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 E. Rouan
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Corin Stone

EXECUTIVE SECRETARY
John P. Fitzpatrick
Director
INFORMATION SECURITY OVERSIGHT OFFICE

February 7, 2013

Reference: ISCAP No. 2013-030

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 Dr. Clark S. Penrod of Applied Research Laboratories, University of Texas at Austin. Specifically, by the enclosed correspondence dated January 31, 2013, Dr. Penrod has appealed the failure of the Defense Security Service to provide a written response within 120 days on his classification challenge 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.

Because this classification challenge appeal concerns information classified by your agency, please provide appropriate materials supporting the classification determination that is the subject of 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 William Carpenter or me at (202) 357-5250 and reference ISCAP No. 2013-030.

Sincerely,

JOHN P. FITZPATRICK
Executive Secretary

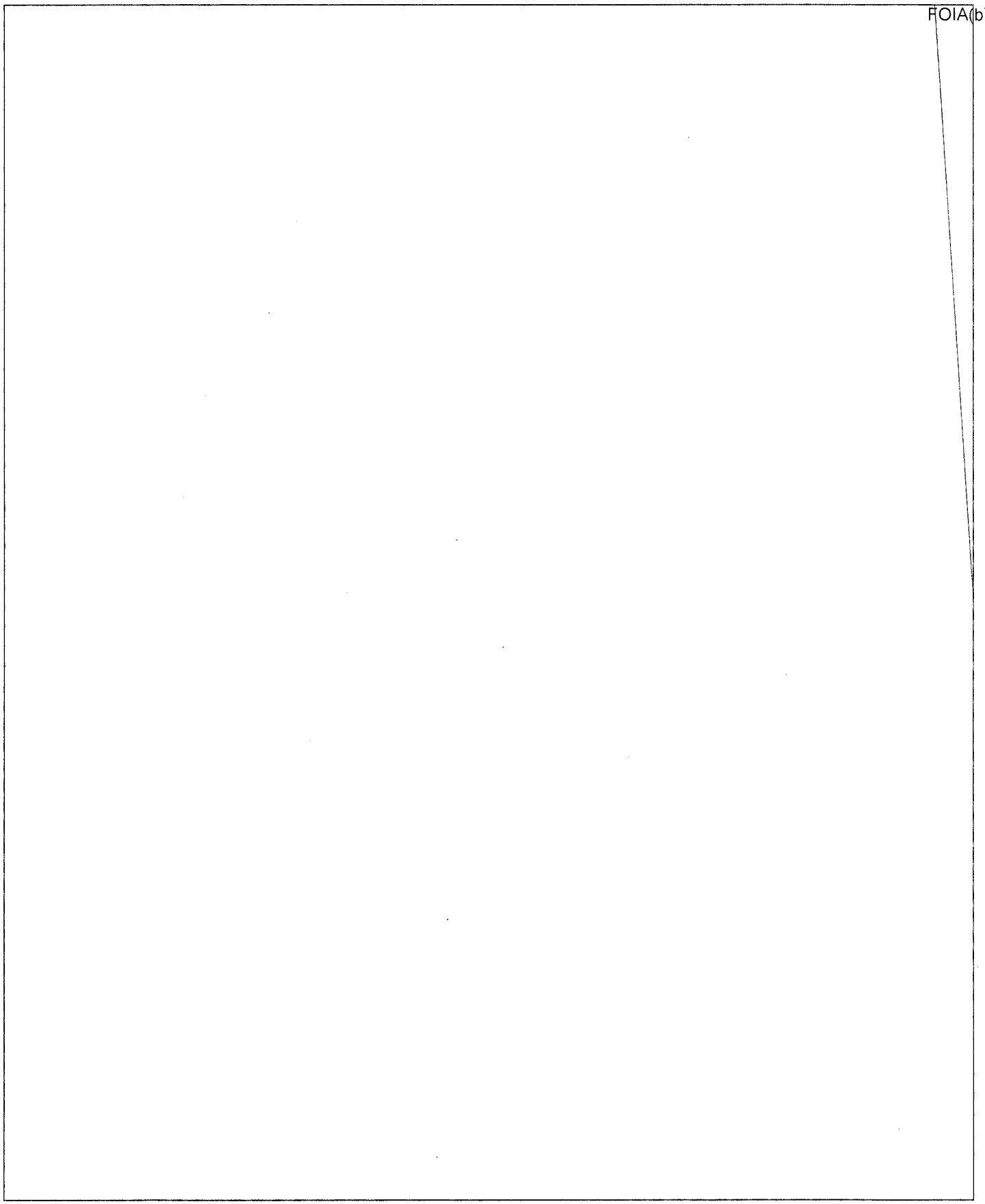
Enclosures

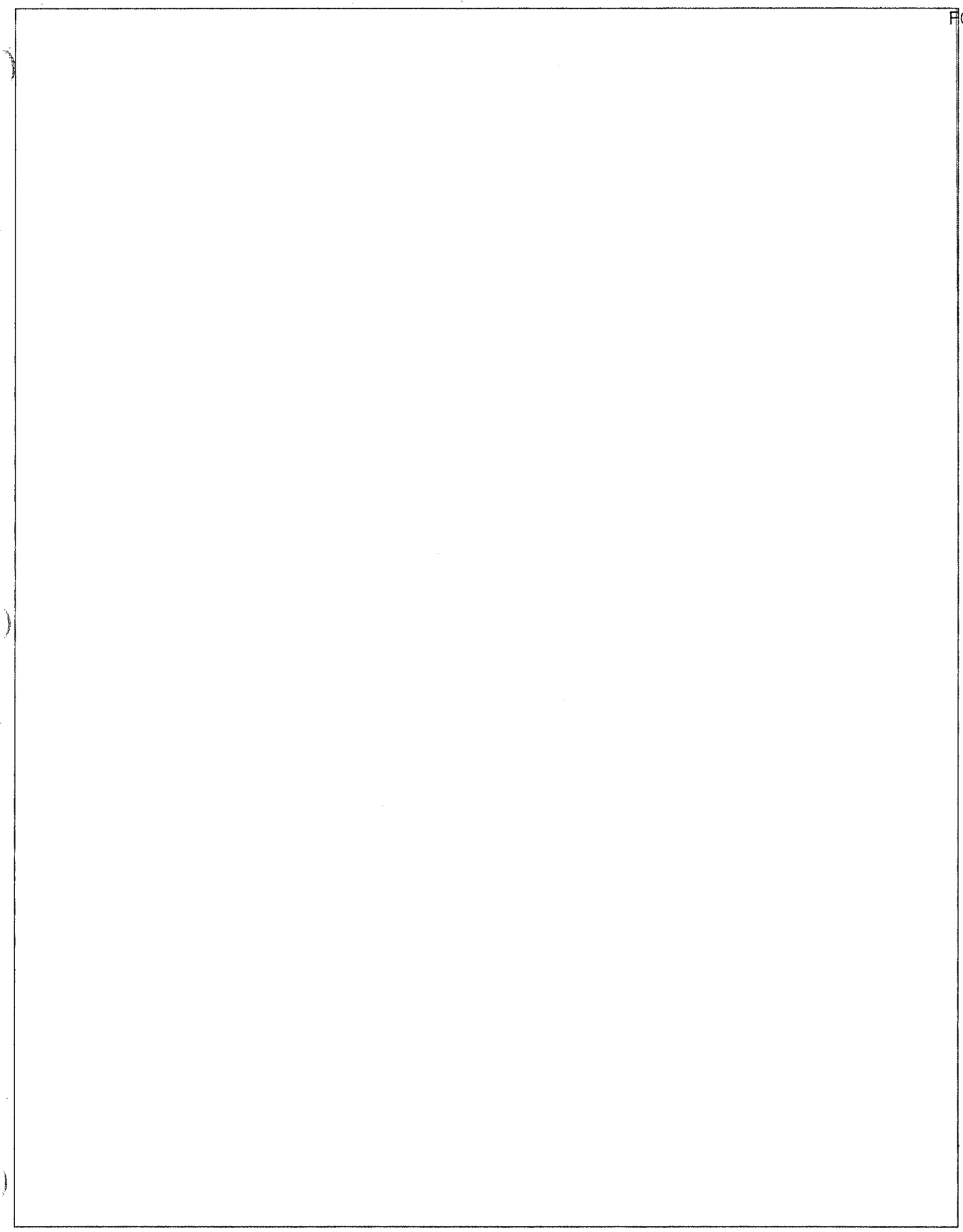
cc: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and FOIA(b)(6)

