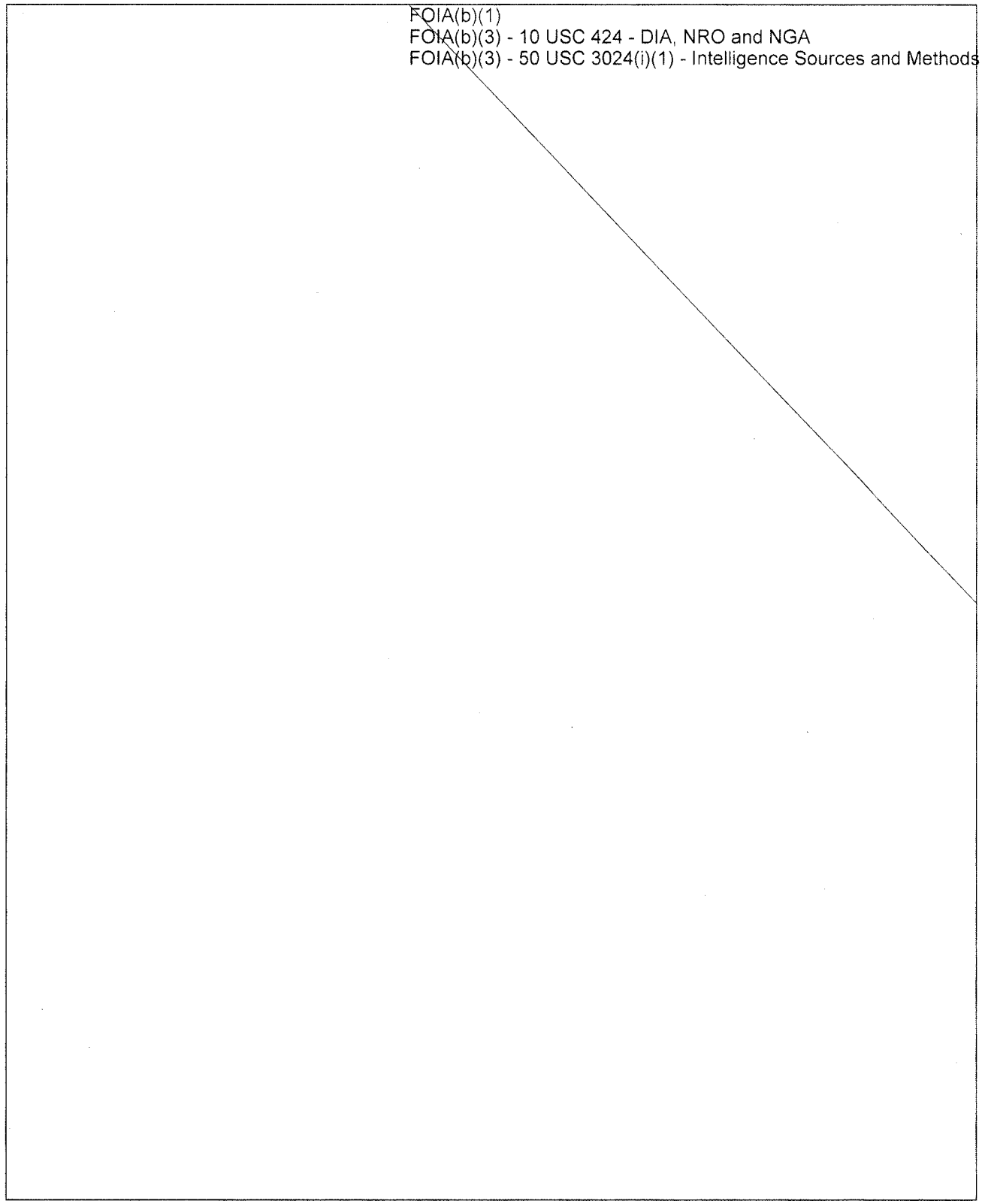
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods



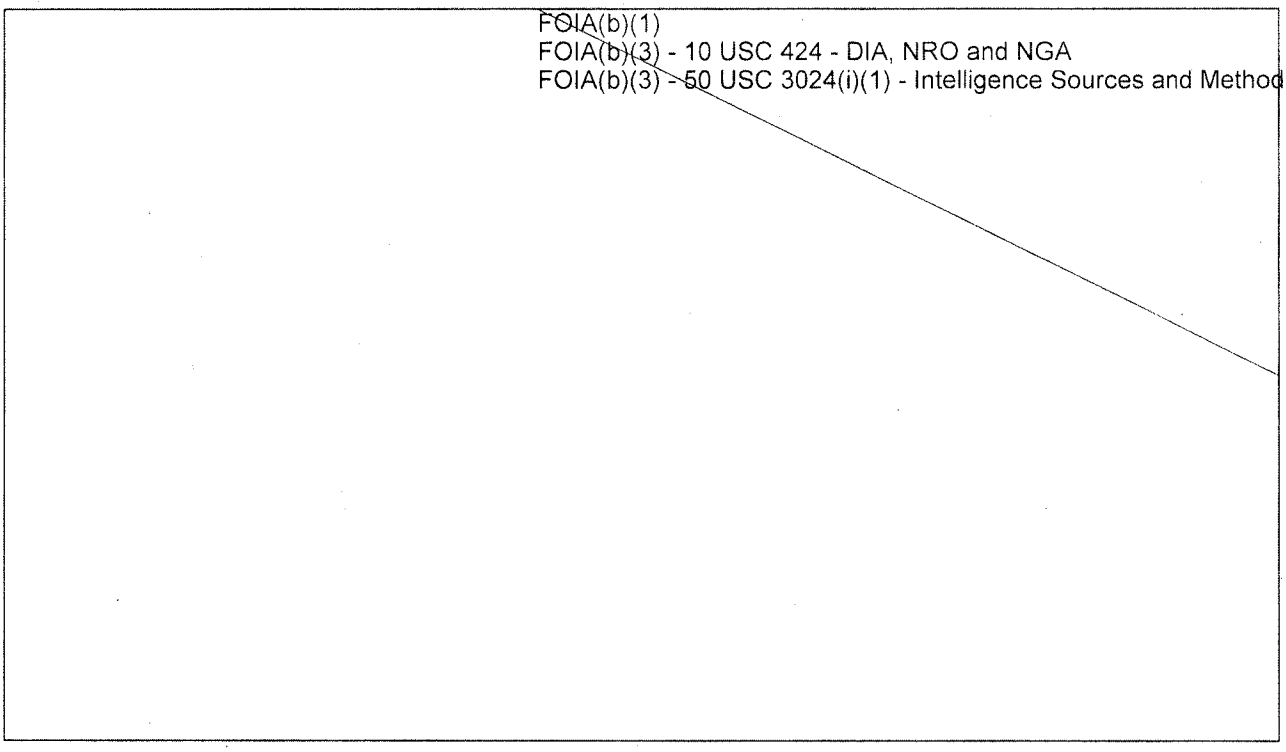


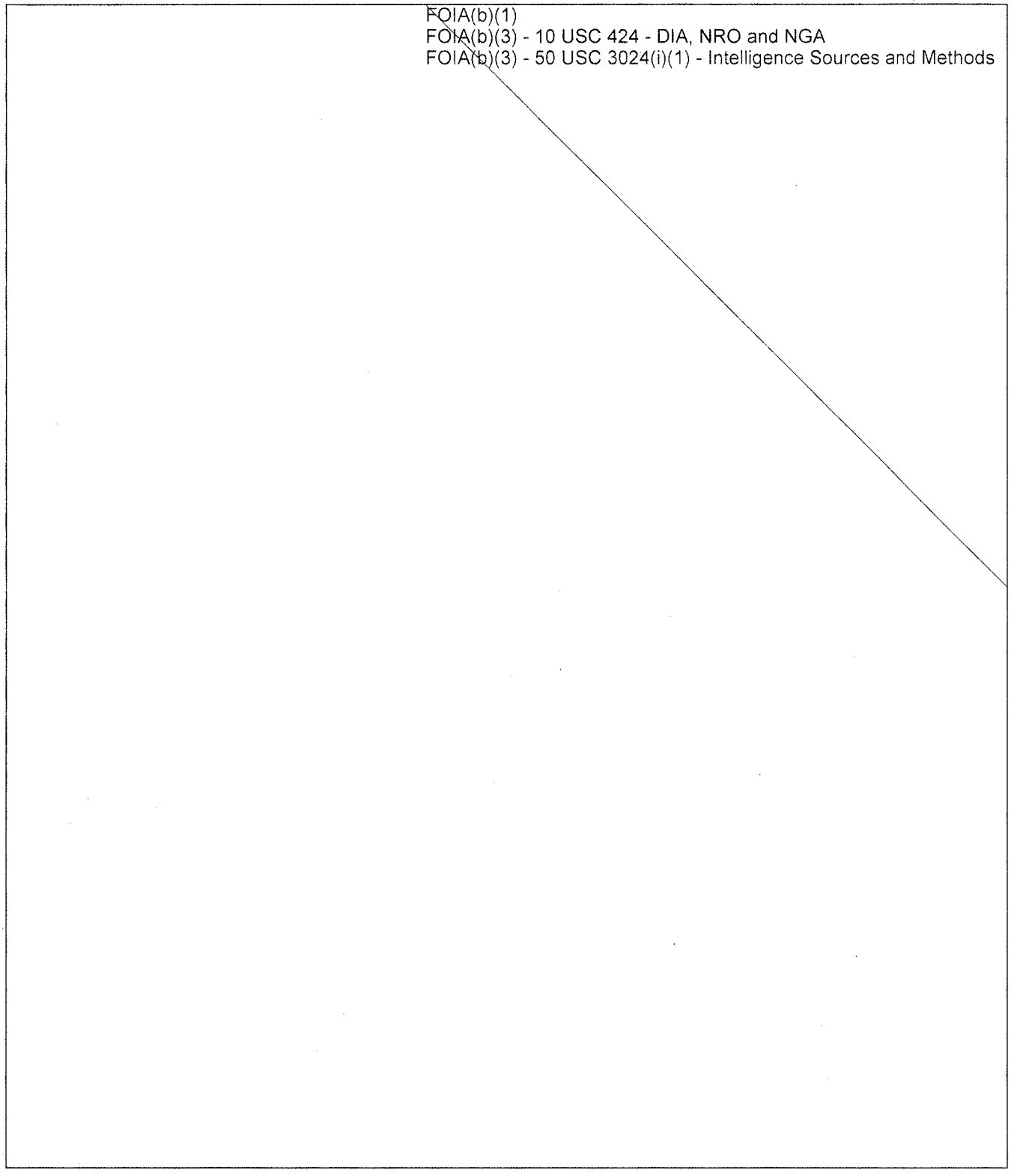
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