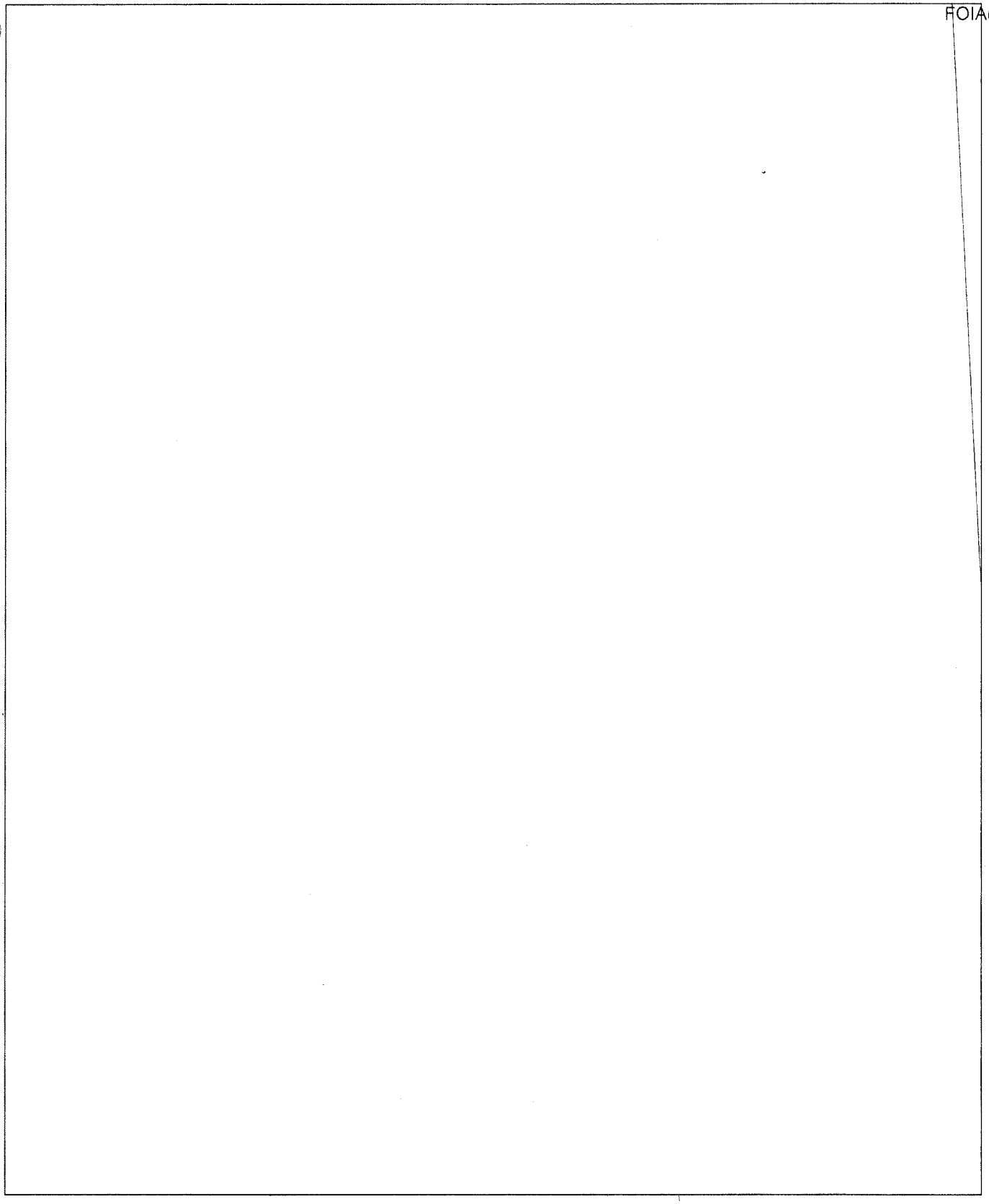
[redacted] Facility Security Officer, FOIA(b)(6)
Applied Research Laboratories, University of Texas at Austin

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

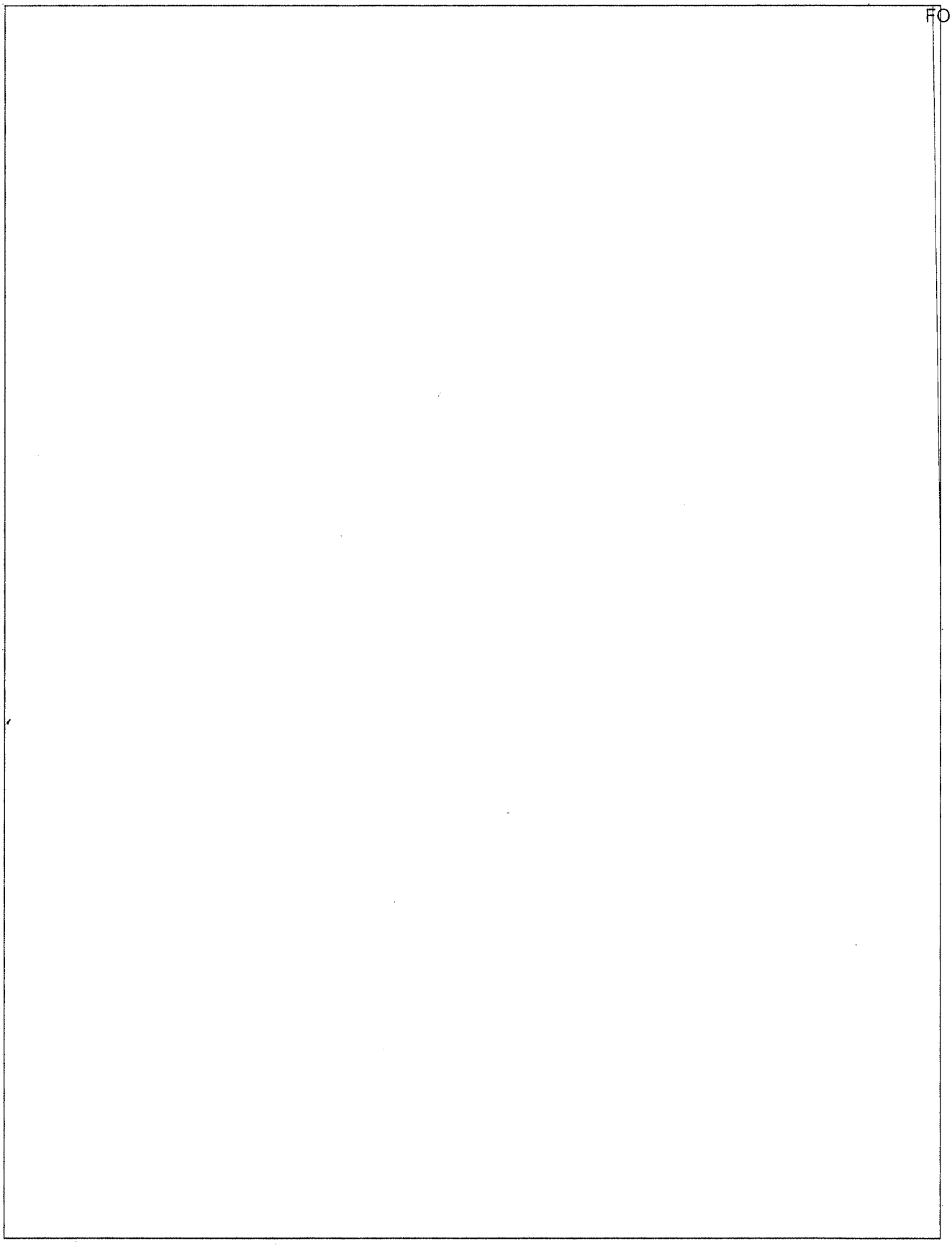
Mr. John F. Hackett, Director, Information Management
Office of the Director of National Intelligence
Liaison to the ISCAP