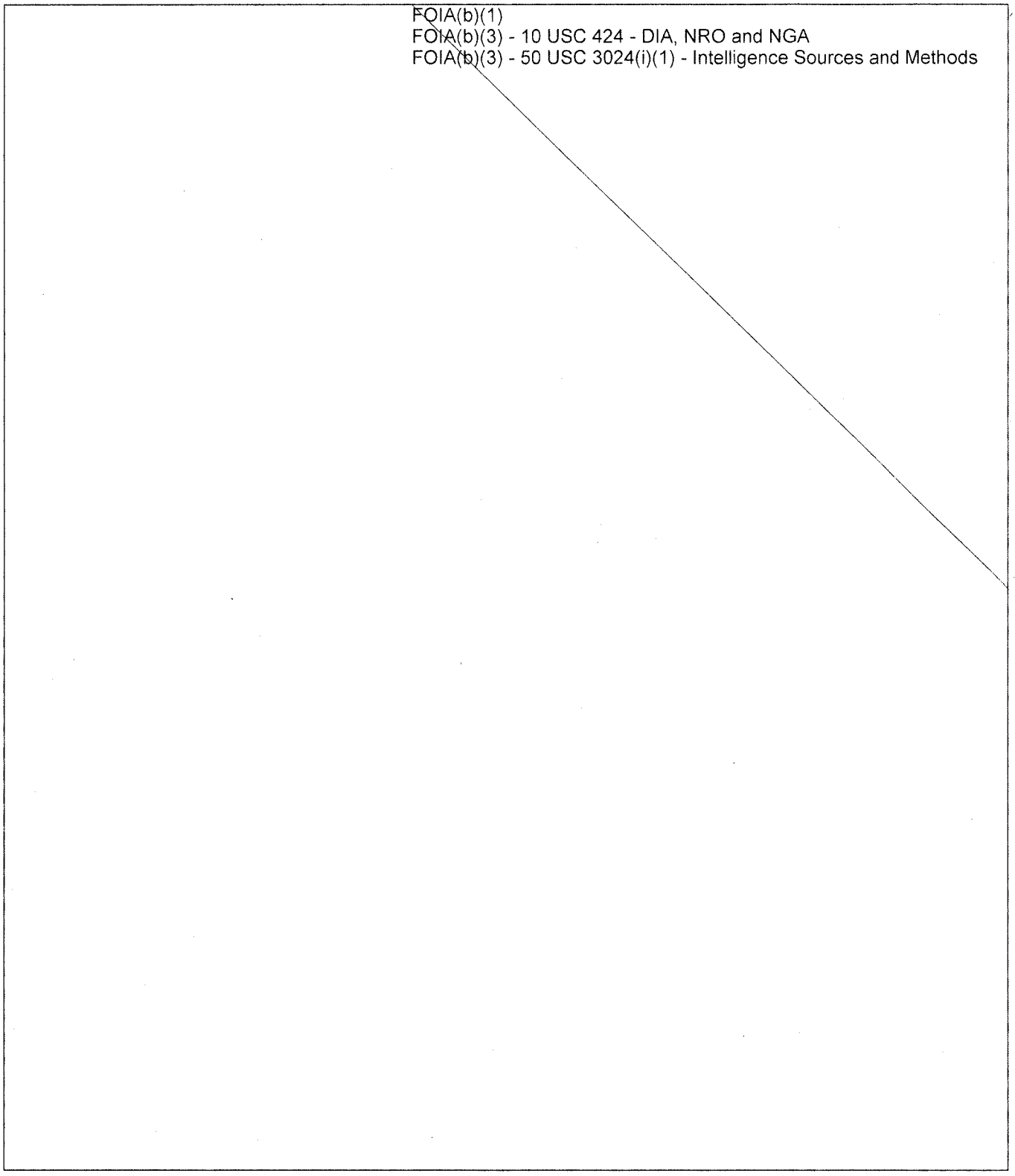


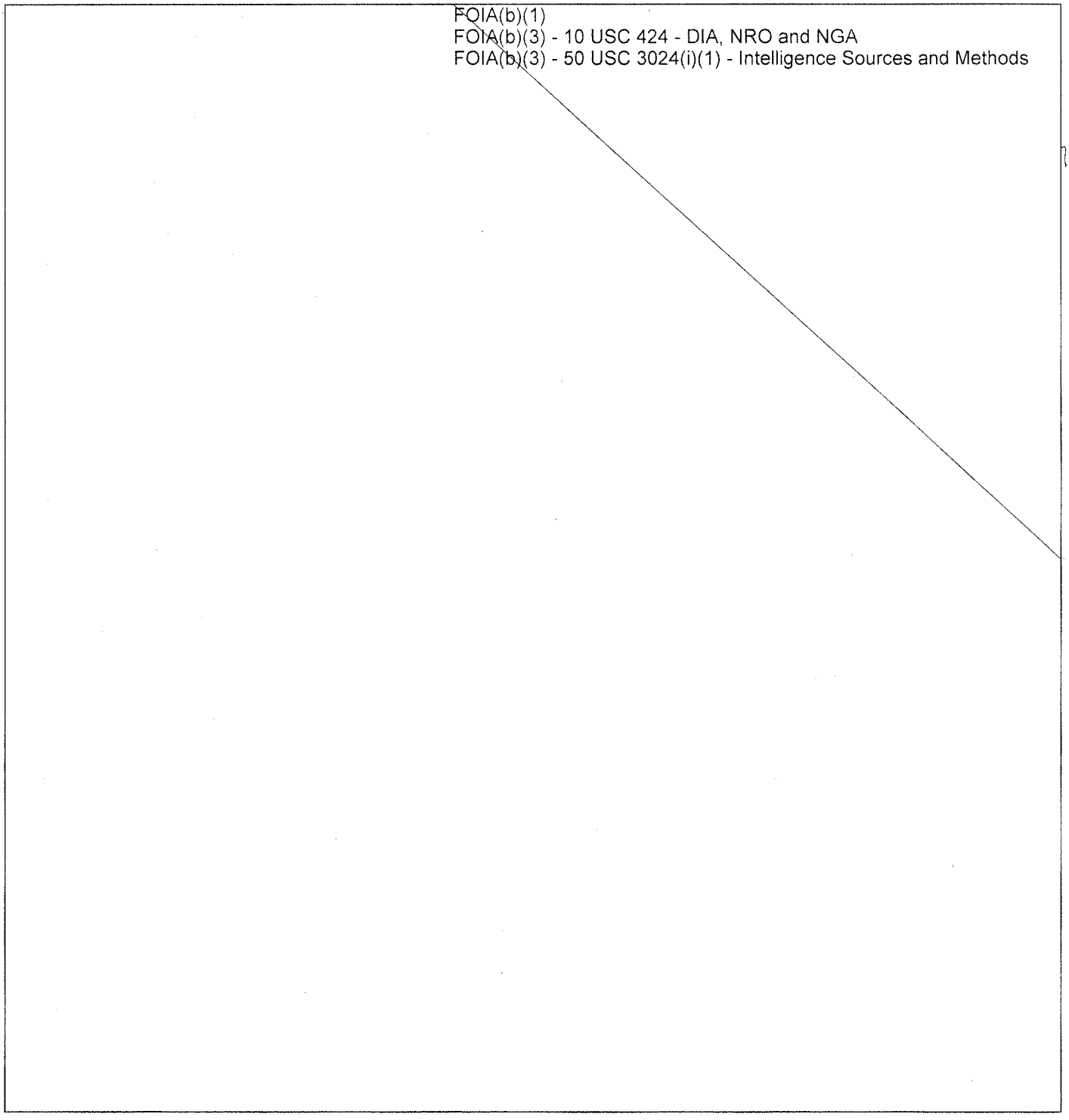


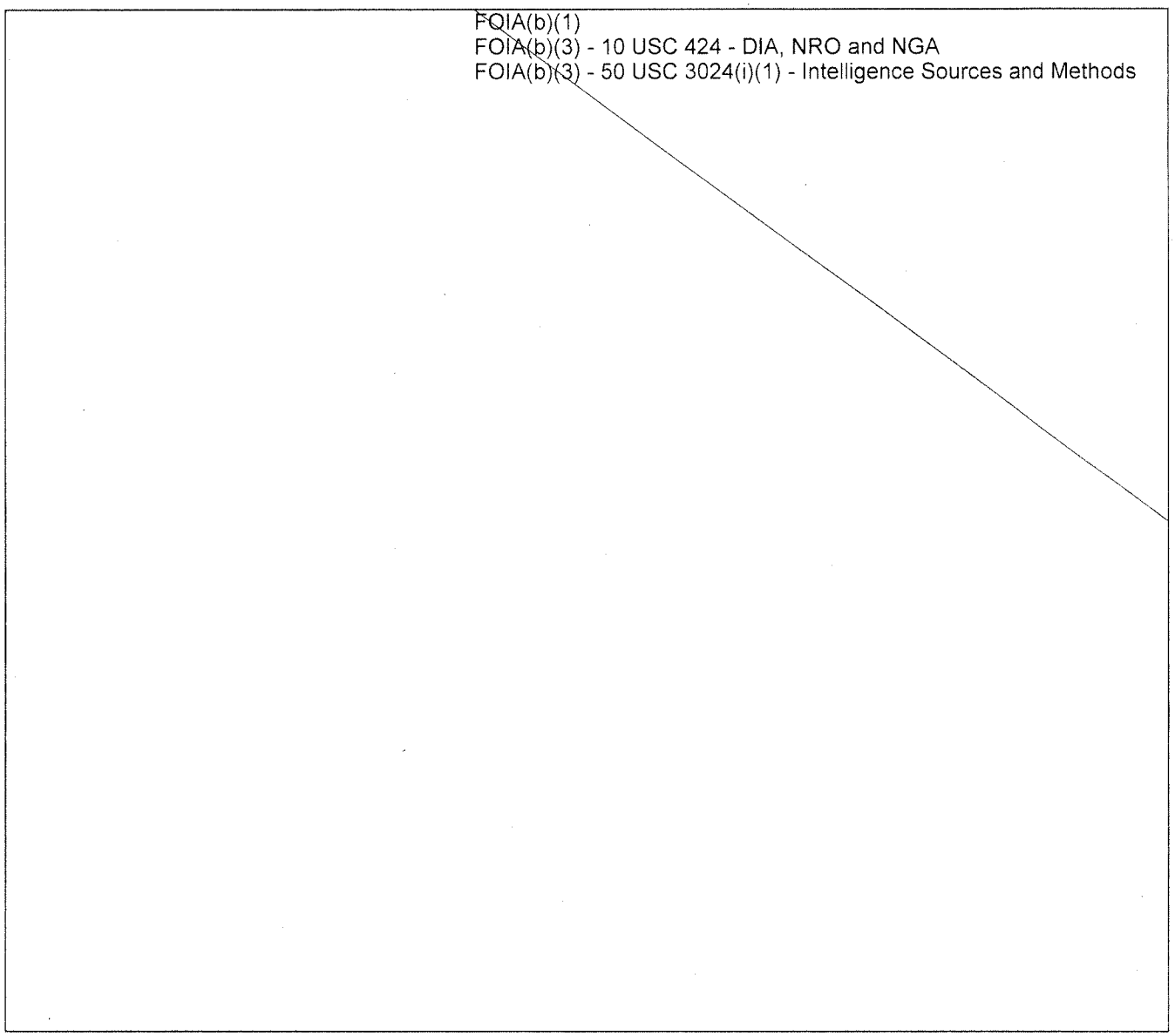
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

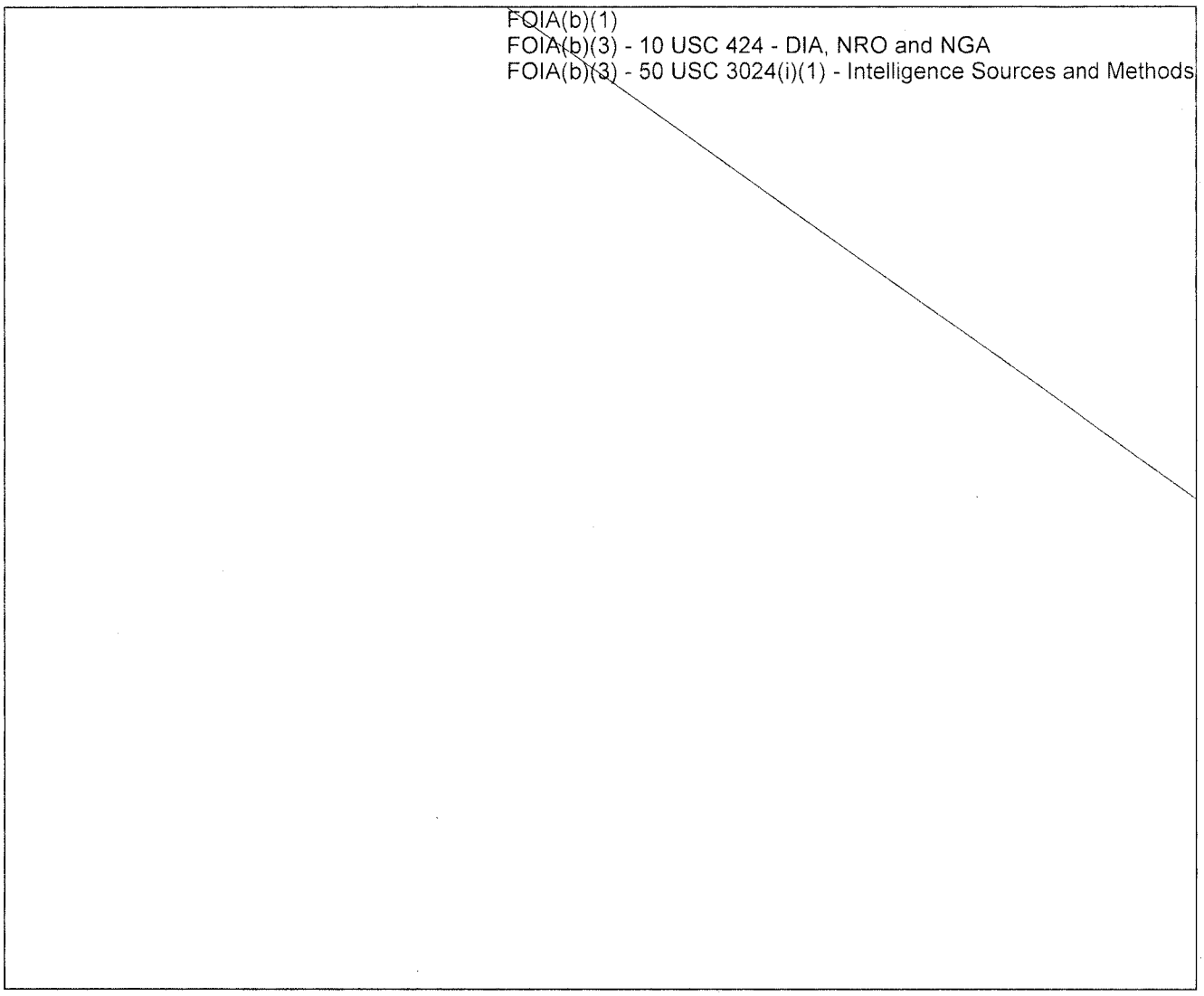


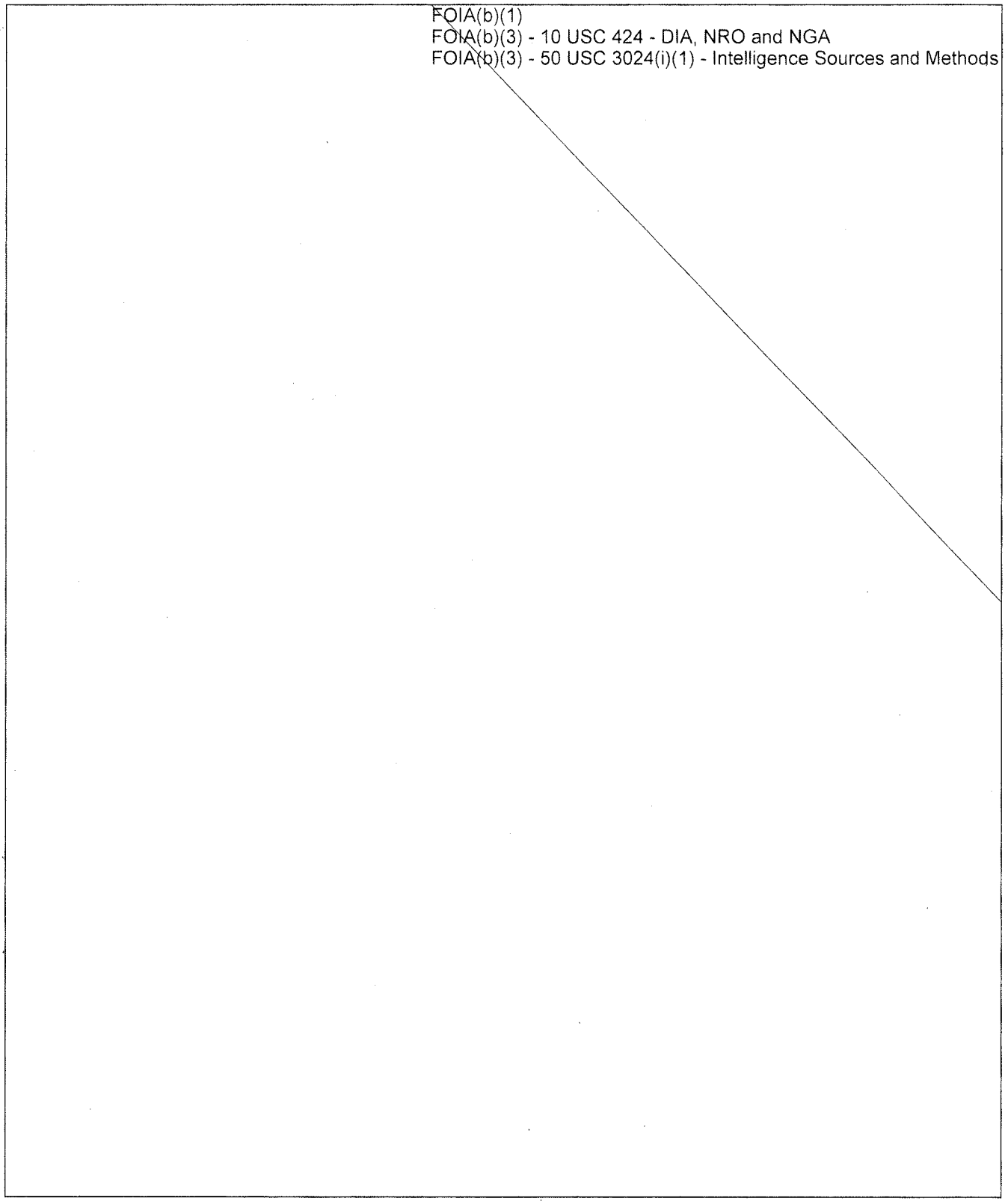


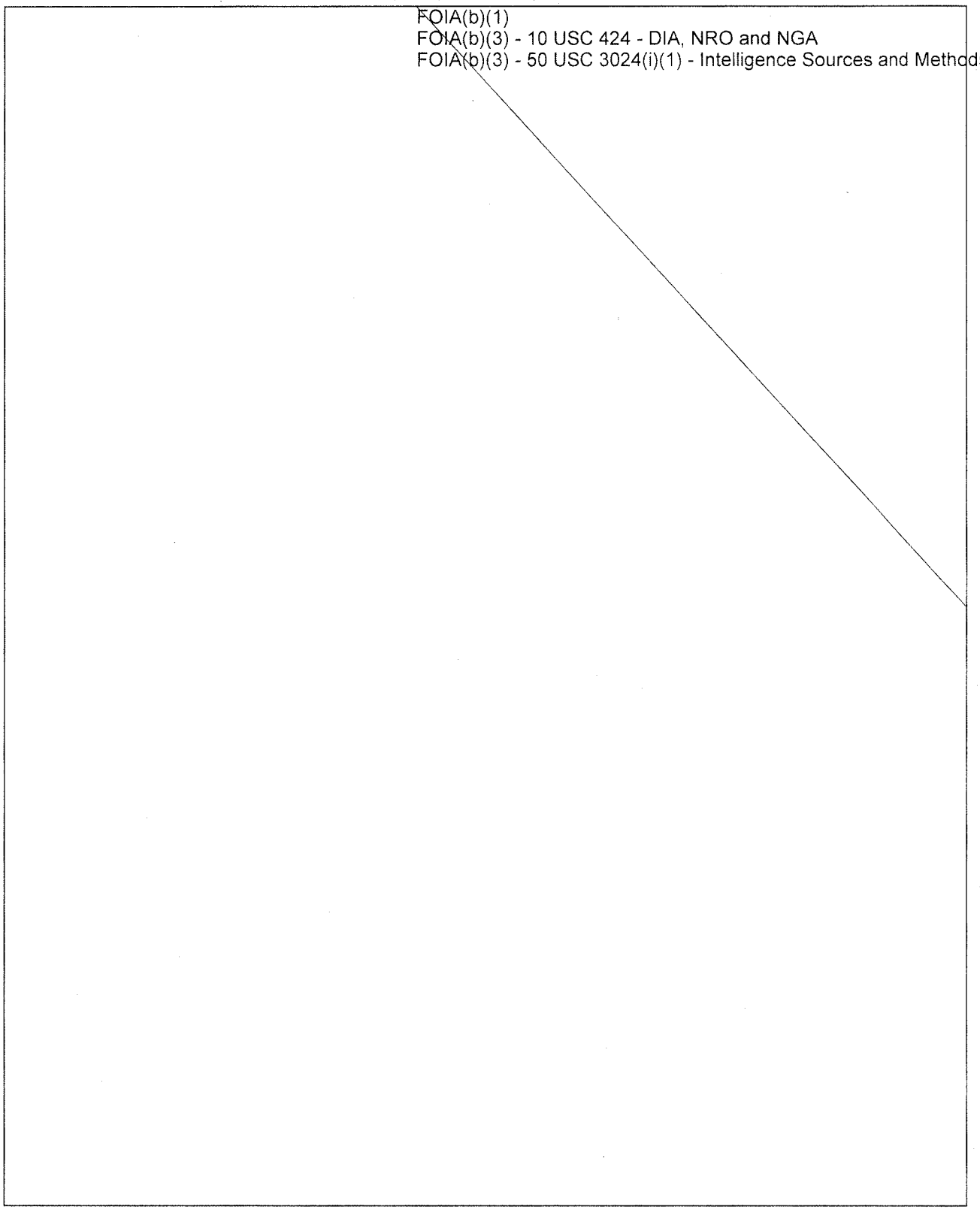


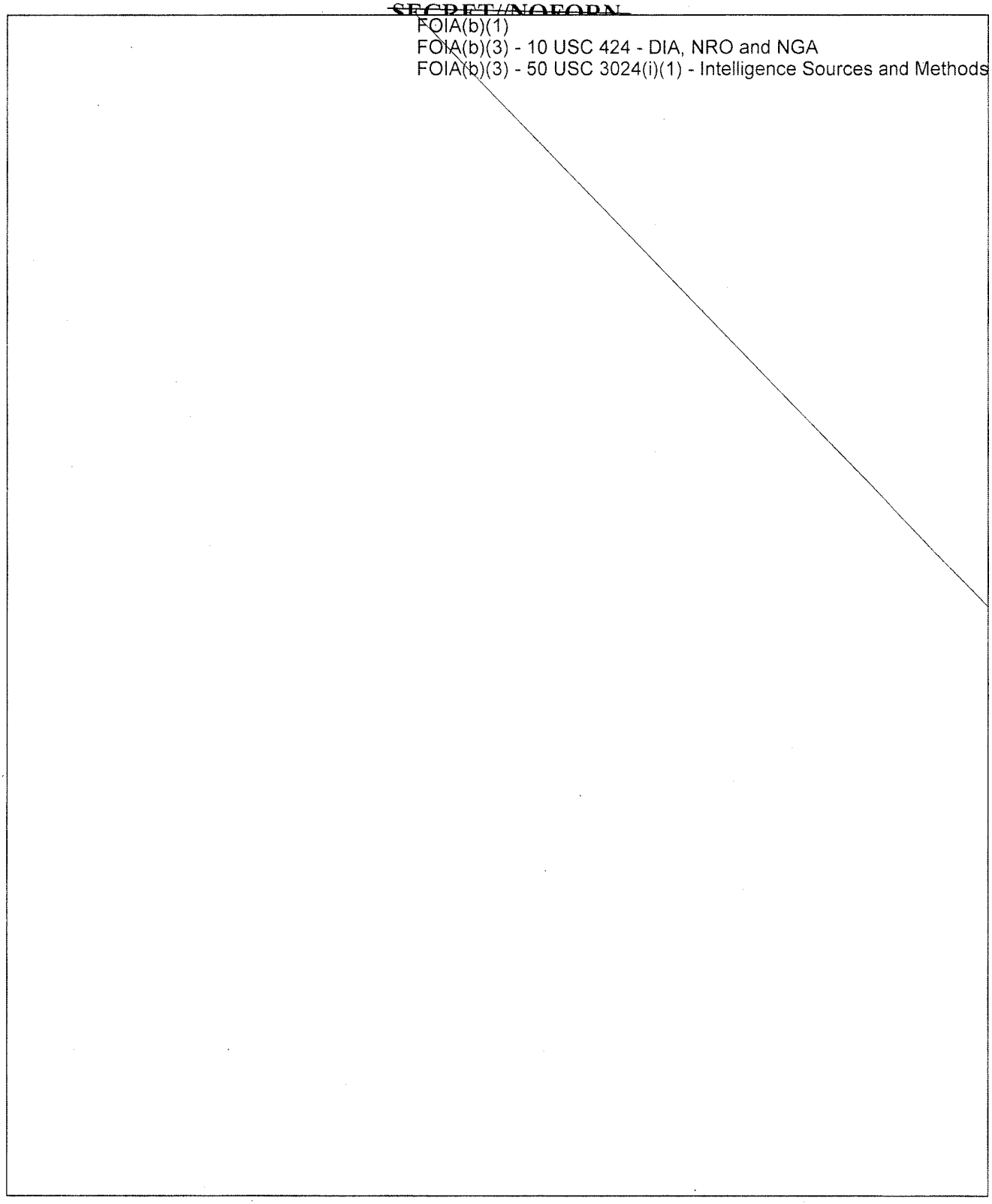


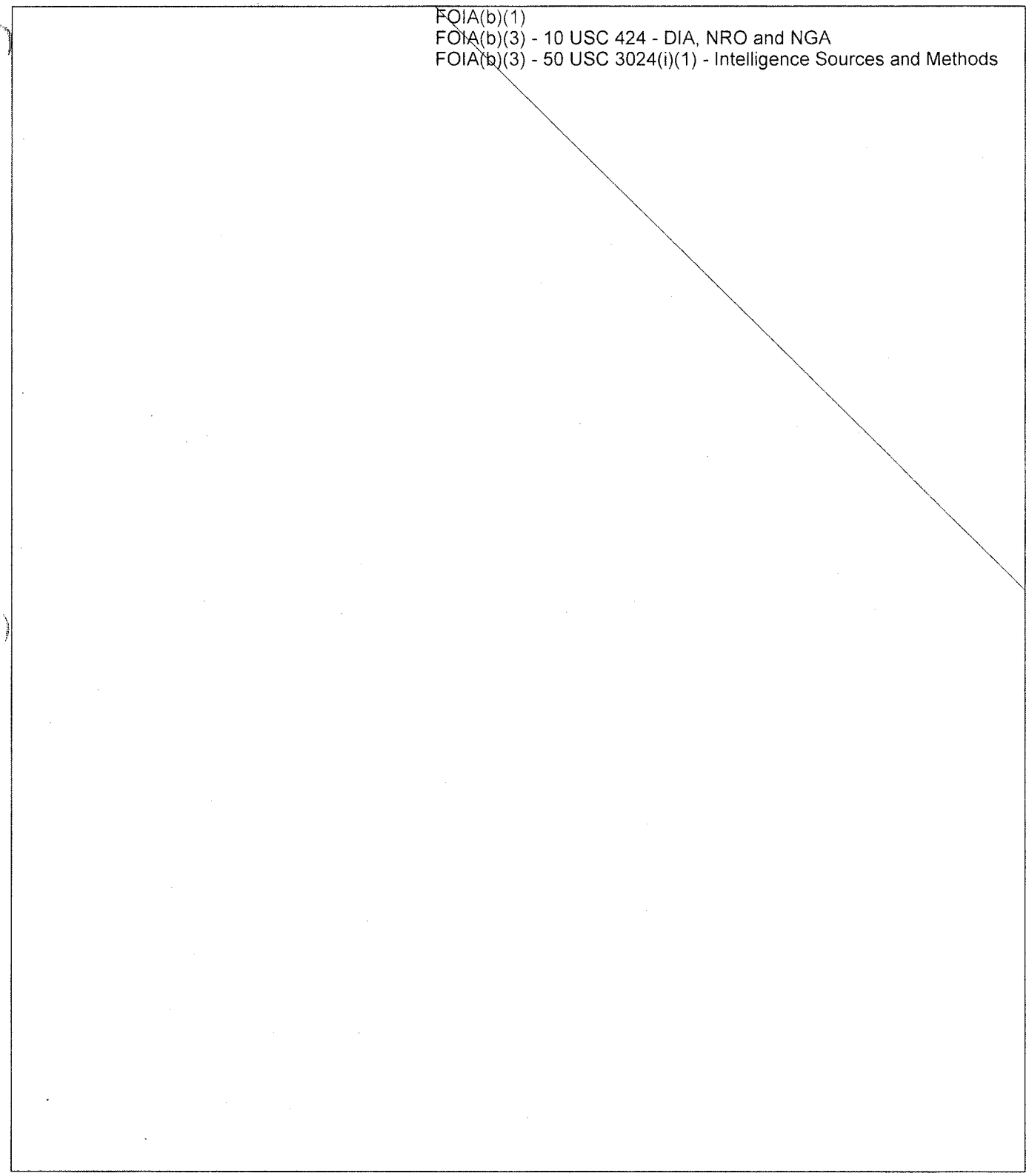


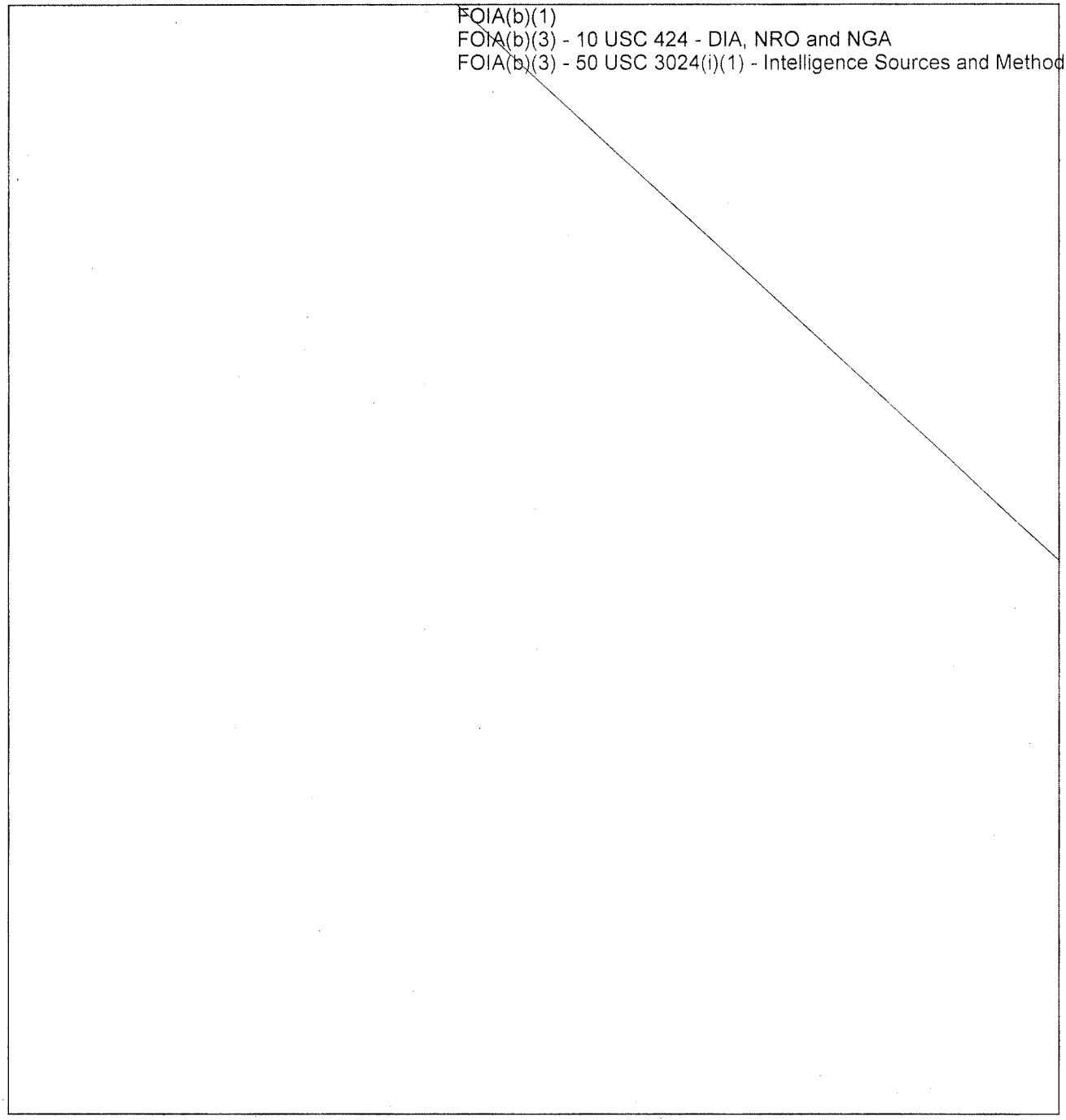