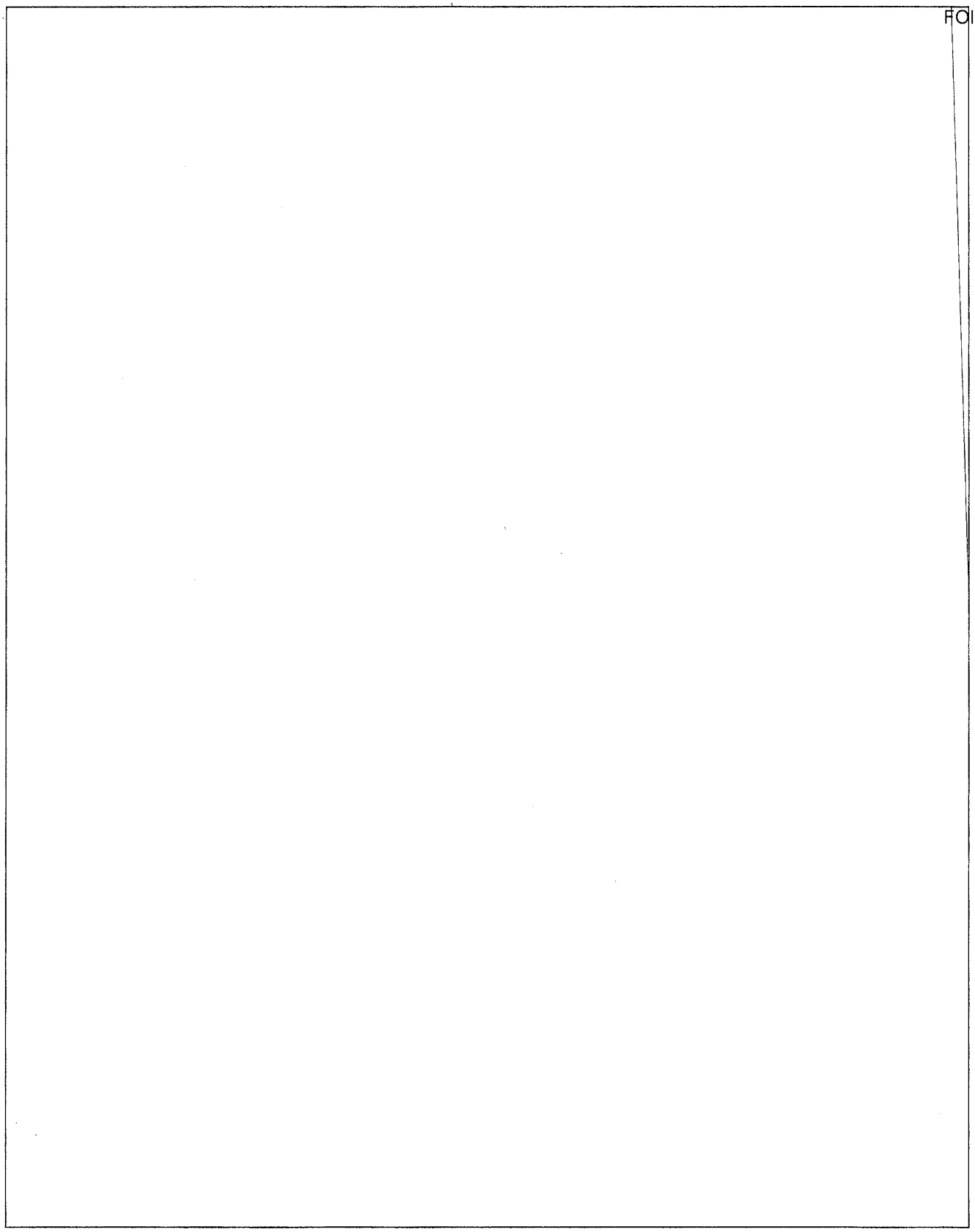



FOIA(b)(4)

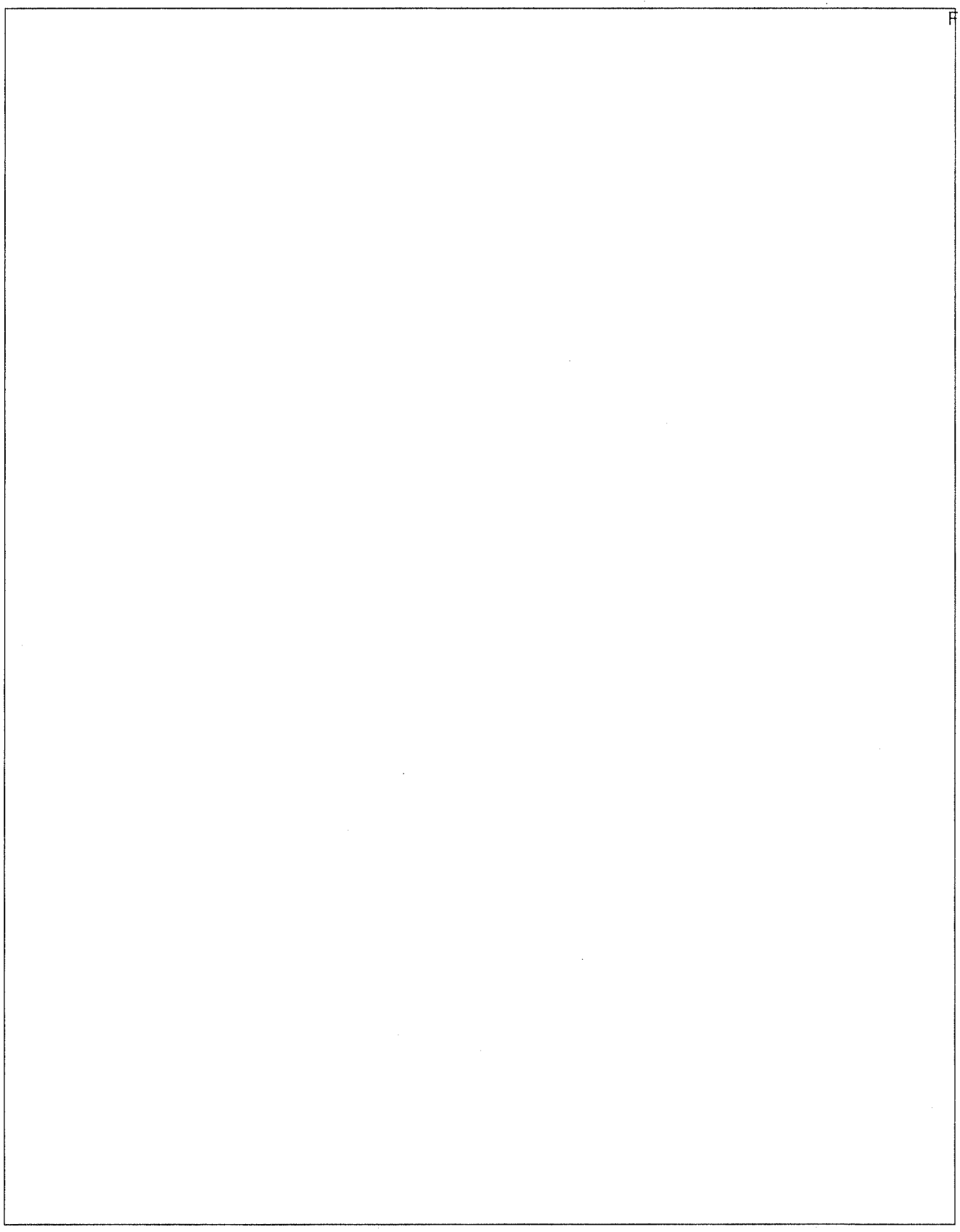


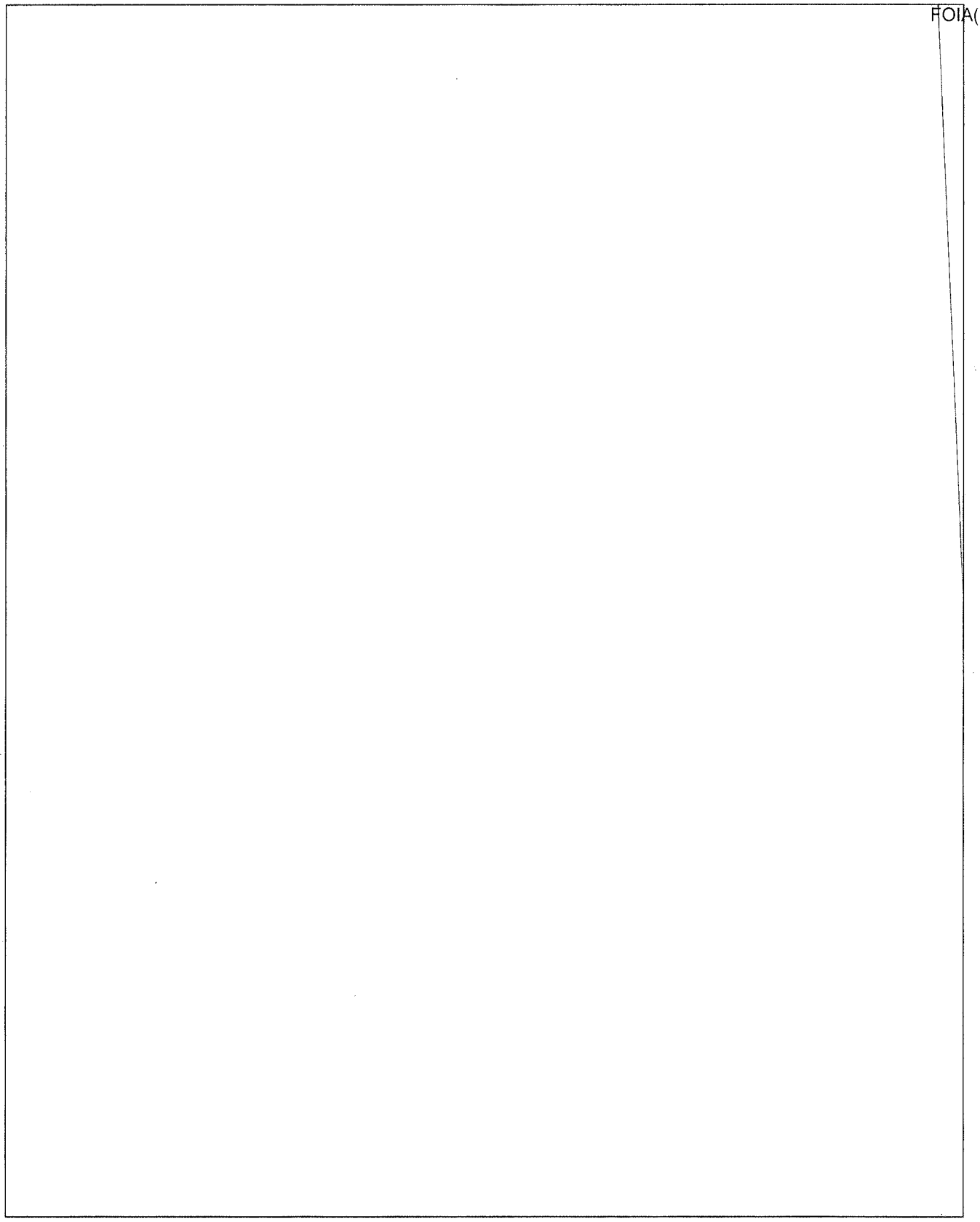
FOIA(b)(4)

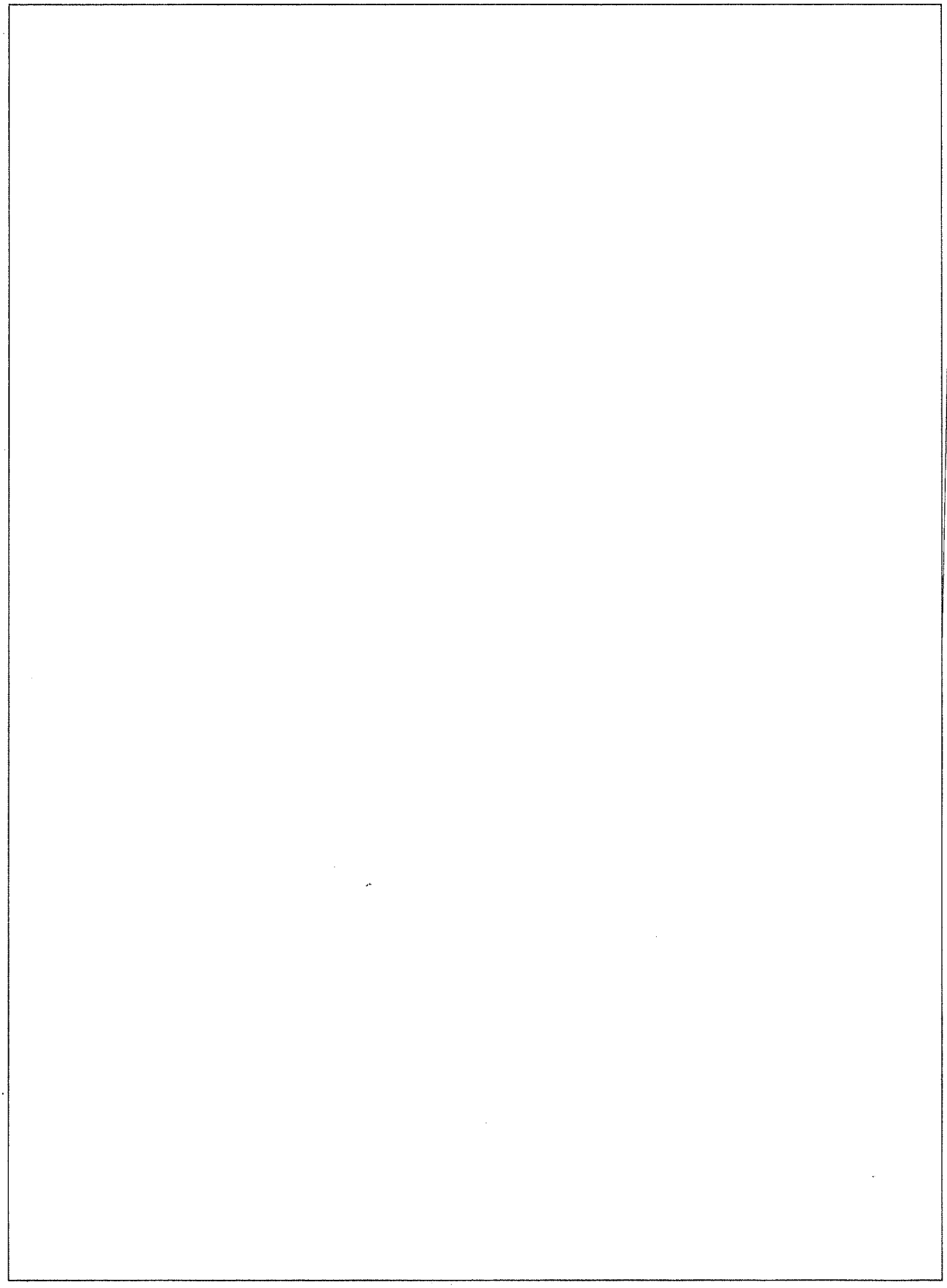



FOIA(b)(4)

FOIA(b)(4)




FOIA(b)(4)



FOIA(b)(4)

INFORMATION TO ACCOMPANY REQUEST FOR
INTELLIGENCE-RELATED CONTRACTING SUPPORT

1.	IRC REQUIREMENTS CHECKLIST (PHOTONICS ESM)	YES	NO
a.	Does the Statement of Work (SOW) and/or contract contain requirements for SCI	X	
b.	Does the SOW accurately describe the efforts to be performed? (Note: If SCI is to be utilized in contract performance, it must be identified in the SOW)	X	
c.	Is the contract product SCI?		X
d.	Does the contract performance require use/storage of SCI at the Contractor's SCIF?		X
e.	Does contract performance require: (1) Substantial access to SCI areas or materials at U.S. Government SCIFs? (Note: Substantial access refers to a contract that requires knowledge of sensitive intelligence collection sources and methods or analytical or operational intelligence capabilities.)		X
	(2) Other than substantial access to SCI areas, information or systems?		X
	(3) Only entry and unescorted access within U.S. Government SCIFs?	X	
f.	Do the Government Contracting Activity (GCA) administrative personnel, in performance of contract award administration and other oversight functions require access to SCI?		X
g.	Does the contracting effort, although non-SCI and non-compartmented, reveal sensitive operations or missions?		X

2.0	CONTRACT INFORMATION
a.	Contractor Name: Applied Research Laboratories, The University of Texas at Austin Contract Number: N00024-07-D-6200 Unclassified Title: FY12 MSN System Performance
b.	SCI Cleared Contracting Officer's Representative (COR) certifying IRC requirements: Name: Activity: Code: Phone: Email:
c.	Contractor Project Manager: Name: Phone: Contractor Special Security Officer: Name: Phone:
d.	Sub-Contractor: N/A Sub-Contractor Project Manager Name: Phone: Sub-Contractor Special Security Officer: Name: Phone: Sub-Contract Number:
e.	Brief description of required service or product: The performance of this task requires coordination with SCI customers of the NGA MSN to ensure the customer requirements are fully met and sustained. Delivery requires access to Government SCIFS.

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

FOIA(b)(6)

FOIA(b)(6)

f.	Justify the need-to-know for each SCI program (e.g., SI/TK, etc.), or sensitive mission revealing information required in support of this contract: SCI/TK/SI/G/HCS is required to physically access the components of the MSN housed at NGA's facility on an as needed basis for the purposes of installation, verification, and test of the deliverable.

3.	PHYSICAL SECURITY		
a.	SCIF Requirements: N/A (1) List all locations where contract work will be performed.		
	(2) Is an accredited contractor SCIF required? If yes, has a fixed facility checklist or concept approval been sent to DIA? If answer to (2) is no, proceed to section 4. AIS Security	YES	NO X
	(3) Is an accredited contractor SCIF presently available for use on this contract? If no, has a pre-construction checklist been submitted to DIA?		
	(4) Is a Co-Utilization Agreement (CUA) required?		
	(5) With what other agency (if known)?		
	(6) Has CUA already been executed? If no, attach a request for a CUA for processing by SSO Navy.		
b.	What categories of SCI/other sensitive material will be used/stored at the contractor's SCIF? (for "other," be specific.) SI_____ TK_____ OTHER_____ NONE__X__		
c.	If a co-utilization of an existing SCIF is required, what is the estimated volume of SCI/other sensitive material to be stored at the contractor's SCIF?		