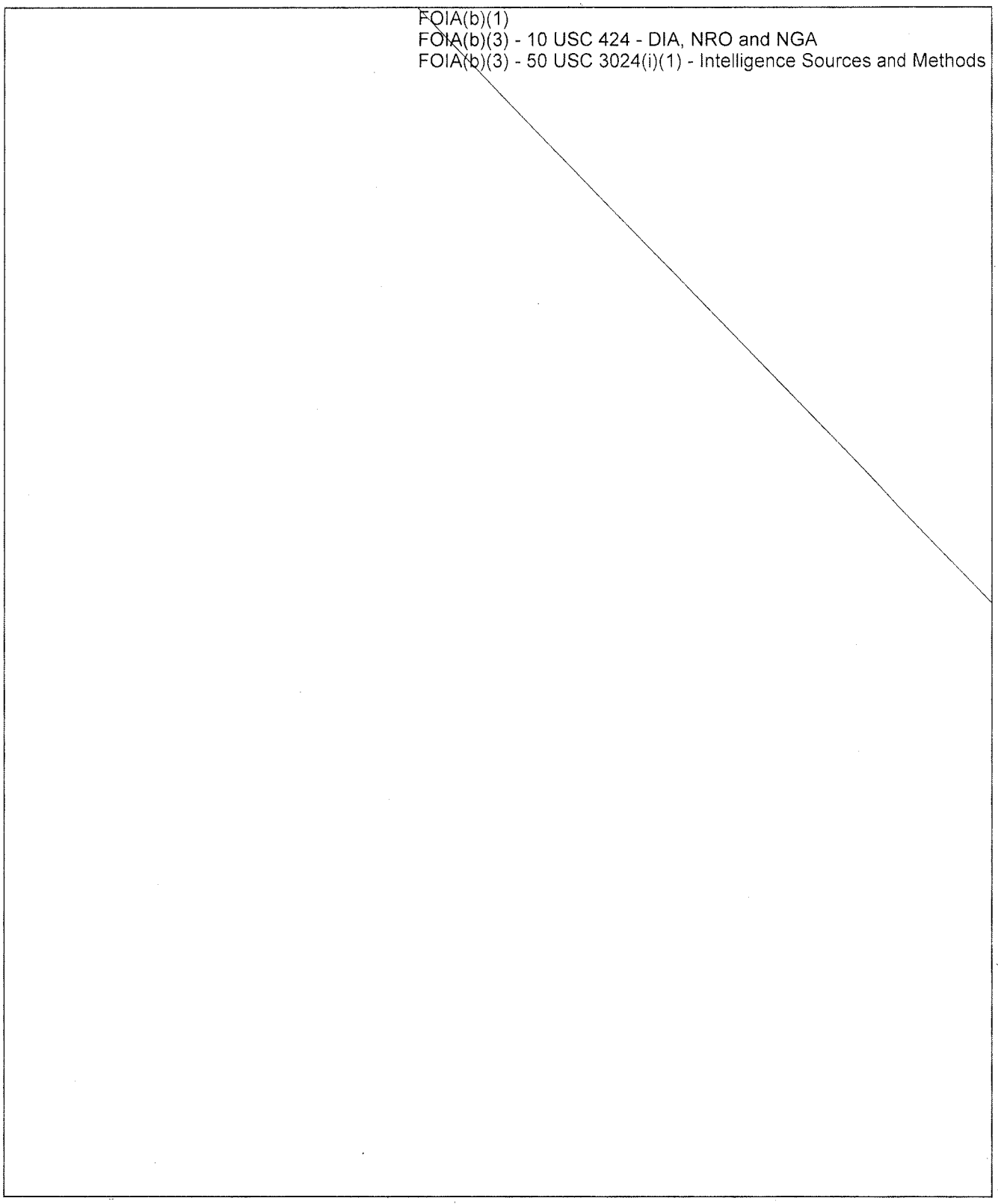


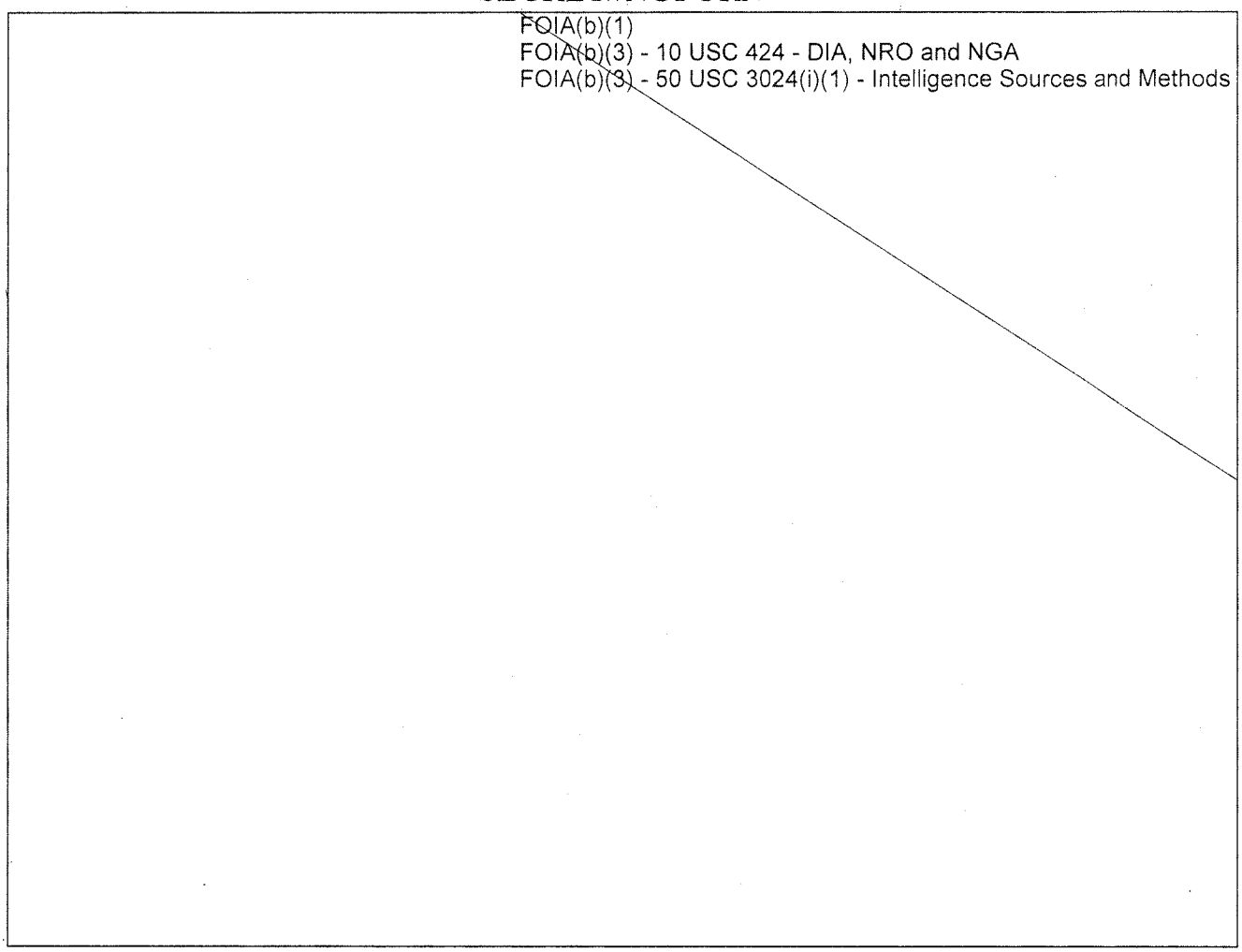


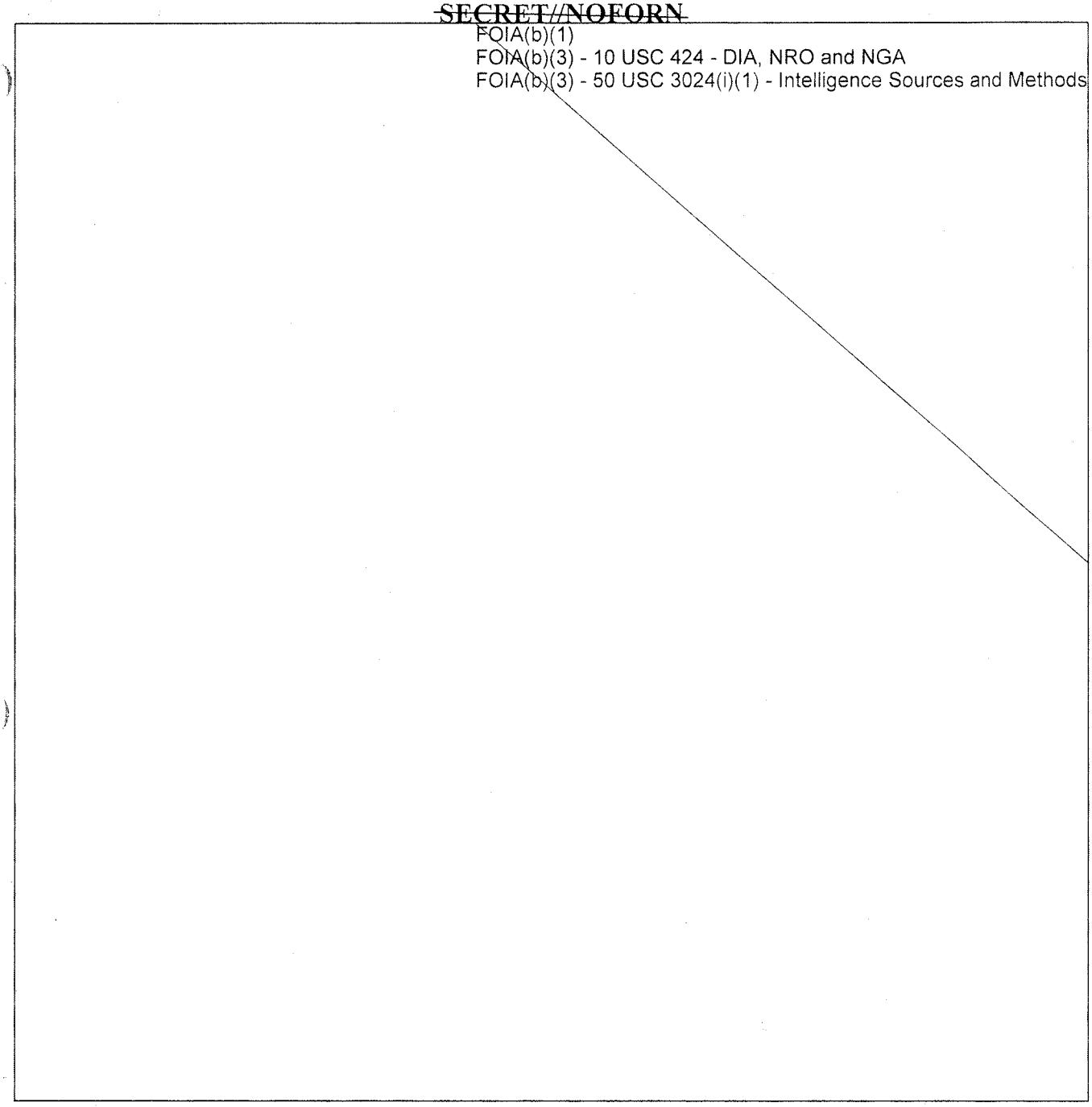


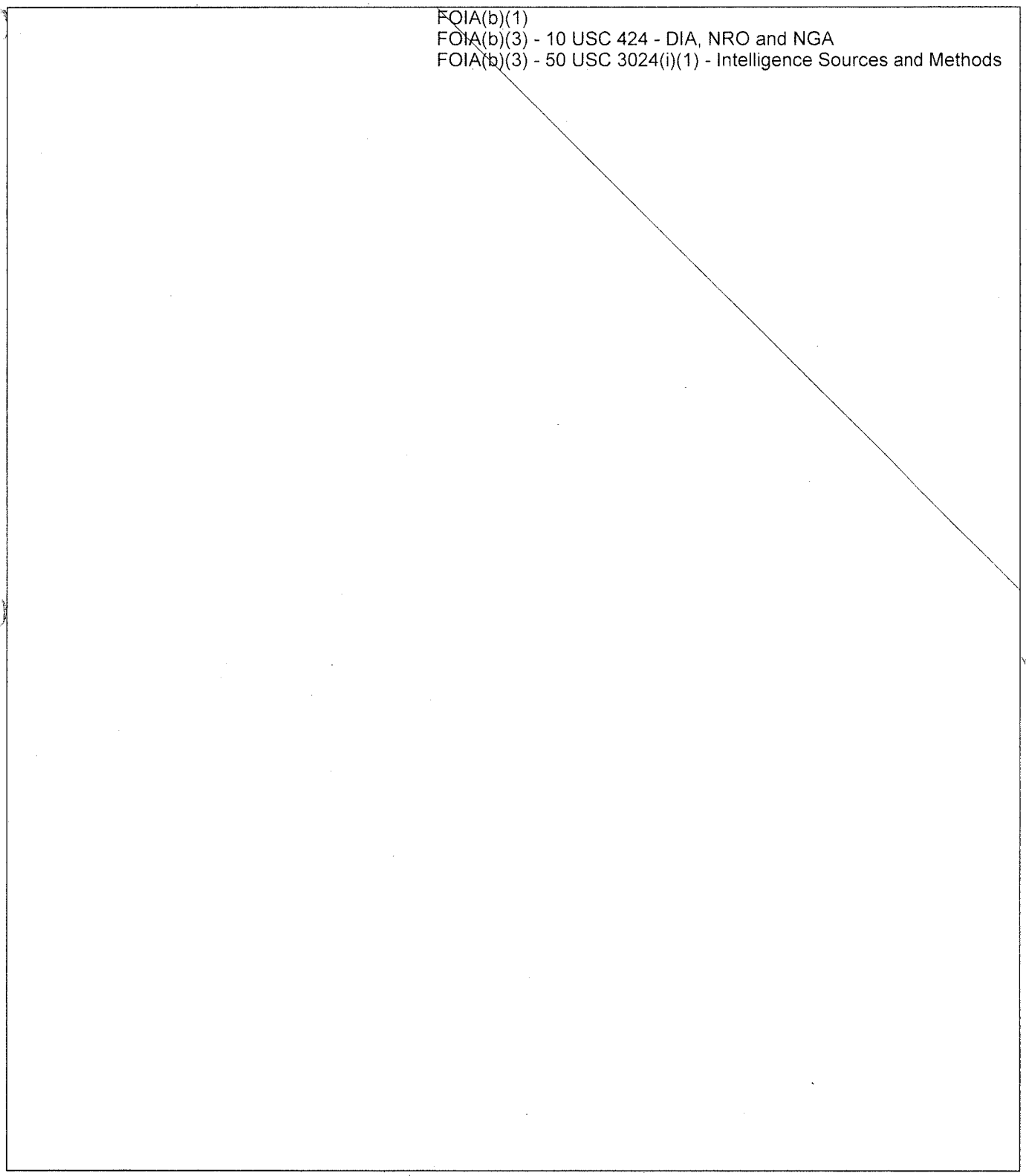


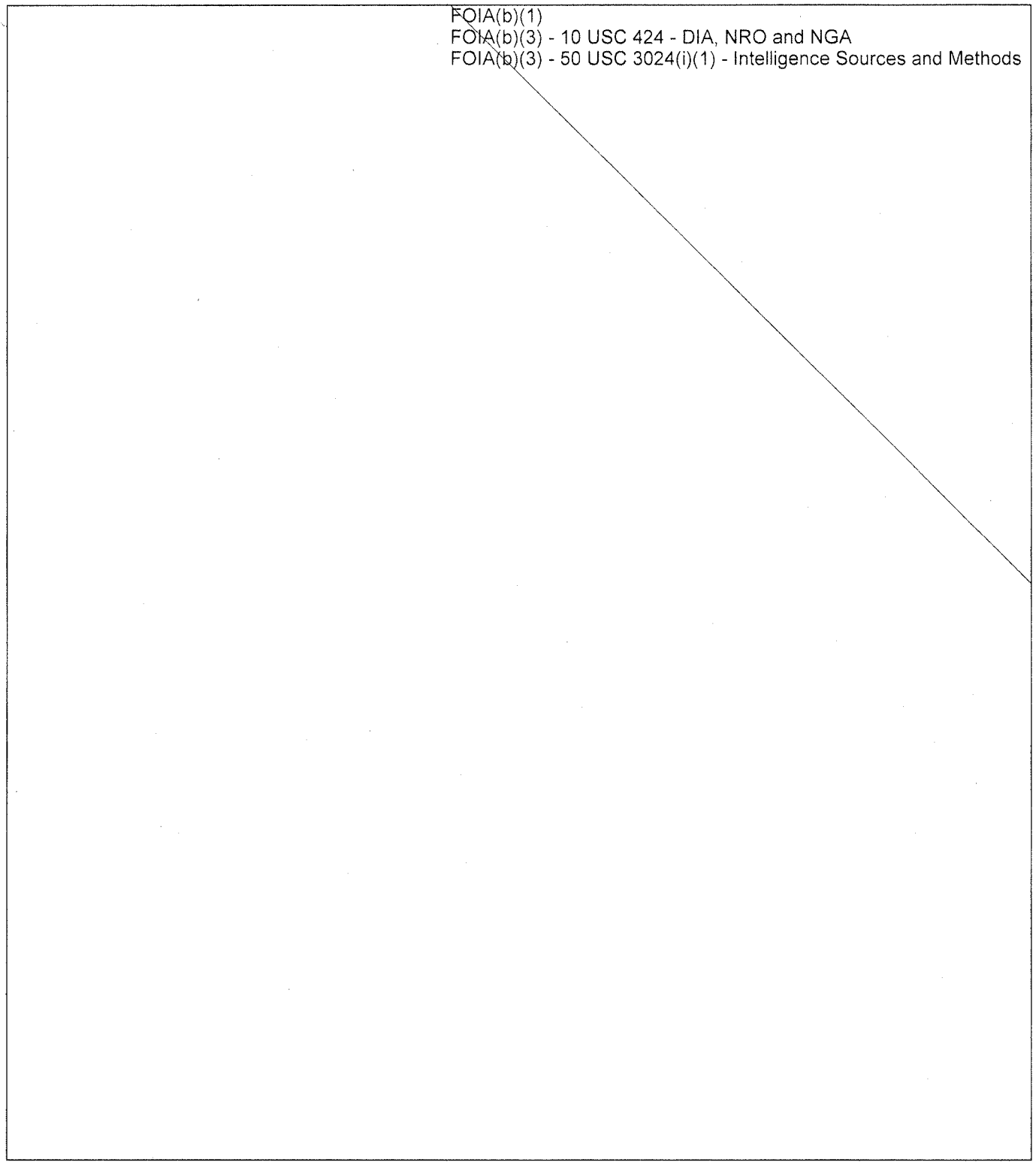
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