4.	AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY	YES	NO
a.	Does this contract require development, delivery, support or use of AIS systems and/or networks that will process SCI/other sensitive information?		X
b.	Has the proper authority accredited AIS and/or networks? N/A If yes, by whom: If no, contact SSO Navy for guidance		

5.	ADMINISTRATIVE SECURITY	YES	NO
a.	Does the contractor require access to SCI documents or other sensitive material to support this contract? If yes, list specific SCI documents requiring release to the contractor. Identify specific subject areas of SCI/other sensitive material required.		X
b	Does the contractor require SCI/other manuals, directives indoc tapes, oaths, cover sheets, technical classification guides, etc? If yes, list specific items. SSO Navy will provide these items to the contractor.		X
c	Please identify the total number of billets required to support this effort. SI 6 TK 6 OTHER 6 NONE		

FOIA(b)(6)

Contract Monitor Signature and Date

CONTRACT SPECIAL SECURITY
APPLIED REASEARCH LABS

FOIA(b)(6)

SSO Navy Validation (SSO Navy Use Only)

FOIA(b)(4)

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

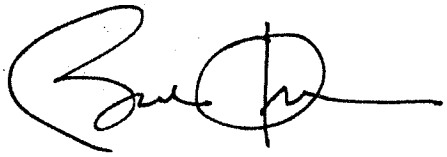
extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(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

CLASSIFIED DOCUMENT ACCOUNTABILITY RECORD	Date March 12, 2013

SECTION I – GENERAL

TO:	FROM:
David K. Daley, ISCAP Liaison Office of Security Review Asst. Branch Chief, Office of Security Review 1155 Defense Pentagon, Room 2A534 Washington, DC 20301-1155	ISCAP Information Security Oversight Office National Archives and Records Administration 700 Pennsylvania Avenue, NW Washington, DC 20408 (202) 357-5466

CONTROL, LOG, OR FILE NUMBER (a)	CLASSIFICATION (b)	NUMBER OF PAGES (c)	DESCRIPTION (Type File Reference, Unclassified Subject or Short Title, and Number of Indorsements/Inclosures) (d)	DATE OF DOCUMENT (e)	ORIGINATOR (f)
----------	S/NOFORN	----------	Briefing Book No. 117	_____	_____

SECTION II - DESTRUCTION CERTIFICATE (*Check appropriate box*)

MATERIAL DESCRIBED HEREON HAS BEEN

☐ DESTROYED ☐TORN IN HALF AND PLACE IN A CLASSIFIED WASTE CONTAINER

OFFICE SYMBOL	DATE	PRINTED NAME OF CUSTODIAN OR REPRESENTATIVE	SIGNATURE
DESTRUCTION RECORD NUMBER	DATE	PRINTED NAME OF CERTIFYING/DESTRUCTION OFFICIAL	SIGNATURE
PAGE OR COPY NUMBER	DATE	PRINTED NAME OF WITNESSING OFFICIAL	SIGNATURE

SECTION III - RECEIPT/TRACER ACTION (*Check appropriate box*)

☐ RECEIPT OF DOCUMENT(S) ACKNOWLEDGED

☐ DOCUMENT(S) HAS (HAVE) NOT BEEN RECEIVED

TRACER ACTION: SIGNED RECEIPT FOR MATERIAL
☐ DESCRIBED ABOVE HAS NOT BEEN RECEIVED

DATE	PRINTED NAME, GRADE OR TITLE	SIGNATURE

COMMENTS (*Use reverse if necessary*)

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Know the Earth... Show the Way... Understand the World

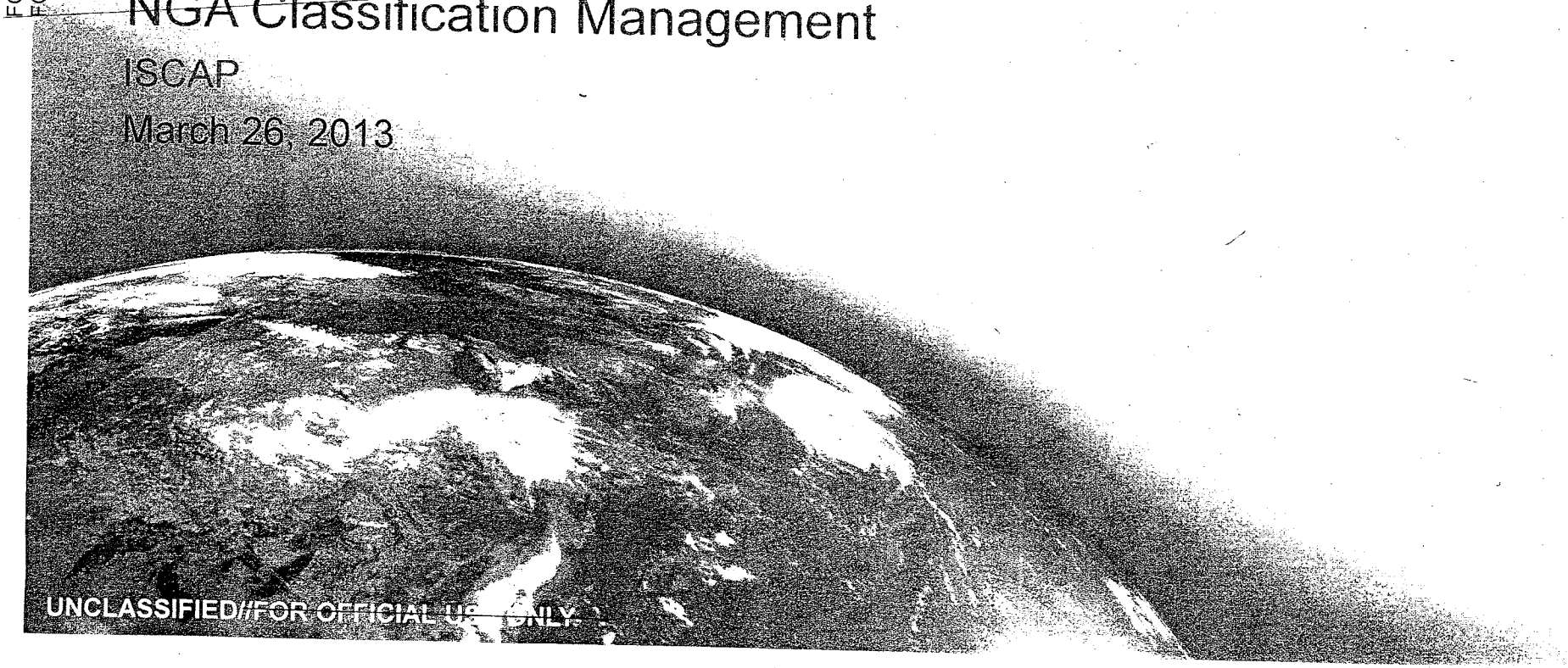
NGA Rebuttal to Classification Challenges

[redacted]

NGA Classification Management

ISCAP

March 26, 2013



Rebuttal to

Classification Challenges

GeoEye

Advanced Research Laboratory – University of Texas

Rebuttal to GeoEye Classification Challenge

NGA reviewed briefings created by GeoEye and using published and Original Classification Authority (OCA) signed classification guidance, determined the briefing is classified. NGA concludes that this appeal is invalid.

Exhibits – Supporting Documentation

- Exhibit A – GeoEye Appeal Letter to ISCAP
- Exhibit B – GeoEye Briefing
- Exhibit C – NGA Security Classification Guide
  (identified in Functional Classification Guidance Review (FCGR)
- Exhibit D – Government Contract Authority (GCA) Email
- Exhibit E - Letter from NGA Contracting Officer Representative (COR)

Exhibit F - GeoEye Statement of Work

Review Sequence of GeoEye Briefing

- NGA Computer Investigations and Awareness Division (CIAD) received GeoEye briefing (Exhibit B) from NGA Chief Information Office (CIO) Designated Accreditation Authority (DAA)

  - Issue: CIO DAA believed a flow diagram (tab) in the briefing was under classified IAW NGA SCG (Exhibit C) Table 1.1, line #17
    - Identifies flow of data between:
      - classified and unclassified domains, and
      - commercial data provider domains (to include satellite operations, connectivity & contingency)
    - Identifies 'High Speed Guard' (HSG) cross domain solution
      - Raytheon (Garland, TX) developed product
      - Approved by the Unified Cross Domain Management Office (UCDMO)
    - Identifies external interfaces to commercial vendors and DISA provided (SIPRNet/NIPRNet) networks
    - Identifies parent-child relationships for the system security plans

GeoEye Classification Challenge

- NGA asserts this appeal is invalid
- Briefing content was determined to be classified in accordance with signed OCA classification guidance
- General cyber concerns across the DoD and IC are addressed as part of NGA's strategy for protecting its systems
  - Guidance for protection is codified in the Security Classification Guide (SCG)
  - The SCG is signed by an OCA
  - The SCG was identified during the FCGR
  - The guidance in the SCG is consistent with the rest of the government
    - Knowledge of specific devices allows targeted research into vulnerabilities which, if successfully exploited, allows access to an entire classified network (Exhibit B, tab)

Rebuttal to GeoEye Classification Challenge

- GeoEye's signed Statement of Work (SOW) (Exhibit F) confirms GeoEye's obligation and commitment to protect information according to the classification levels and dissemination controls assigned in the NGA SCG

- Decision was supported by the GCA (Exhibit D) and COR Letter (Exhibit E)
    - Authorized communication channel for requirements clarification with contractor

- Non compliant with NISPOM
    - Did not follow policies and procedures to challenge the classification decisions
    - Used leverage of the Executive Order over established contractual doctrine (Facility Accreditation/SCIF letters, statement of work)--

Rebuttal to ARL-UT Classification Challenge

NGA reviewed briefings presented by ARL-UT and using published and OCA signed classification guidance.