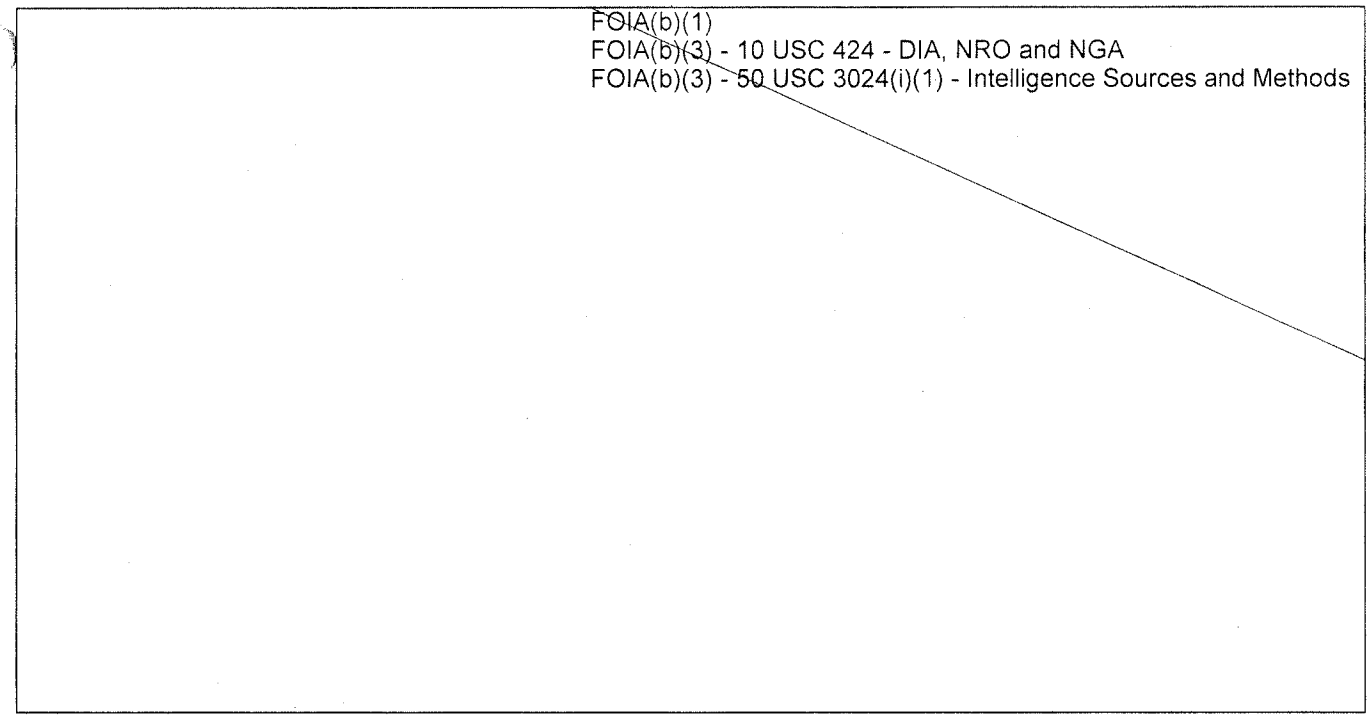


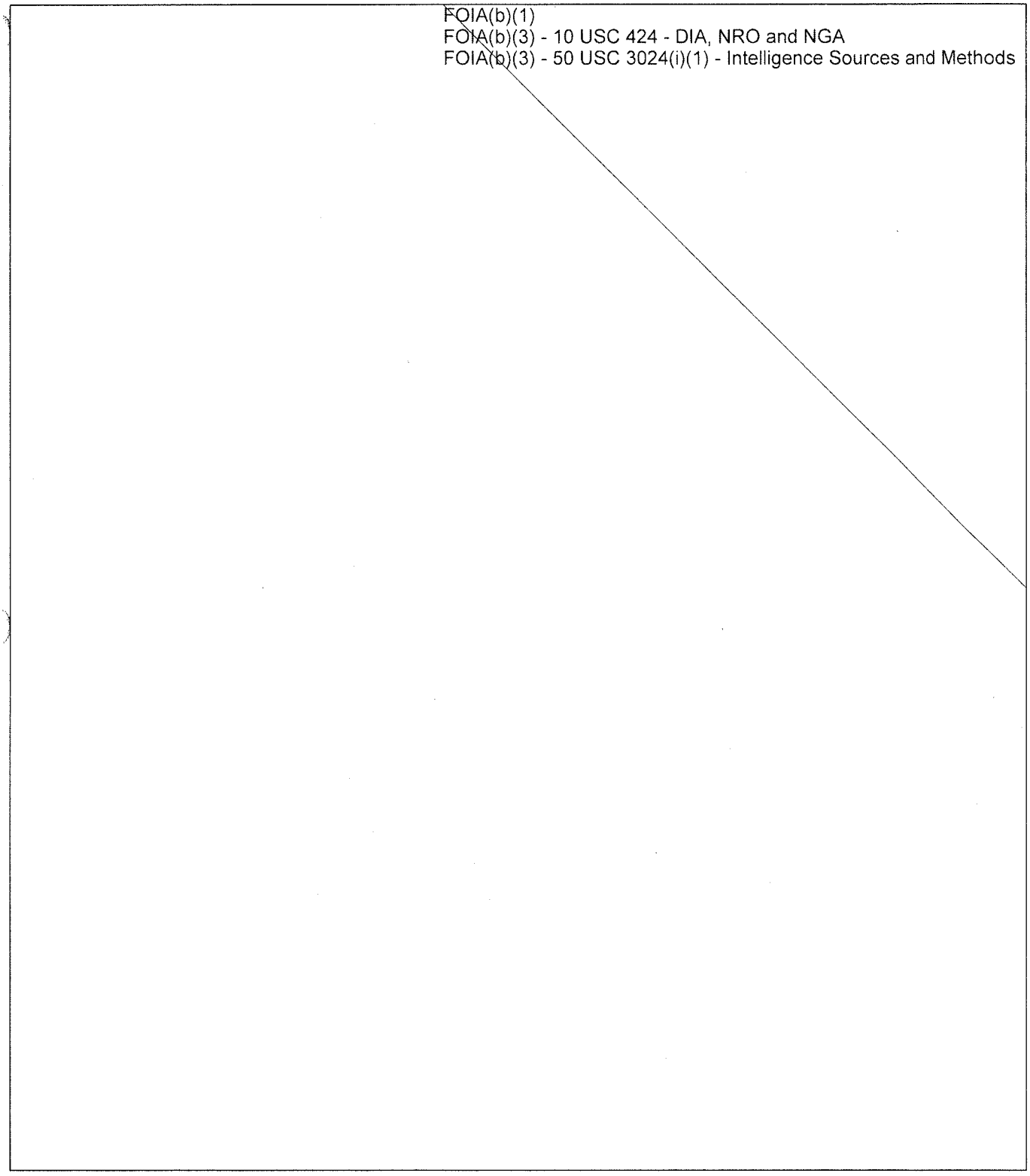


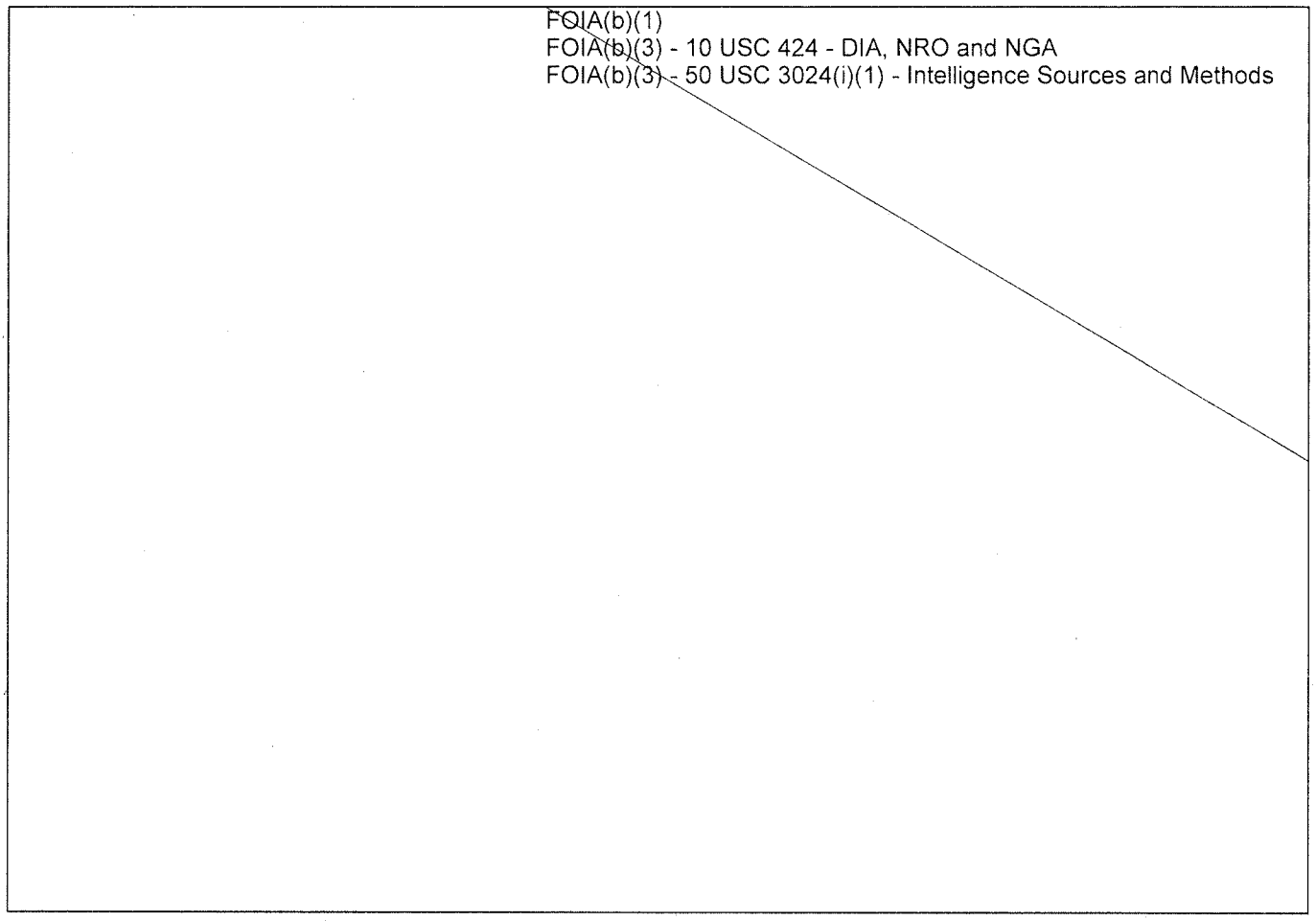


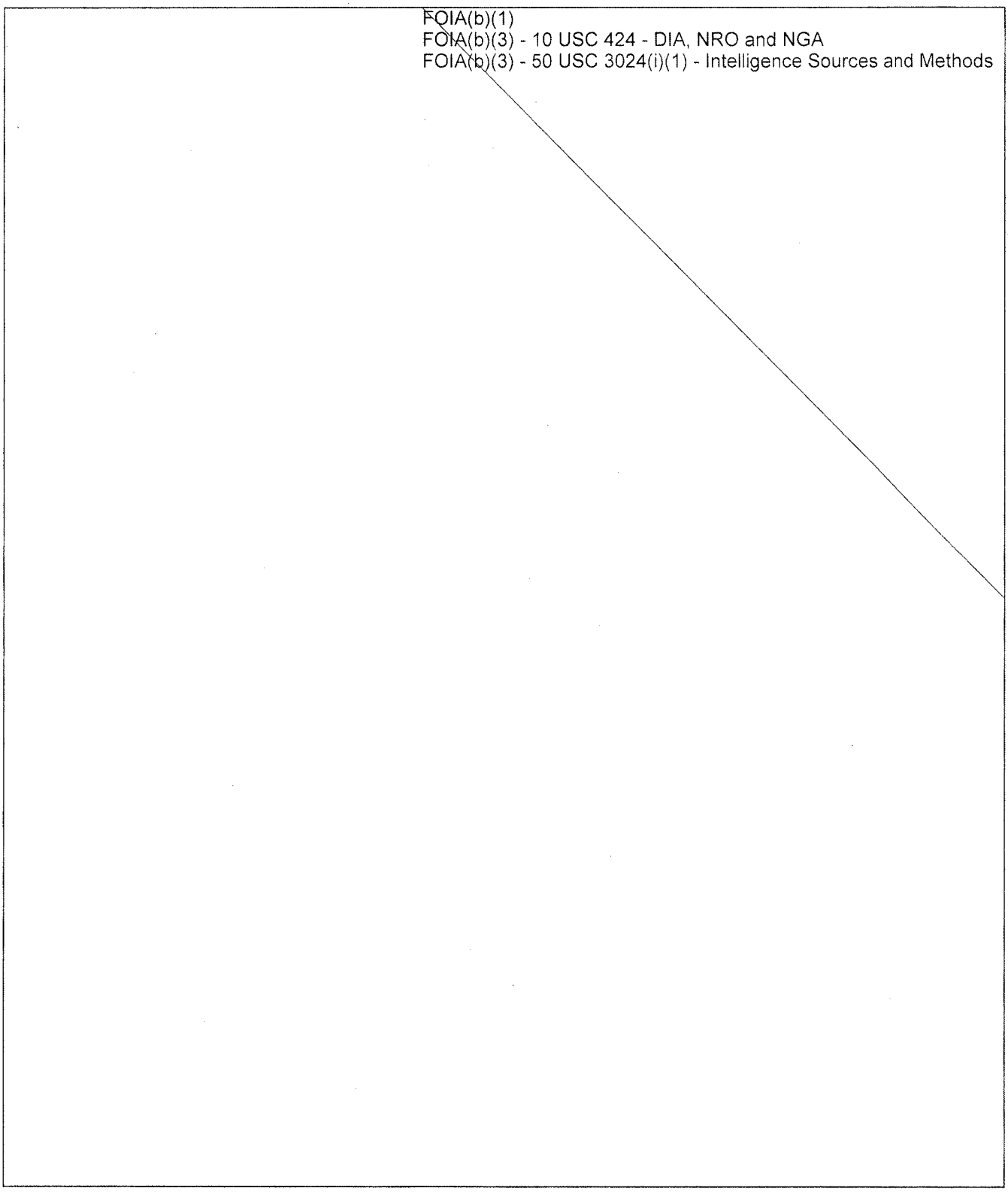


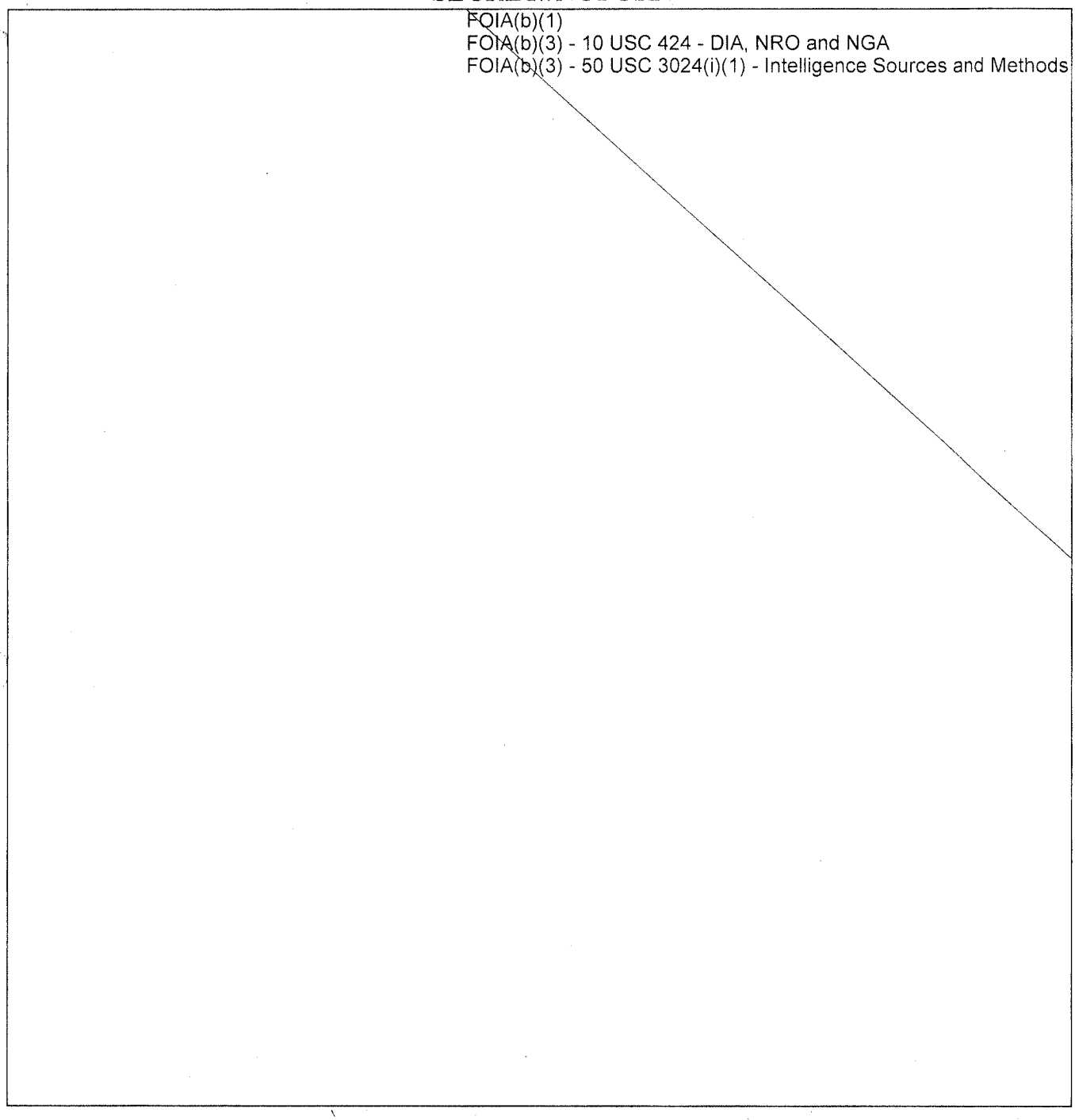


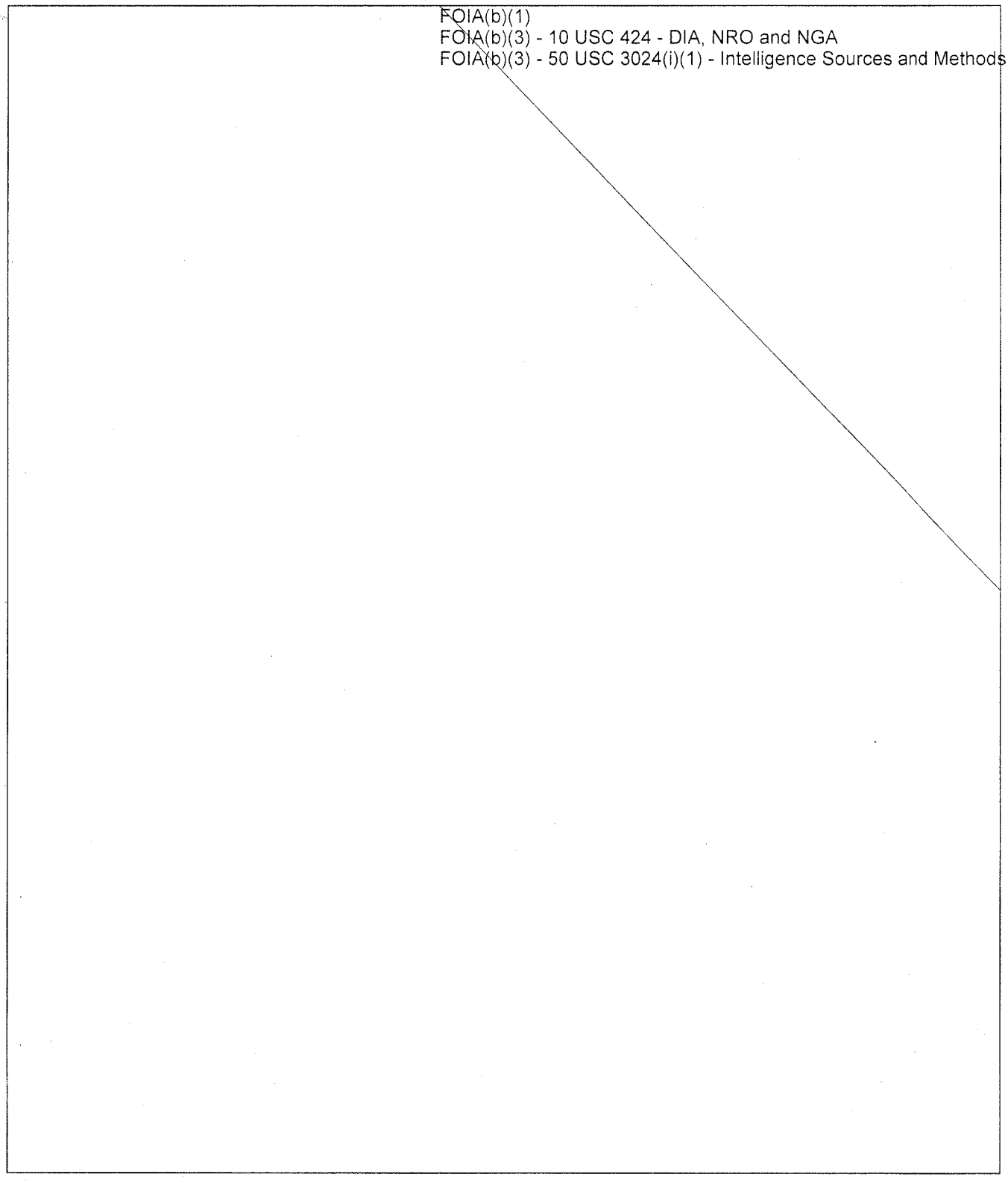


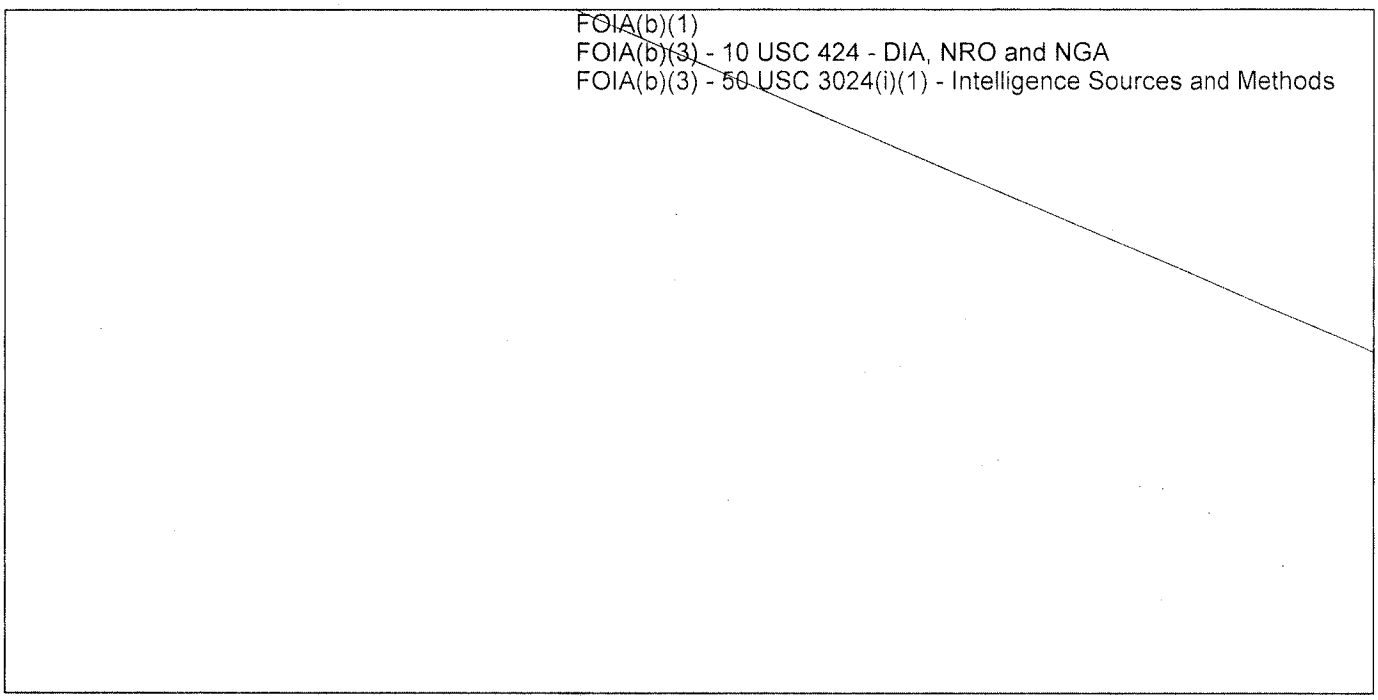


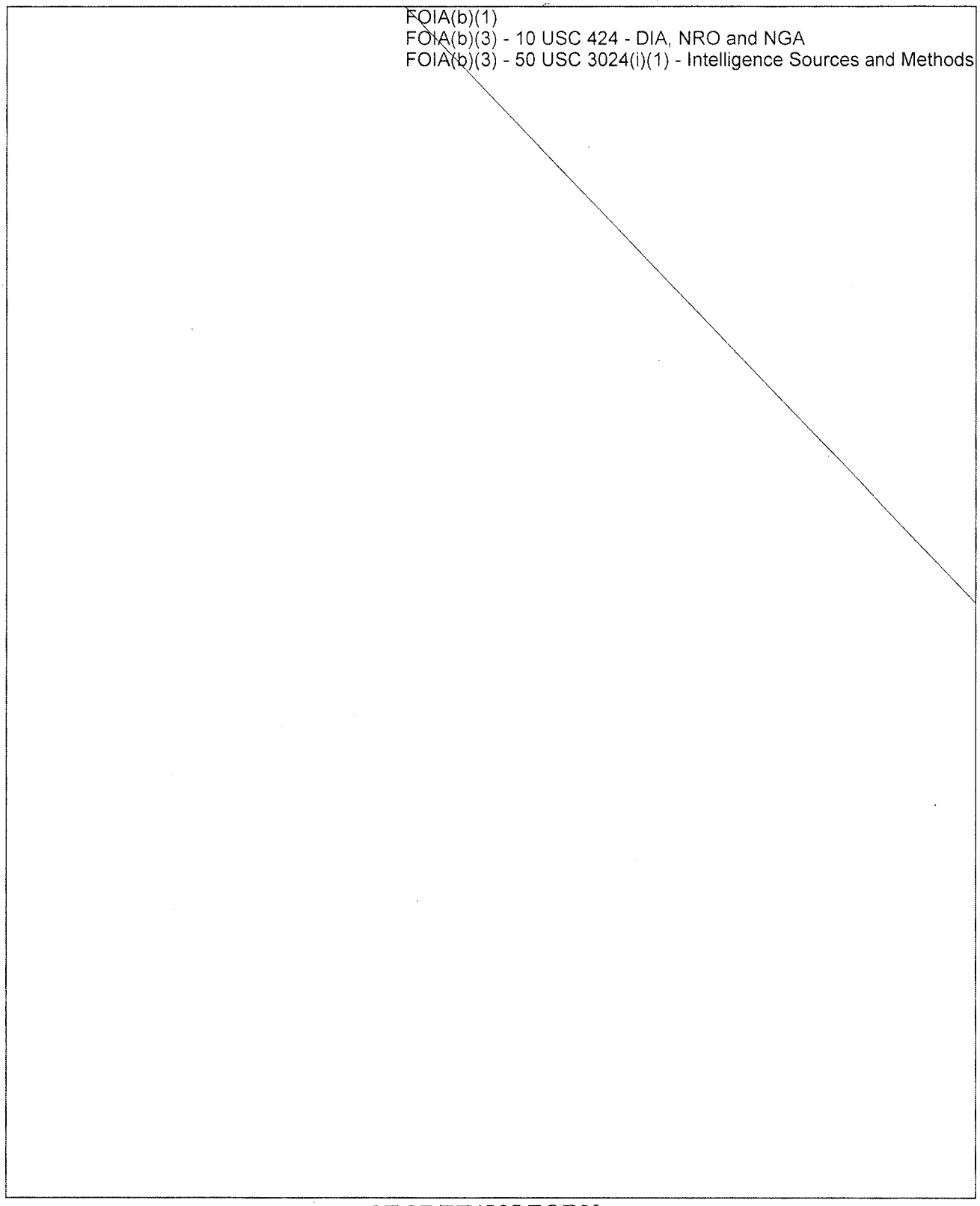


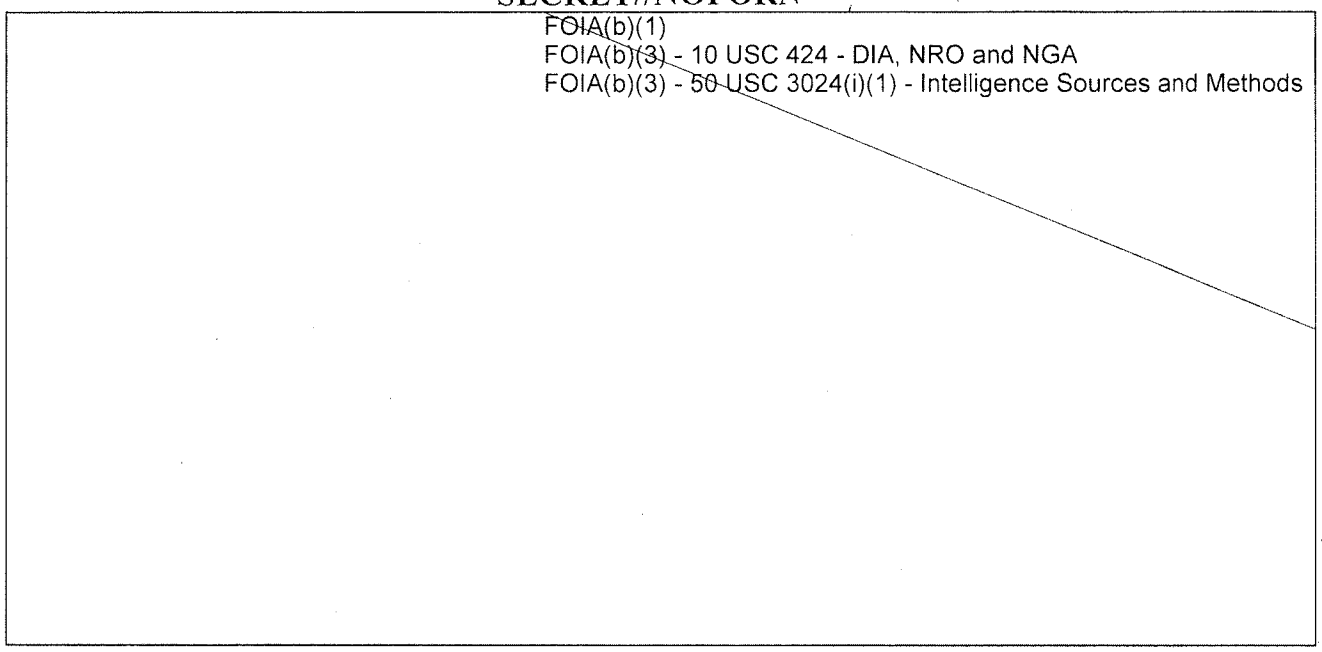


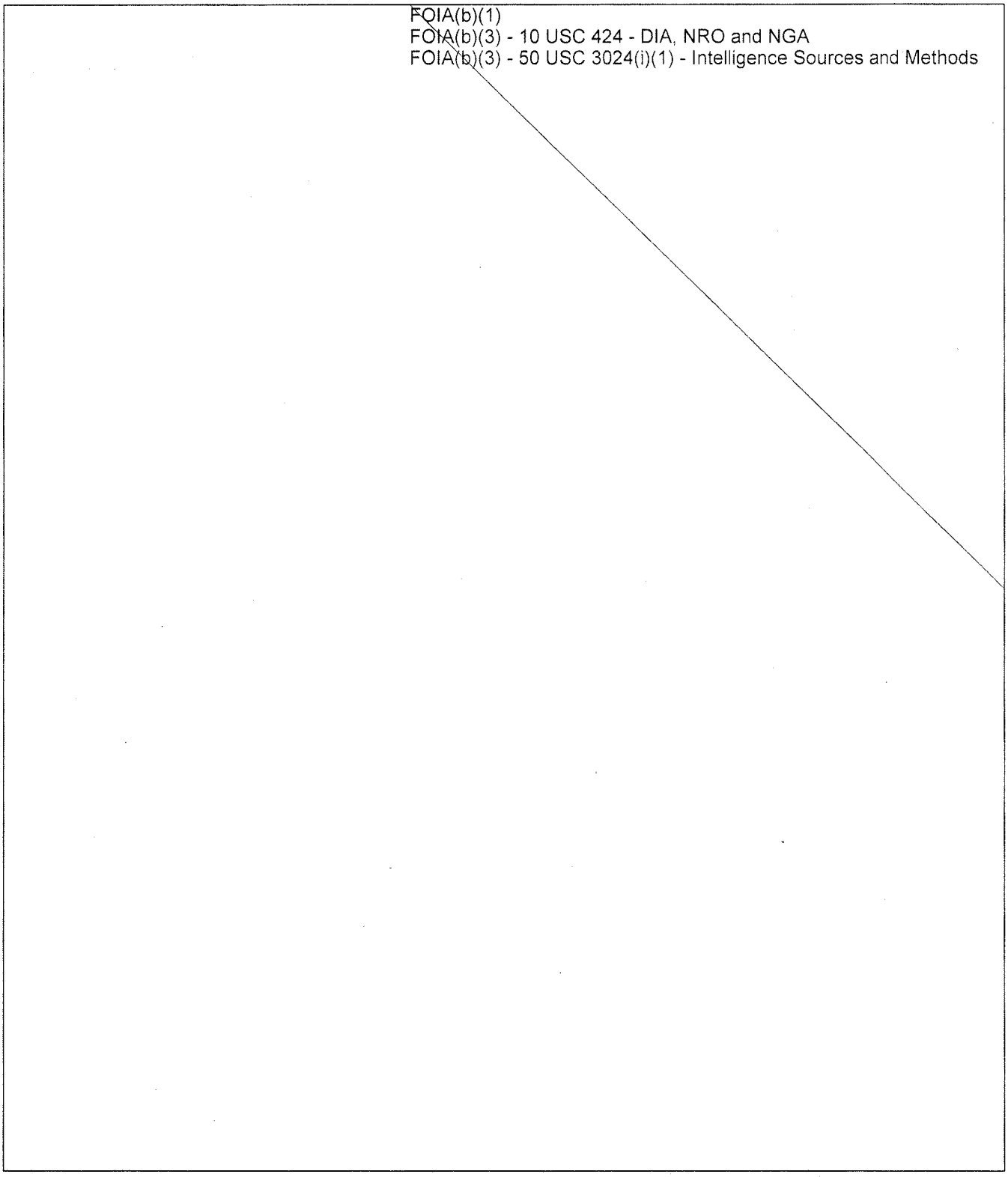




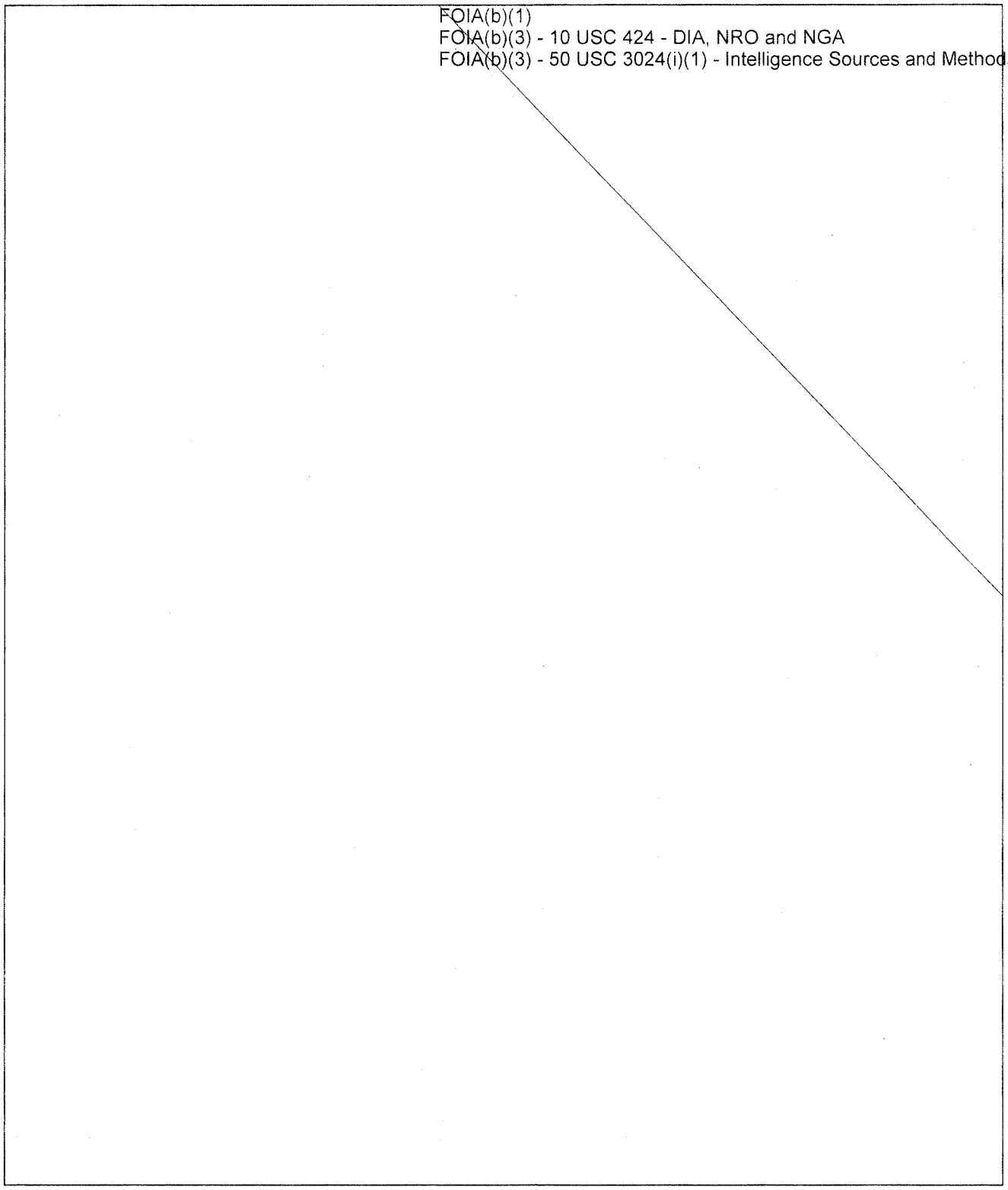


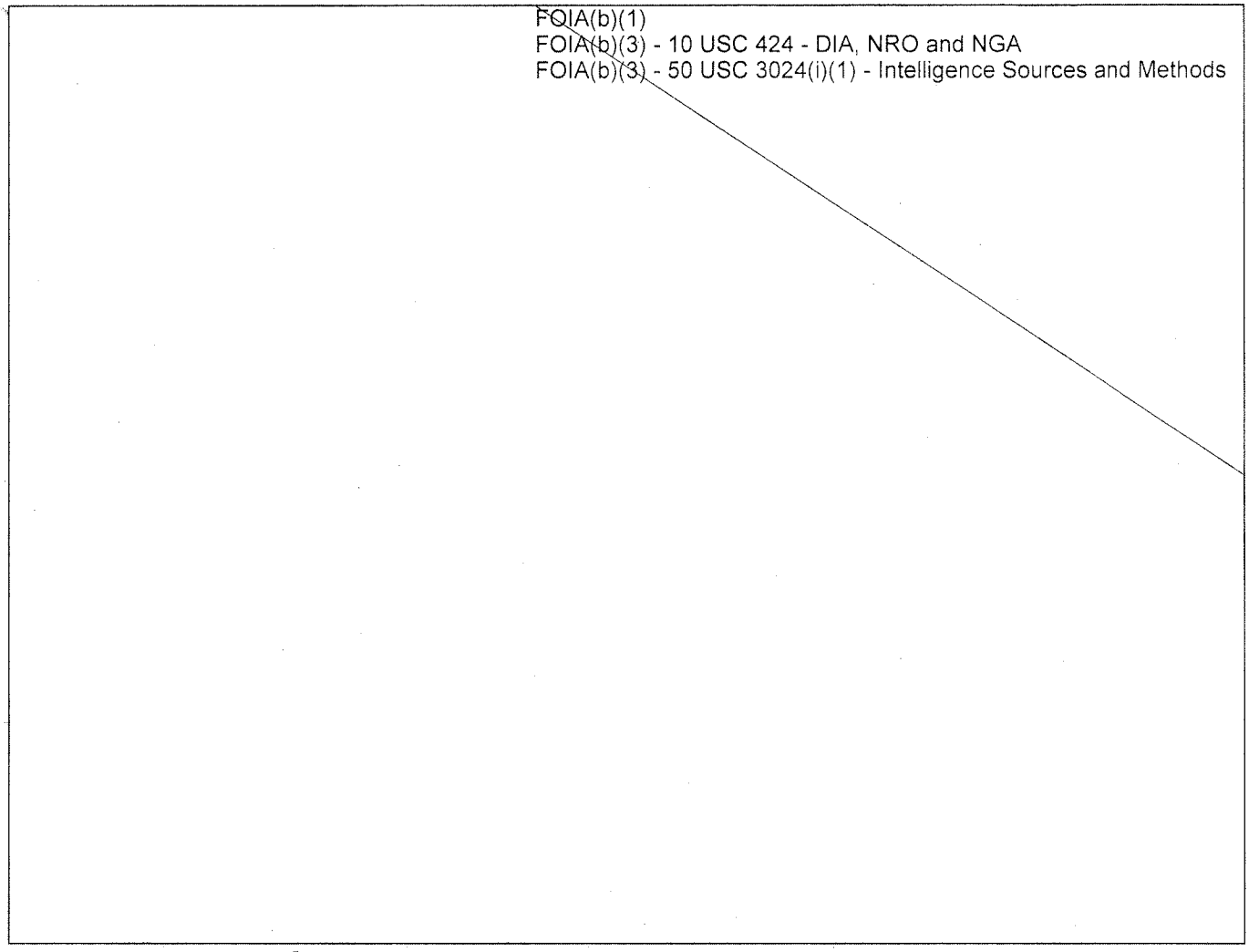


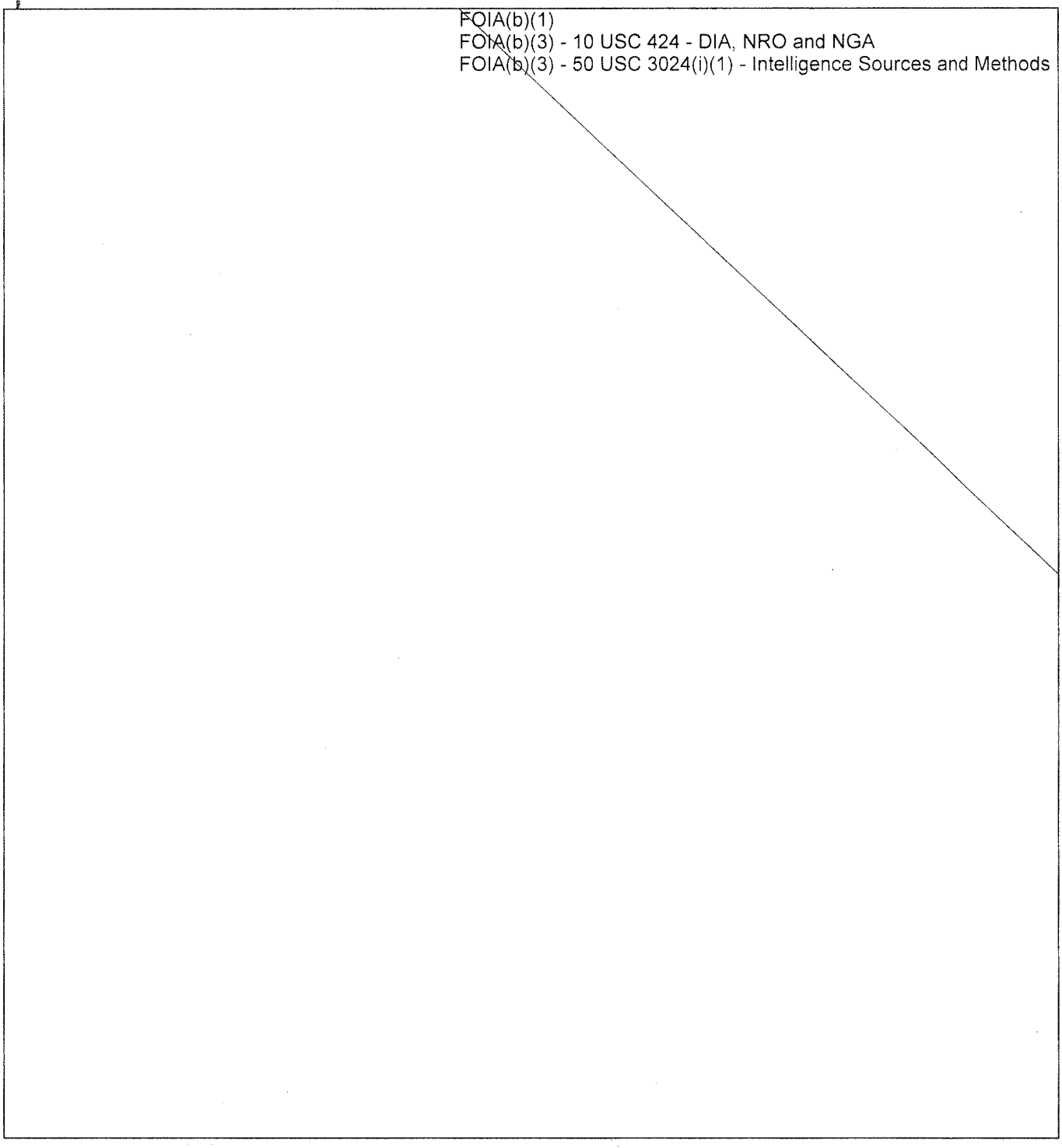


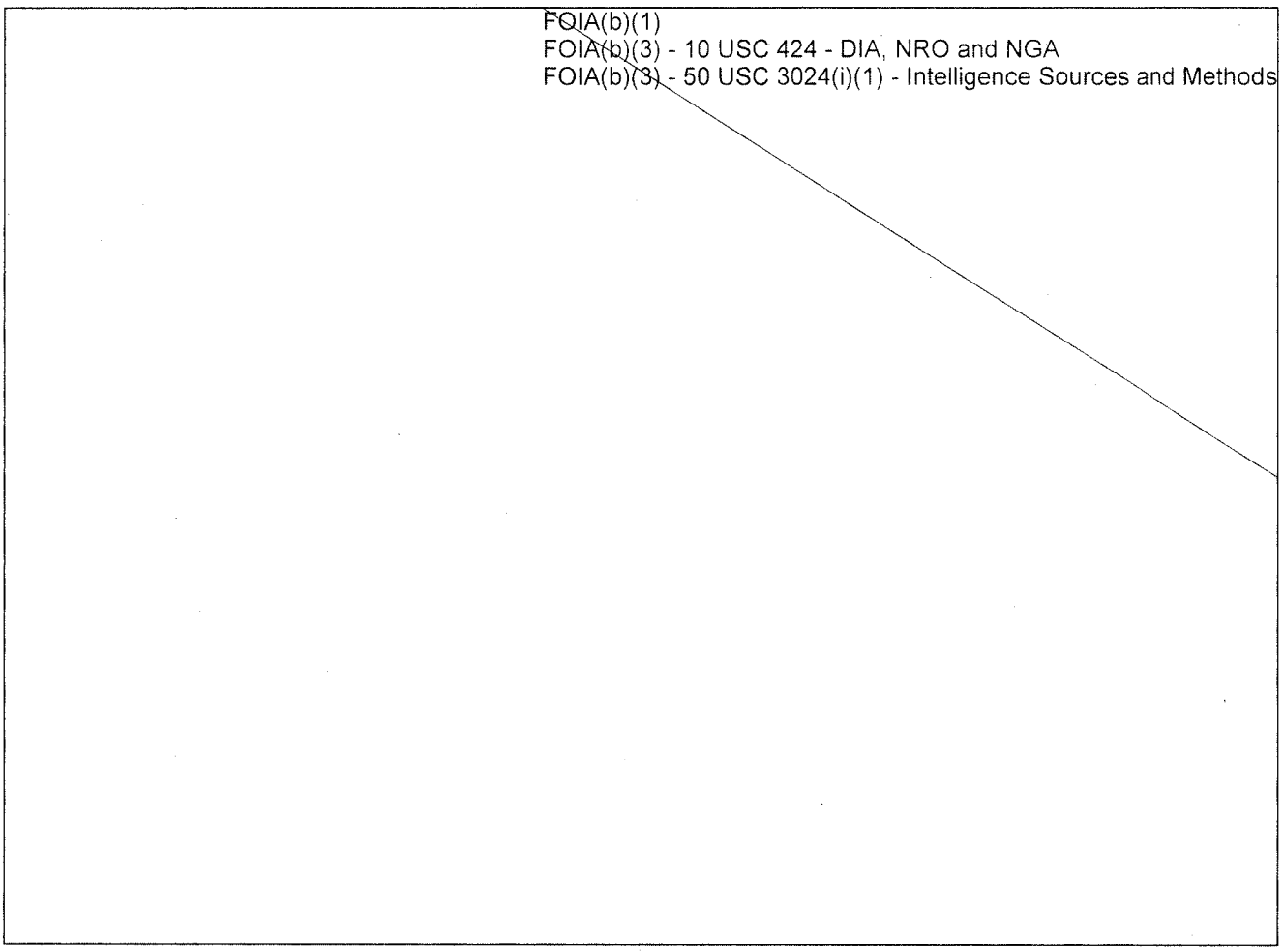


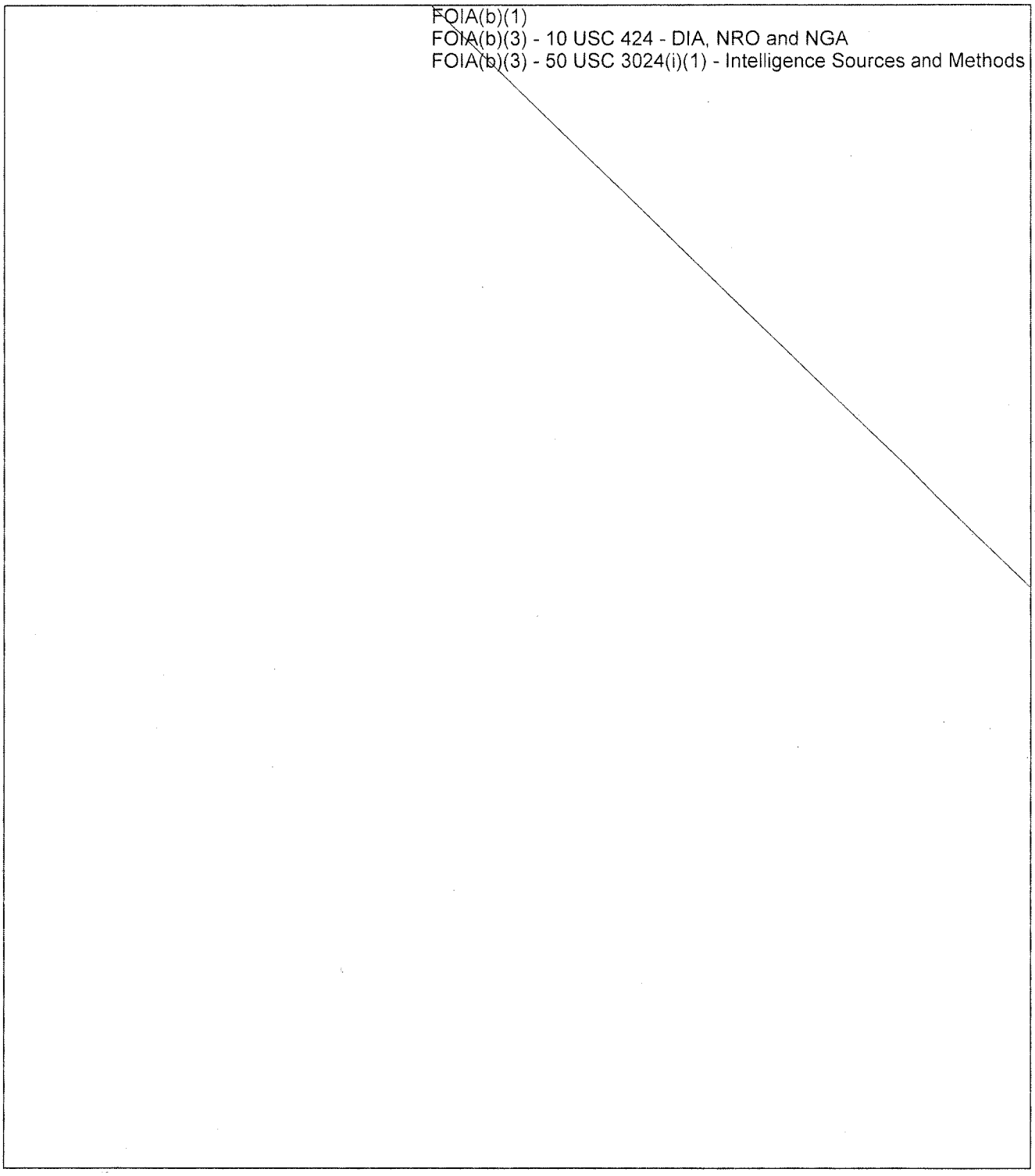
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods

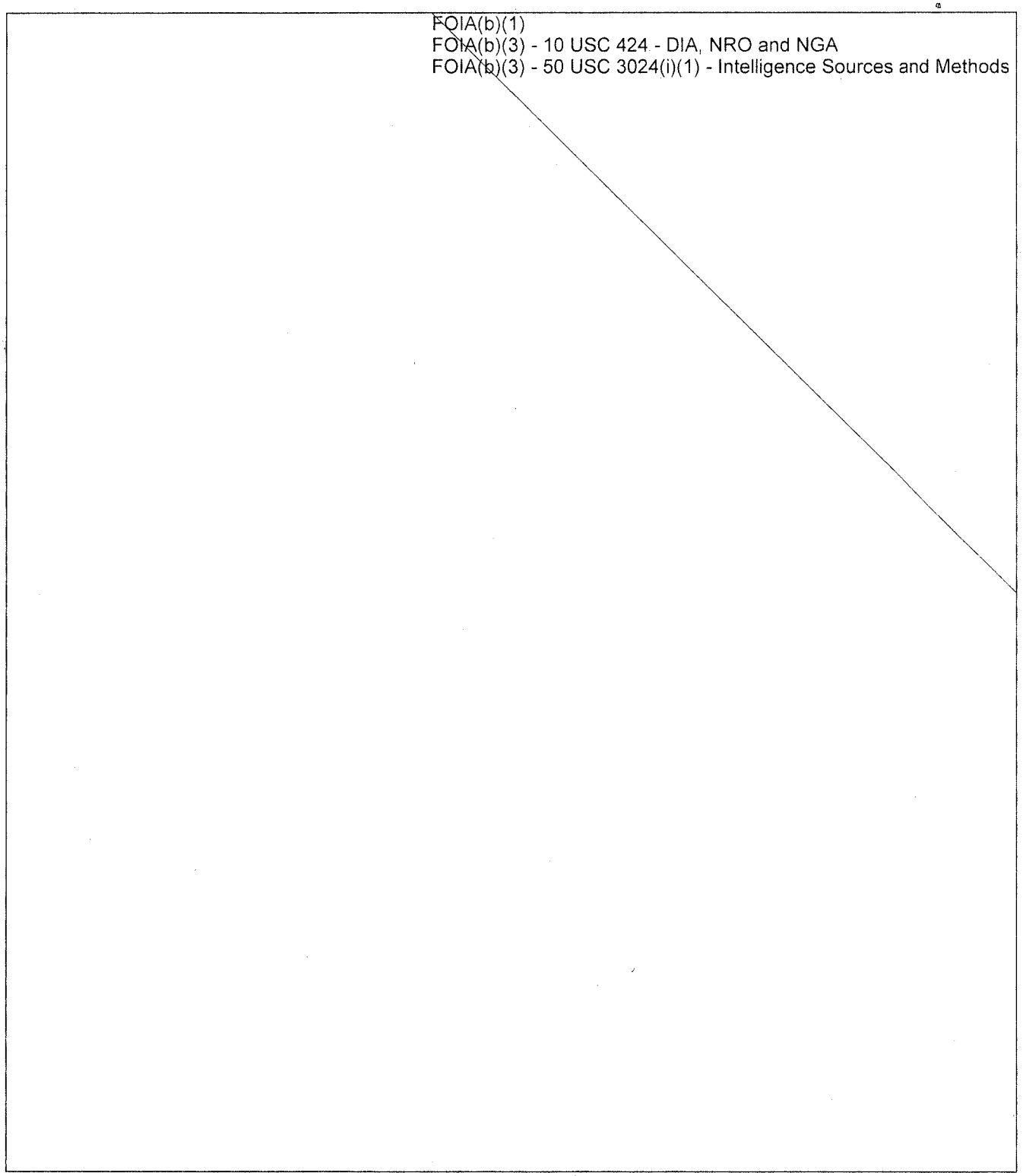




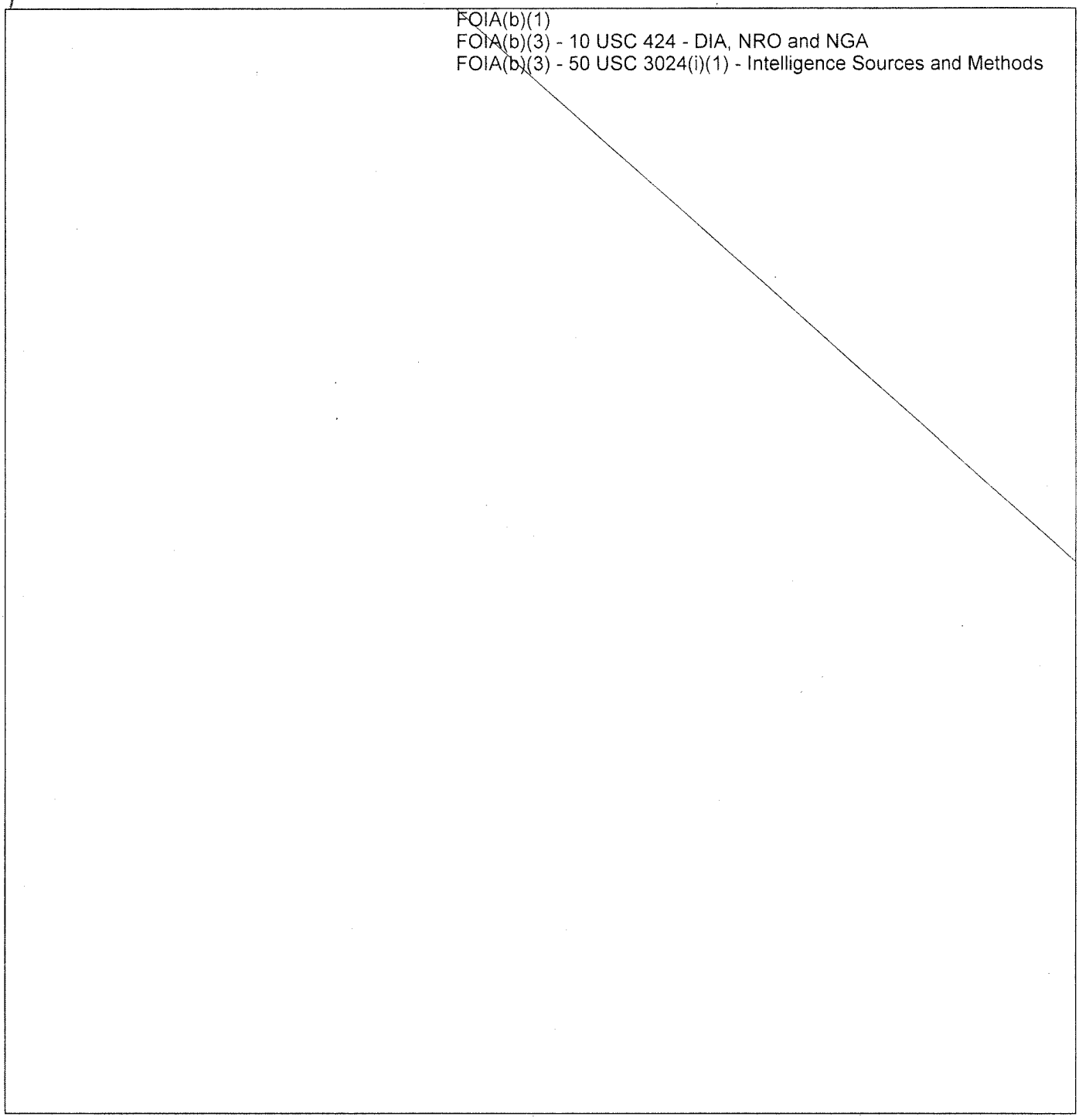


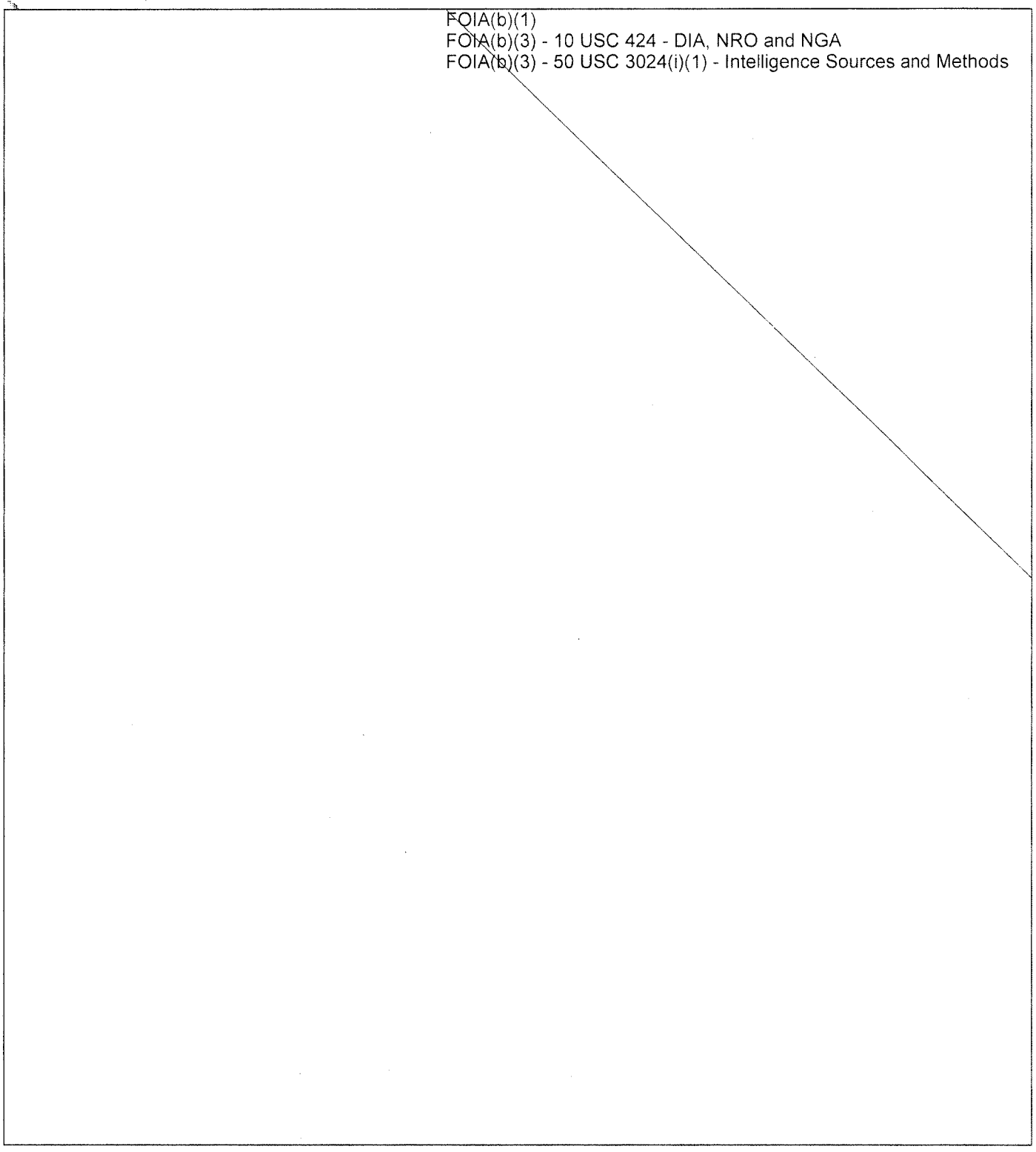






FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(3) - 50 USC 3024(i)(1) - Intelligence Sources and Methods





[redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)

**From:** [redacted]
**Sent:** Monday, June 25, 2012 9:30 AM
**To:** [redacted]
**Cc:** [redacted]

**Subject:** Compliance Documents, Contract HM0210-10-C-0003, RE: REQUEST FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

**Importance:** High

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270625
==========

[redacted] NGA wishes to reiterate that GeoEye shall remain compliant with the documents listed in the EnhancedView Statement of Work, especially those cited in Table 1 – List of Compliance Document, until such time as a document is formally revised either by Contract Modification or by direction of the Contracting Officer. These documents include all cited Security Classification Guides.