Exhibits

- Exhibit A – ARL-UT Appeal Letter to ISCAP
- Exhibit B – Notification Letter to NGA from ISCAP
- Exhibit C – IT/IS Migration Briefing
- Exhibit D – Mission Ops Support Briefing
- Exhibit E - DD254

Rebuttal
ARL-UT

- The appeal is invalid because the information was determined to be classified in accordance with signed OCA classification guidance

- General cyber concerns across the DoD and IC are addressed as part of NGA's strategy for protecting its systems
  - Guidance for protection is codified in the SCG
  - The SCG is signed by an OCA
  - The SCG was identified during the FCGR
  - The guidance in the SCG is consistent with the rest of the government
    - Knowledge of outages and schedules allows targeted exploitation of vulnerabilities into the classified network

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

Know the Earth... Show the Way... Understand the World

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Background Information for Rebuttal
ARL - UT

- NGA received 2 ARL-UT briefings (Exhibits C and D) from NGA Computer Investigations Awareness Division (CIAD)

  • Issue: Request by investigations to make a classification determination on briefing that was sent across unclassified network
    - Discussed outages of classified networks
    - Identified DISA as SIPRNET authority
    - Identified a patch schedule for the network

FOIA b(1)

FOIA b(1)

From:
Sent: Wednesday, February 29, 2012 12:00 PM
To:
Subject: CIAD abd ARL contact info

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

Classification: UNCLASSIFIED//~~FOUO~~

==========

is the Project Lead for my system and is one of their ISSOs. He is leading the clean-up effort on the Austin side.

FOIA(b)(6)

is the person we are working with in security. He has offered to help out with specific questions that are beyond my job jacket.

I of course will still remain plugged in with both sides throughout the process.

National Geospatial-Intelligence Agency
ESOG StL
MSNCC System Engineer/Service MAnager
unclassified email
secret email

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

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted]

From: [redacted] FOIA(b)(6)
Sent: Thursday, March 01, 2012 10:20 AM
To: [redacted]
Subject: RE: CIAD abd ARL contact info

Classification: UNCLASSIFIED//~~FOUO~~

[redacted]

I would like to understand the specific reasons the two presentation needed to be deleted. We want to prevent an issue like this in the future and also make sure it is not elsewhere in our documentation. At this point I do not have enough information to do either.

Thanks,

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

From: [redacted]
Sent: Wednesday, February 29, 2012 12:00 PM
To: [redacted]
Subject: CIAD abd ARL contact info

[redacted] s the Project Lead for my system and is one of their ISSOs. He is leading the clean up effort on the Austin side.

[redacted] is the person we are working with in security. He has offered to help out with specific questions that are beyond my job jacket.

I of course will still remain plugged in with both sides throughout the process.

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

[redacted]
National Geospatial-Intelligence Agency
ESOG StL
MSNCC System Engineer/Service MAnager
[redacted]
unclassified email: [redacted]
secret email: [redacted]

Classification: UNCLASSIFIED//~~FOUO~~

ESOG StL
MSNCC System Engineer/Service MAnager
[redacted]
unclassified email: [redacted]
secret email: [redacted]

==========

Classification: UNCLASSIFIED/~~FOUO~~

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

Warning: This document may not be used as a source of derivative classification.
CL By: Unknown
CL Reason: Sec.1.4(g)
DECL ON:
Derived From:
~~SECRET//NOFORN//~~

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Tuesday, April 10, 2012 9:43 AM
To: [redacted]
Cc: [redacted]
Subject: Incident 3325

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

classification:UNCLASSIFIED//~~FOUO~~

[redacted]

Good Morning.

Thank you for your follow-up questions regarding this incident.

To recall our conversation regarding this incident, we talked about vulnerabilities to the systems and how it affects NGA's methodology in protecting its assets. For this reason, the decision remains that the information should be protected at the S//NF level because of the software controls, vulnerabilities associated with specific hosts, and scheduling identified. This is consistent with NGA SCG AIS Table, line item.

Please ensure that you pass this guidance along to [redacted] the Facility Security Officer.

Please let me know if you have additional questions.

[redacted]

UNCLASSIFIED//~~FOUO~~

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Wednesday, April 11, 2012 11:09 AM
To: Richard Mach
Cc: [redacted]
Subject: FW: Incident 3325
Attachments: Incident 3325

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

classification:UNCLASSIFIED//~~FOUO~~
<<Incident 3325>>

[redacted]

I apologize for the delay. I did not realize that you hadn't received it. If you have additional questions, please call to discuss.

[redacted]

From: Postmaster
Sent: Tuesday, April 10, 2012 10:43 AM
To: [redacted]
Subject: Undeliverable: Incident 3325

Delivery has failed to these recipients or distribution lists:

[redacted] FOIA(b)(6)

An error occurred while trying to deliver this message to the recipient's e-mail address. Microsoft Exchange will not try to redeliver this message for you. Please try resending this message, or provide the following diagnostic text to your system administrator.

Diagnostic information for administrators:

Generating server: ncesc-eg1b-5500-tc105.nga.smil.mil

[redacted]

#< #5.0.0 smtp; 510 Invalid Domain Address.> #SMTP#

Original message headers:

Received: from [redacted] by [redacted] with
ESMTP with TLS id 3DVJQN1.359920; Tue, 10 Apr 2012 10:36:23 -0400
Received: from [redacted]
[redacted] by [redacted]
[redacted] with mapi; Tue, 10 Apr 2012 10:43:04 -0400
[redacted]
To: [redacted]
[redacted]
Date: Tue, 10 Apr 2012 10:43:04 -0400
Subject: Incident 3325
Thread-Topic: Incident 3325
Thread-Index: Ac0XJ5bpfT4ae98/T+W4ZGp7Vx9vdA==
Message-ID:
[redacted]
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
[redacted]
acceptlanguage: en-US
MIME-Version: 1.0
Content-Type: text/plain

UNCLASSIFIED//~~FOUO~~

FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
FOIA(b)(6)
FOIA(b)(6)
FOIA(b)(7) - (E)

FOIA(b)(6)

From:
Sent: Friday, April 13, 2012 8:19 AM
To:
Subject: RE: Incident 3325

Classification: UNCLASSIFIED//~~FOUO~~

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

(U) Thank you for the information. I have reviewed what I believe are the referenced sections of the NGA security classification guide and I do not understand how it classifies the information in either of the presentations individually or in aggregate. I will detail my understanding below. I need to understand where my reading of the information is in error or if the ruling should be revised. Please provide specific information on how the guide classifies the presentations so we can determine if we have the same potential aggregation issue/classification issue in other documentation for the project (other than the referenced presentations) as well as understand what specific information we need to classify in the future.

(U) In reading the information you provided in your email, I believe the relevant sections from the NGA security classification guide are:

(U) Table 1.1 Automated Information Systems (AIS)

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

(U) I believe the issue that you noted is that the presentations in aggregate are classified because they identified "the software controls, vulnerabilities associated with specific hosts, and scheduling identified." To me this means you believe that the presentations identified vulnerabilities in specific hosts that could be used to circumvent or negate the security of the host.

(U) In reading the "MSN Ops Support" presentation, it did identify that a past run of the SRR script on the MSN unclassified servers had some reported items there were still in progress or needed for production. The presentation did not identify what specific items were outstanding, if these outstanding items were vulnerabilities that could be used to negate any security controls , or which hosts the vulnerabilities applied to as the results varied on a per host basis.

(U) In reading the "IT/IS Migration" presentation, the presentation contained an incomplete list of MSN servers that were identified by a partial host name (not the fully qualified name of the host). Note that this list did not include the servers located at the monitor stations, the backup MSNCC, the EDL, or the NDL. The list of partial names were noted as "red" or "black" and not a specific classification.

(U) In reading the "MSN Ops Support" presentation, it did identify a patch schedule. Noting the reasoning in the above two paragraphs, this schedule does not add any additional aggregation since neither specific host names nor specific vulnerabilities were discussed. Furthermore, the picture presented by that schedule is incomplete - there are "out of schedule" patches applied as necessary to fix critical vulnerabilities.

(U) With the information from these presentations, I do not understand how one can identify a specific vulnerability associated with a specific host that could be used to circumvent the security of the host.

(U) Thanks for your help.

[redacted]
ARL:UT
[redacted]

FOIA(b)(6)

Classification: UNCLASSIFIED//~~FOUO~~

-----Original Message-----
From: [redacted]
Sent: Tuesday, April 10, 2012 9:43 AM
To: [redacted] FOIA(b)(6)
Cc: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
Subject: Incident 3325 FOIA(b)(6)

classification:UNCLASSIFIED//FOUO

[redacted]

Good Morning.

Thank you for your follow-up questions regarding this incident.

To recall our conversation regarding this incident, we talked about vulnerabilities to the systems and how it affects NGA's methodology in protecting its assets. For this reason, the decision remains that the information should be protected at the S//NF level because of the software controls, vulnerabilities associated with specific hosts, and scheduling identified. This is consistent with NGA SCG AIS Table, line item.

Please ensure that you pass this guidance along to [redacted] the Facility Security Officer.

Please let me know if you have additional questions.

[redacted]

UNCLASSIFIED//~~FOUO~~

FOIA(b)(6)

From:
Sent: Thursday, April 26, 2012 10:24 AM
To:
Cc:
Subject: RE: Incident 3325

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

I sent this message almost two weeks ago and have yet to get a response. I really need specific answers to the questions in the original email (included below) because, looking at the guide, we cannot determine any classified information in the combined or individual briefings. We need to understand the specifics that make it classified so that we can protect it in the future and determine if we have similar information elsewhere in our documentation that would be considered classified. If it is not classified, we need the ruling reversed so we avoid the costly destruction of much equipment at ARL:UT and the expense of replacing and reinstalling all those systems.