This reiteration is being provided due to Government concern raised by the statement contained in the GeoEye email below, second full paragraph:

[redacted] FOIA(b)(1)

[redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)

**From:** [redacted]
**Sent:** Thursday, June 14, 2012 12:48 PM
**To:** [redacted]
**Cc:** [redacted]

**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]

[redacted]

**From:** [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)
**Sent:** Thursday, June 14, 2012 12:48 PM
**To:** [redacted]
**Cc:** [redacted]

NGA-SU USA CTR

**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270614
==========

[redacted]

Thanks for the added clarification; that helps.

Per direction from Mr. Harris, and to avoid being non-compliant with Agency policy and procedure, please be advised we have completed clean-up efforts regarding spill issue for CIAD Case 3890. However, we strongly dispute this conclusion based on the past 15 months of working with the government customer in revising the *Commercial* SCG, with one goal in mind, to lessen ambiguity and avoid incidents such as this. Per the *Commercial Imagery* classification guide (revised draft) that was recently provided to the CDPs, citation numbers 4, [redacted] FOIA(b)(1) NGA

As you may not be aware, over the past 15 months, we have expended, on our own initiative and at our own cost, resources to bring clarity to extremely ambiguous classification statements that have confounded both CDPs and the government customer. We recognized early on and were instrumental in addressing the gaps associated with these unclear statements to NGAs attention, in order to provide much needed clarity. As we move forward with the EV program, we cannot continue operating in the present environment. We simply need clarity with respect what is sensitive and what is not, in order to protect EV equities. Unless otherwise directed, we shall continue to use the *draft revised Commercial SCG*, as the source for our derivative classification determinations.

In sum, we simply believe the basis for classifying slide #9, is unfounded based on the existing *Commercial* SCG and the revised draft. [redacted] FOIA(b)(1)

We respectfully request an expedited **final determination be made by the government** with respect to this issue. In the event our conclusions are not supported, we fully intend to submit a formal classification challenge to the NGA OCA, with appeal to the DNI if necessary, to support your classification decision along with a description describing the

damage sustained to the national security, in accordance with EO 13526, section 1.8 and ISOO implementing directive 32 CFR Part 2001, section 2001.14. Should such an appeal be resolved in our favor, we also intend to seek reimbursement for the costs associated with clean-up efforts. FOIA(b)(1) NGA

I look forward to hearing from you soon.

Respectfully,

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

Director, Security
GeoEye Inc.

**From**
**Sent:** Tuesday, June 12, 2012 3:00 PM
**To:**
**Cc:**
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270612
==========

Thank you for your patience in this review. Please understand that this is not merely the fact that FOIA(b)(1) NGA

Please let me know if you have additional questions.

**From:**
**Sent:** Friday, June 01, 2012 1:17 PM
**To:**

**Cc:** [redacted]
**Subject:** FW: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270601
==========

[redacted]

I am requesting clarification on the GeoEye UNCLAS//FOUO/PROPIN PPT slide deck that was forwarded to your office for review and a classification determination [redacted] directed me back to your organization. See details below.

With respect to the PPT content, please clarify the specific slide(s) where the information was determined to be classified. Upon my review, I did not draw the same conclusion. My understanding is that OCIO determined the issue to be:

**"... At issue is the fact that the slide shows that the UNCLASS and classified systems are connected via the High Speed Guard."**

The slide deck shows an architectural diagram with a box labeled as "HSG" without revealing specific details such as message content, rule sets, data payloads, IP addresses, ISO model information, processing methodologies or any 2 items from the enumerated list that are directly tied to the HSG components.

When standing alone, the SCG states the enumerated list is UNCLAS//FOUO . There is no association with the secure operating environment to include accredited systems.
The slide is simply an architectural overview.

In view of the above and because a new commercial guide has not been published with the HSG details, I am requesting classification guidance be provided to me regarding functional architectural diagrams, drawings, charts with interfaces that do not reveal any specific details. I would like this guidance at the earliest opportunity for mitigation plans.

Respectfully,

[redacted]
Director, Security
GeoEye Inc.

---

**From:** [redacted]
**Sent:** Friday, June 01, 2012 11:29 AM
**To:** [redacted]
**Cc:**
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270601
==========

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

Please contact NGA Classification Management for additional details regarding specific slides.

v/r,

**From:**
**Sent:** Friday, June 01, 2012 10:46 AM
**To:**
**Cc:**
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270601
==========

A comprehensive clean-up effort will be initiated for this presentation. Please be advised the content of this presentation resides on the GeoEye corporate network.

The Defense Security Service (DSS) also will be notified as well. Your contact information will be provided to the DSS representative, may require additional privileged information from your office. FOIA(b)(6)

With respect to the content in the presentation, please clarify the specific slide that classified information is to be found. It is not clear in your email below. The enumerated list as a standalone is UNCLAS//FOUO.

Director, Security
GeoEye Inc.

**From:**
**Sent:** Friday, June 01, 2012 10:16 AM
**To:**
**Cc:**

**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890
**Importance:** High

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270601
==========

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

The content in the PowerPoint should be protected as S//NF based on the NGA SCG AIS Table Lines 11 and 17. Please provide your incident cleanup report. If I have not received confirmation of the sanitization effort before my investigation is completed, I will include that non-compliance within the report as well.

Please see below for Classification Management's decision (two separate emails) and have provide me a statement explaining what, when, how, networks used, etc.).

Thanks.

--
**From:**
**Sent:** Thursday, May 31, 2012 5:35 PM
**To:**
**Cc:**
**Subject:** RE: CIAD Case Ref 3890

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370531
==========

The information is classified IAW NGA SCG AIS Table, line items 11 & 17.

Please let me know if you have any questions.

--
Portion of the additional explanation...

**From:**
**Sent:** Thursday, May 31, 2012 12:14 PM
**To:**

**Cc:** [redacted]
**Subject:** RE: CIAD Case Ref 3890

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370531
==========

[redacted]

FOIA(b)(1) NGA

[redacted]

--

v/r,

[redacted]

**From:** [redacted]
**Sent:** Thursday, May 31, 2012 3:04 PM
**To:** [redacted]
**Cc:** [redacted]
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890
**Importance:** High

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270531
==========

[redacted]

I need to see a final review of the material and a formal determination from CM that the material in question is considered classified with references to the source document and an explanation of why the determination was made. I have yet to date received this or an initial discovery report that even stated this document is in question. The only official correspondence that this material is in question is from you informing me that this was a concern.

Please advise, as I am not comfortable going through a very costly sanitization and clean up of material with no official document from the office of principle responsibility.

Thanks!

[redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

**From:** [redacted]
**Sent:** Thursday, May 31, 2012 2:44 PM
**To:** [redacted]
**Cc:** [redacted]
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890
**Importance:** High

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270531
==========

[redacted]

I have been informed that NGA's Classification Management Team's decision is final (information contained in the spreadsheet should be S//NF) and to move forward with my investigation. Please execute your classified spillage cleanup plans within your accreditation paperwork and provide me a written statement of what was done when completed. Your staff should ensure that [redacted] corporate system and network shares are sanitized. You are advised that the email would have been created on or prior to 19 April 2012 and the attachment was titled 'Read-Ahead for 20120423 GeoEye C and A Discussion.pptx'.

[redacted]

Where did you originally create the PowerPoint presentation? On NGANet, SecNet or your Corporate System? If other than NGANet, how was the file transferred to NGANet to be subsequently emailed?

v/r,

[redacted]

**From:** [redacted]
**Sent:** Thursday, May 31, 2012 9:14 AM
**To:** [redacted]
**Cc:** [redacted]
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Reason: 1.4(c), (g)
Declassify On: 20270531
Derived From: NGA SCG AIS-08.1.1
==========

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

[redacted]

The information that you have seen from my emails is the only correspondence regarding the request...

I am assuming that in this case silence is consensus on closing this out?

Thank you for the follow-up...

[redacted]

**From:** [redacted]
**Sent:** Wednesday, May 30, 2012 5:12 PM
**To:** [redacted]
**Cc:** [redacted]
**Subject:** RE: REQUEST FOR FOR FINAL CLASSIFICATION DETERMINATION - CIAD Case Ref: 3890

Classification: ~~SECRET//NOFORN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20270530
==========

[redacted]

Have you all clarified anything with the Classification Management? If so, can you forward the information to me so that I can close out this incident? If not, can you follow up with Classification Management for an update?

Thanks.

v/r,

[redacted]

**From:** [redacted]
**Sent:** Tuesday, May 15, 2012 10:49 AM
**To:** [redacted]

[redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6) FOIA(b)(6)

**rom:** [redacted]
**Sent:** Tuesday, November 15, 2011 1:10 PM
**To:** [redacted] FOIA(b)(6)
**Cc:** [redacted]
**Subject:** RE: Interim Security Classification Guidance

[redacted]

Unfortunately the SI group did not agree with providing interim guidance and we need to wait until a revised, released version is available.

[redacted]

[redacted]
GeoEye Program Manager - EnhancedView/NextView NGA/SUG
Office: [redacted]
Cell: [redacted] (Blackberry)

-----Original Message-----
From: [redacted] FOIA(b)(6)
Sent: Tuesday, November 08, 2011 4:40 PM
To: [redacted]
Cc: [redacted]
Subject: Interim Security Classification Guidance

[redacted]

I have asked [redacted] to add to the SCG working group agenda, the need for "interim" security classification guidance to be promulgated by the USG in lieu of working with the current acquisition guide which as you know, has many inconsistencies and lacks the fidelity need to protect the data.

The pros behind doing so now will reduce any spills that come about as a result of old guidance. My understanding is that you will be at GeoEye soon and I will be happy to give you more background. We believe this issue is good for the USG and the CDP's and will avoid unnecessary work associated with data spills until the revised guide is signed.

**Interagency Security Classification Appeals Panel**

c/o Information Security Oversight Office
700 Pennsylvania Avenue, N.W., Room 100
Washington, D.C. 20408
Telephone: (202) 357-5250
Fax: (202) 357-5907
E-mail: iscap@nara.gov

MEMBERS

DEPARTMENT OF DEFENSE
Reginald D. Hyde
DEPARTMENT OF JUSTICE
Mark A. Bradley, Acting Chair
DEPARTMENT OF STATE
Margaret P. Grafeld
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
Sheryl J. Shenberger
NATIONAL SECURITY STAFF
Mary I. Ronan
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Corin Stone

EXECUTIVE SECRETARY

John P. Fitzpatrick
Director
INFORMATION SECURITY OVERSIGHT OFFICE

January 17, 2013

Reference: ISCAP No. 2013-035

Brigadier General Joseph Composto, USMC (Ret.)
Director, Security and Installation Operations
Mail Stop N81-SI
National Geospatial-Intelligence Agency
7500 GEOINT Drive
Springfield, VA 22150

Dear General Composto:

The Interagency Security Classification Appeals Panel (ISCAP) has received a classification challenge appeal under section 5.3(b)(1) of Executive Order 13526, "Classified National Security Information," from Mr. William Schuster of GeoEye, Incorporated. Specifically, by the enclosed correspondence dated January 9, 2013, Mr. Schuster has appealed the National Geospatial-Intelligence Agency's final decision on his internal agency challenge appeal under section 1.8 of the Order. Please be advised that his request now falls under the jurisdiction of the ISCAP pursuant to 32 C.F.R. Part 2003, section 2003.11, the ISCAP Bylaws.

Please provide copies of the pertinent material and related correspondence regarding this classification challenge appeal to the ISCAP staff as soon as possible and within 30 days of the date of this letter. If you wish to discuss this appeal, please contact Neena Sachdeva, William Carpenter, or me at (202) 357-5250 and reference ISCAP No. 2013-035.

Sincerely,

JOHN P. FITZPATRICK
Executive Secretary

Enclosures

cc: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

Mr. Mark A. Bradley, Director of FOIA, Declassification, and Pre-publication Review,
National Security Division, Office of Law and Policy, U.S. Department of Justice
Acting Chair of the ISCAP

Mr. John F. Hackett, Director, Information Management
Office of the Director of National Intelligence
Liaison to the ISCAP

**Interagency Security Classification Appeals Panel**

c/o Information Security Oversight Office
700 Pennsylvania Avenue, N.W., Room 100
Washington, D.C. 20408
Telephone: (202) 357-5250
Fax: (202) 357-5907
E-mail: iscap@nara.gov

MEMBERS

DEPARTMENT OF DEFENSE
Reginald D. Hyde
DEPARTMENT OF JUSTICE
Mark A. Bradley, Acting Chair
DEPARTMENT OF STATE
Margaret P. Grafeld
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Corin Stone
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
Sheryl J. Shenberger
NATIONAL SECURITY STAFF
Mary I. Ronan

EXECUTIVE SECRETARY

John P. Fitzpatrick
Director
INFORMATION SECURITY OVERSIGHT OFFICE

Real file

COPY

January 17, 2013

Reference: ISCAP No. 2013-035

Mr. William Schuster
Chief Operating Officer
GeoEye, Inc
2325 Dulles Corner Boulevard
Herndon, VA 20171

Dear Mr. Schuster:

Please be advised that on January 15, 2013, the Interagency Security Classification Appeals Panel (ISCAP) received your letter dated January 9, 2013, lodging a classification challenge appeal under section 5.3(b)(1) of Executive Order 13526, "Classified National Security Information." As Executive Secretary, I have requested copies of the pertinent material and related correspondence from the National Geospatial-Intelligence Agency. Following receipt of this material and pending our determination that the classification challenge appeal meets the requirements of the Order and the ISCAP bylaws, your appeal will be placed on the ISCAP docket.

Copies of the Order, its Implementing Directive, and the ISCAP Bylaws 32 C.F.R. Part 2001 and 2003 respectively, are available to you on the Information Security Oversight Office (ISOO) website www.archives.gov/isoo/policy-documents. If you have any questions regarding your challenge, please contact Neena Sachdeva, William C. Carpenter or me at (202) 357-5250 and reference ISCAP No. 2013-035.

Sincerely,

JOHN P. FITZPATRICK
Executive Secretary

cc [redacted] Director, Security, GeoEye, Inc.

FOIA(b)(6)

NW#:67776
DocId:34498398


# FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

## The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

Federal Register
Vol. 78, No. 33
Tuesday, February 19, 2013

# Presidential Documents

Title 3—

The President

## Executive Order 13636 of February 12, 2013

## Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1.** *Policy.* Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

**Sec. 2.** *Critical Infrastructure.* As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

**Sec. 3.** *Policy Coordination.* Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

**Sec. 4.** *Cybersecurity Information Sharing.* (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of

Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

**Sec. 5.** *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

**Sec. 6.** *Consultative Process.* The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

**Sec. 7.** *Baseline Framework to Reduce Cyber Risk to Critical Infrastructure.* (a) The Secretary of Commerce shall direct the Director of the National

Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 *et seq.*), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

**Sec. 8.** *Voluntary Critical Infrastructure Cybersecurity Program.* (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

**Sec. 9.** *Identification of Critical Infrastructure at Greatest Risk.* (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

**Sec. 10.** *Adoption of Framework.* (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification

of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

**Sec. 11.** *Definitions.* (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

**Sec. 12.** *General Provisions.* (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater

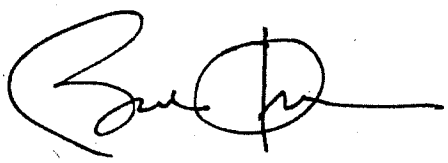
extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
*February 12, 2013.*

[FR Doc. 2013–03915
Filed 2–15–13; 11:15 am]
Billing code 3295–F3

[redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)

**From:** [redacted]
**Sent:** Thursday, December 27, 2012 10:38 AM
**To:** [redacted]
**Subject:** FW: Read-Ahead Package for Monday Meeting with OCIO
**Attachments:** Read-Ahead for 20120423 GeoEye C and A Discussion.pptx

Classification: ~~SECRET//NOFORN/PROPIN~~

Classified By: [redacted]
Derived From: NGA SCG AIS-08.1.1
Declassify On: 20371231
==========

Here's the original email when I sent this to the government. I went ahead and labeled this email S//NF even though I still believe the material to be U//FOUO.

[redacted]

**From:** [redacted]
**Sent:** Thursday, April 19, 2012 12:27 PM
**To:** [redacted]
**Subject:** Read-Ahead Package for Monday Meeting with OCIO

Classification: UNCLASSIFIED/~~/FOUO~~
==========

[redacted]

Attached is the read-ahead for Monday's 1000 meeting with OCIO and the PMO. We're a "go" for the meeting on our side. Please be sure to include me on the meeting invite so I can further distribute to others.

Please provide the secure VTC/dial-in number as we will have remote participants.

Regards,

[redacted]

==========
Classification: UNCLASSIFIED/~~/FOUO~~

==========
Classification: ~~SECRET//NOFORN/PROPIN~~