Thanks,

-----Original Message-----
From:
Sent: Friday, April 13, 2012 8:19 AM
To:
Subject: RE: Incident 3325

Classification: UNCLASSIFIED//~~FOUO~~

(U) Thank you for the information. I have reviewed what I believe are the referenced sections of the NGA security classification guide and I do not understand how it classifies the information in either of the presentations individually or in aggregate. I will detail my understanding below. I need to understand where my reading of the information is in error or if the ruling should be revised. Please provide specific information on how the guide classifies the presentations so we can determine if we have the same potential aggregation issue/classification issue in other documentation for the project (other than the referenced presentations) as well as understand what specific information we need to classify in the future.

(U) In reading the information you provided in your email, I believe the relevant sections from the NGA security classification guide are:

(U) Table 1.1 Automated Information Systems (AIS)

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

(U//FOUO)

(U) I believe the issue that you noted is that the presentations in aggregate are classified because they identified "the software controls, vulnerabilities associated with specific hosts, and scheduling identified." To me this means you believe that the presentations identified vulnerabilities in specific hosts that could be used to circumvent or negate the security of the host.

(U) In reading the "MSN Ops Support" presentation, it did identify that a past run of the SRR script on the MSN unclassified servers had some reported items there were still in progress or needed for production. The presentation did not identify what specific items were outstanding, if these outstanding items were vulnerabilities that could be used to negate any security controls , or which hosts the vulnerabilities applied to as the results varied on a per host basis.

(U) In reading the "IT/IS Migration" presentation, the presentation contained an incomplete list of MSN servers that were identified by a partial host name (not the fully qualified name of the host). Note that this list did not include the servers located at the monitor stations, the backup MSNCC, the EDL, or the NDL. The list of partial names were noted as "red" or "black" and not a specific classification.

(U) In reading the "MSN Ops Support" presentation, it did identify a patch schedule. Noting the reasoning in the above two paragraphs, this schedule does not add any additional aggregation since neither specific host names nor specific vulnerabilities were discussed. Furthermore, the picture presented by that schedule is incomplete - there are "out of schedule" patches applied as necessary to fix critical vulnerabilities.

(U) With the information from these presentations, I do not understand how one can identify a specific vulnerability associated with a specific host that could be used to circumvent the security of the host.

(U) Thanks for your help.

ARL:UT

FOIA(b)(6)

Classification: UNCLASSIFIED//~~FOUO~~

-----Original Message-----
From:
Sent: Tuesday, April 10, 2012 9:43 AM
To:
Cc:
Subject: Incident 3325

FOIA(b)(6)

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

classification:UNCLASSIFIED//~~FOUO~~

Good Morning.

Thank you for your follow-up questions regarding this incident.

To recall our conversation regarding this incident, we talked about vulnerabilities to the systems and how it affects NGA's methodology in protecting its assets. For this reason, the decision remains that the information should be

protected at the S//NF level because of the software controls, vulnerabilities associated with specific hosts, and scheduling identified. This is consistent with NGA SCG AIS Table, line item.

Please ensure that you pass this guidance along to [redacted] ~~the Facility Security Officer~~. FOIA(b)(6)

Please let me know if you have additional questions.

[redacted]

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

UNCLASSIFIED/~~FOUO~~

FOIA(b)(6)

From: [redacted]
Sent: Friday, December 14, 2012 3:01 PM
To: 'ISCAP@nara.gov'
Subject: Challenge to Classification
Attachments: FW: Challenge to Classification Request for ISCAP (12.9 KB); Security Incident Report.pdf
Signed By: [redacted]

Executive Secretary
ISCAAP
Classification Challenge Appeals

Paragraph 4-104 of the NISPOM provides guidance for "Challenges to Classification" should the contractor believe information is classified improperly or unnecessarily. Accordingly, Applied Research Laboratories at the University of Texas (ARL:UT) seeks to challenge the National Geospatial Intelligence Agency's (NGA) determination that the information contained in unclassified presentations prepared by ARL:UT employees for the Program and Technical Review (PMTR) on 25 January 2012 is classified.

Attached you will find a copy of ARL:UT's Final Report regarding security violation "55354-20120228-C1" submitted to the Defense Security Service (DSS) San Antonio Field Office in June of 2012. In that report, ARL:UT challenged NGA's classification determination. A copy of the report was provided to NGA requesting clarification of why the information in question was considered classified. To date, NGA has not provided a response to our inquiry. IAW NISPOM 4-104, paragraph 6 of the final report requested that the CSA (DSS) provide assistance in obtaining a satisfactory response; to date, DSS has not provided a response to our inquiry or request for assistance/determination. Therefore, IAW NISPOM 4-104, absent a response from the NGA or the CSA (DSS), this challenge is being forwarded to the ISCAP for resolution.

Copies of the slides in question and NGA classification guides are available upon request. We are seeking a detailed and specific explanation of why the information contained in the slide presentations, when aggregated, is considered classified. The ARL:UT Principal Investigator (PI) working on the program cannot determine from the classification guidance why the information contained in the slides is considered by NGA to be classified. It is critical to ARL:UT and in the best interest of the government that a determination be made and an explanation provided; we are still using the same classification guides and do not want to make the same mistake again, if in-fact it was a mistake to begin with.

As the Facility Security Officer (FSO) I serve as the ARL:UT POC for this matter. If you require additional information, need any clarification or have any questions please contact me. Your assistance in is greatly appreciated.

[redacted]
Facility Security Officer
The University of Texas System/
The University of Texas at Austin
Applied Research Laboratories
[redacted]

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Friday, July 13, 2012 5:22 PM
To: [redacted]
Cc:
Subject: Re: ACTION REQUIRED from the January 2012 MSN PMTR at Austin
Signed By: [redacted]

[redacted]

Here are the organizations and the addresses as far as I'm aware. I broke out the original email into each organization. I don't have full address for some but may able to get them from other next week. I almost am not sure which organization one of them is part of, namely:

[redacted] FOIA(b)(6)

[redacted]

National Geospatial-Intelligence Agency
Fort Belvoir, VA

[redacted]

National Geospatial-Intelligence Agency
3838 Vogel Road
Arnold, MO 63010-6238

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

[redacted]

[redacted]

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

USAF/SMC/GP
483 North Aviation Blvd.
El Segundo, CA 90245

FOIA(b)(6)

[redacted]

USAF/SMC
1050 E. Stewart Ave.
Bldg. 2025
Peterson AFB, CO 80914

[redacted]

NGA/USAF
2nd Space Operations Squadron
300 O'Malley Ave., Suite-41
Schriever AFB, CO 80912-3041

[redacted]

Aerospace
El Segundo, CA

[redacted]

FOIA(b)(6)

Aerospace
Colorado Spring, CO

[redacted]

Naval Surface Warfare Center

17214 Ave B
Suite 122
Dahlgren, VA 22448

[redacted] FOIA(b)(6)

ARL:UT
10000 Burnet Rd.
Austin, TX 78758

[redacted] FOIA(b)(6)

MSN Team <msn_team@arlut.utexas.edu> -- about 30+ people see entry in Ganymede

[redacted]

On 7/13/2012 3:33 PM [redacted] wrote:

[redacted]

I cannot tell from your email what facilities the folks are from. Please separate out the names of the folks you emailed and provide for each of them their telephone number, the organization the belong to with the location and address of the organization. I need the location and address of the organization in order to determine the CAGE Code. If I cannot determine the CAGE Code I will have to call the individuals. You can see from [redacted] email that this is not my requirement but hers...

Thanks

[redacted]

From: [redacted]
Sent: Friday, July 13, 2012 2:10 PM
To: [redacted]
Cc: [redacted]
Subject: Re: ACTION REQUIRED from the January 2012 MSN PMTR at Austin

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

National Geospatial-Intelligence Agency

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

3838 Vogel Road
Arnold, MO 63010-6238

[redacted]

On 7/13/2012 1:40 PM, [redacted] wrote:

To clarify, I didn't notify people of a spill. The information was that there was the potential to create a spill and to delete these presentations to remove the potential.

I do not know CAGE codes and appropriate security POCs for these organizations. The best I can provide is the list of people and organizations to which we emailed the link (which you can see in the email below). I'm also in the process of determining who we mailed copies to as well. Do I need to contact each person and ask for a CAGE code and a security POC? Is there a way the security office at ARL can lookup that type information?

[redacted]

On 7/13/2012 12:45 PM [redacted] wrote:

[redacted]

I would like for you to answer the question; not me since you are the one who notified the folks that there was a spill. Please provide one or two short paragraphs delineating what organizations were notified and if they were contractor organizations, their CAGE Code as well as a POC for each organization. If they were just government organizations then the organization name and POC is all.

Thanks

[redacted]

From: [redacted]
Sent: Friday, July 13, 2012 9:51 AM
To: [redacted]
Cc: [redacted]

(b)(6)

FOIA(b)(6)

From:
Sent: Friday, July 13, 2012 9:51 AM
To:
Cc:
Subject: Fwd: ACTION REQUIRED from the January 2012 MSN PMTR at Austin
Signed By:

You can see in the To and CC below the list of people/organizations that the original link was sent to and this is the same list that the delete instructions were sent to in the email below.

Does that sufficiently allow you to answer the question you posed this morning?

-------- Original Message --------
Subject: ACTION REQUIRED from the January 2012 MSN PMTR at Austin
Date: Wed, 29 Feb 2012 12:42:11 -0600
From:
To

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

CC

FOIA(b)(6)

NGA has requested that the following unclassified presentations be deleted if you have electronic copies or destroyed if you have hard copies.

- Presentation #6 titled "IT/IS Migration" by [redacted] File name 06-ITIS-MigrationV2.pdf FOIA(b)(6)
- Presentation #10 titled "MSN OPS Support" by [redacted] File name 10-Jan2011-Ops Support-final.pdf

Please contact me or [redacted] with any questions.

Thanks,

[redacted]

On 1/19/2012 3:12 PM, [redacted] wrote:
We have just posted the read ahead material for the meeting next week Wednesday and Thursday (Jan 25 - 26). The only presentations that are missing are for a couple of the side sessions on Thursday (note, not all side sessions have material). You can download the presentation information in a zip file called MSN_PMTR_2012_Jan.zip located at:

https://ftp.arlut.utexas.edu/arl_web_ftp/ftp/ftproot/priv/SGL/bqstaging/January2012PMTR

I will send the password and username in the next email.

Dial in information will be available for the meeting and is as follows:

Call 512-873-5432.
Conference number is 3644#.
Passcode is 44121#

We will attempt to host a web meeting as well but this may or may not happen due to recent issues with the web meeting server. If we are successful, the address for the web meeting is:

https://meeting.arlut.utexas.edu/msnpmtr/

Lunch will be provided each day to facilitate the flow of the meeting.

Please let me know if you have any questions. We are looking forward to the discussion next week.

[redacted]

On 1/10/2012 5:49 PM, [redacted] wrote:

Based on some feedback, I have several updates I want to distribute. The updated agenda is attached. Changes from the previous are:

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

1. Additional talk by [redacted]
2. Several new side sessions resulting in a new end time on Thursday, 26 Jan of 1400. (Note that the ordering of side sessions has not been set and will be varied based on interest and travel schedules of participants.)
3. Due to the number of participates, the main PMTR session (25 Jan) will be held in the main auditorium just behind the ARL lobby.

I will be emailing out a link to the electronic copy of the meeting next week, along with dial in information. I

also plan on mailing hard copies of the presentation. If you are interested in a hard copy to support remote participation, please email me the number of copies and an address to send to.

[redacted] FOIA(b)(6)

On 1/3/2012 5:04 PM, [redacted] wrote:

As of today, I have the following people who have noted they will or may come (see end of email). If there are others, please let me know this week. You can find information about visiting ARL at:

http://www.arlut.utexas.edu/visiting/index.html

and information about submitting a clearance at:

http://www.arlut.utexas.edu/visiting/entry.html

While most of the meeting will be held at the unclassified level, we may have certain sessions or discussion at the SECRET level.

[redacted]

NGA:

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

NSWC:

[redacted] FOIA(b)(6)

USAF:

[redacted] FOIA(b)(6)

On 12/14/2011 3:56 PM, [redacted] wrote:

The agenda for the MSN portion (on the 25th and 26th of January) is attached. Two requests:

1. If you plan on attending in person, please let me know by Friday, 6 January 2012. This is needed so I can plan for food and ensure security paperwork is in place for the visit.

I believe I have incorporated all the suggestions for agenda/side session topics. If you have any comments/additions/changes, please let me know in the next few days so I can work them into the agenda.

All,

We've settled on dates for the next program management and technical review of NGA tasks in progress at ARL:UT and NSWC.

These meetings will be in Austin, TX.

January 24, 2012 (Tuesday) - NSWC PMTR & side sessions (full day)
January 25th, 2012 (Wednesday) - ARL MSN PMTR (full day)
January 26th, 2012 (Thursday) - ARL MSN side sessions (partial day)

I will send out a draft for the MSN portion next week. Please let me know now if you have any topic or side meeting suggestions.

FOIA(b)(6)

From:
Sent: Thursday, July 05, 2012 1:39 PM
To: FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
Subject: ISCAP appeal
Signed By: FOIA(b)(6)

Good afternoon. After reading the final report and subsequent conversation with I understand ARL:UT has appealed the classification determination rendered by NGA Classification Management. Until ISCAP reviews the classification determination and provides a final decision, NGA CIAD will not be able to complete the final investigation report. I've requested keep me informed of the final disposition provided by ISCAP once they have come to a decision. If you could also let me know when you hear something and what the final outcome is, I would appreciate it. I have also informed of ARL:UT's appeal to ISCAP. If you have any questions, please don't hesitate to contact me.

r/

FOIA(b)(6)

From:
Sent: Wednesday, June 27, 2012 10:36 AM
To:
Cc:
Subject: ARL Security Violation 55354-20120531-C1
Attachments: Security Incident Report.pdf

Importance: High

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

Here is the final report as requested which has been sent to our DSS office this morning. At this point we still have not received anything specific from NGA classification management that provides us the details of exactly what information was classified when aggregated regarding the two presentations. We do not agree with NGA's classification determination and are asking for DSS's assistance to challenge the ruling via the ISCAP (Interagency Security Classification Appeals Panel) through the ISOO per NISPOM 4-104. If you have any questions regarding the report please contact the FSO Thanks.

Information Systems Security Manager
Applied Research Laboratories
University of Texas at Austin

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Friday, June 01, 2012 11:15 AM FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)
To: [redacted]
Cc: [redacted]

Subject: NGA Classification Ruling

[redacted] FOIA(b)(6)

Can you please forward me the email that [redacted] sent you about the final classification ruling that we discussed yesterday, I checked my SIPRNET email [redacted] a few minutes ago and didn't have anything from you.

ARL will also need specific details about the classification ruling that was made by NGA [redacted]. ARL had challenged the ruling because we reviewed the SCG and found nothing classified in these presentations after numerous internal reviews. That being said we need to know specifically what exactly is classified in these presentations and the appropriate section of the SCG being cited as to the ruling. Thanks for your assistance in this matter.

[redacted]
Information Systems Security Manager
Applied Research Laboratories
University of Texas at Austin
[redacted]

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Thursday, May 31, 2012 4:25 PM
To: [redacted]
Cc: [redacted]

Subject: Security Incident
Attachments: ISFO Process Manual V3 14 June 2011.pdf

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

[redacted]

Per our phone conversation a few minutes ago here is a summary of actions that we have taken in response to this incident.

When these unclassified presentations had an aggregation concern back in February, the guidance given by NGA [redacted] was to delete these presentations from all computers and destroy all hard copies. The files were removed from the ARL/SGL File Server, ARL FTP site, ARL laptop, ARL email server, and other computers that sync the ARL/SGL file server. All hard copies were destroyed with the exception of one hard copy which is currently kept in a GSA approved safe located in a closed area and was being kept until a final classification ruling had been made. Backup tape catalogs was deleted and put back into rotation where it would be overwritten on its next use.

When a classified spillage occurs our ARL procedures are to either follow the direction and/or guidance of the sponsor/data owner or complete the DSS Approved Sanitization Procedures (Page 91- 110) attached above. Considering the circumstances and events surrounding this incident over the past 4 months and having already deleted the files from all affected computers and tapes in accordance with NGA direction, if ARL were to proceed with completing the DSS procedures now after having deleted all files, our only option would be to destroy all associated drives which would cost ARL a significant amount of money and manpower. As a result I believe that our actions that have already been completed were sufficient and requests this incident be closed out.

Thanks,

[redacted]
Information Systems Security Manager
Applied Research Laboratories
University of Texas at Austin
[redacted]

Defense Security Service
Mobile Phone: [redacted] FOIA(b)(6)

-----Original Message-----
From: [redacted] FOIA(b)(6)
Sent: Wednesday, June 27, 2012 9:45 AM
To: [redacted]
Cc: [redacted]
Subject: 2ARL Security Violation 55354-20120531-C1_rgm.docx

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

Attached is a Final Report of an alleged security violation that occurred at ARL back in February. We have been trying (without success) to get specific information regarding the determination that unclassified information was "aggregated" and that the aggregation resulted in a security violation. I do not agree with NGA's determination; not the fact that aggregated unclassified information may be considered classified but the fact that the information contained on the two slide can be considered aggregated . You will see in my report that I am asking DSS to obtain that information from NGA. If you have any questions regarding the report or require additional information please let me know.

Thank you.

[redacted]

FOIA(b)(6)

From:
Sent: Monday, June 25, 2012 9:25 AM
To:
Subject: FW: Presentation written by [redacted] for January 2012 PMTR.
Signed By:

[redacted] statement..

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, June 25, 2012 9:24 AM
To: [redacted]
Subject: Presentation written by [redacted] for January 2012 PMTR.

During January 2012 I prepared a presentation titled "MSN OPS Support" for the January 2012 NGA MSN Program Management & Technical Review (PMTR) held in Austin, Texas. The presentation discussed operations support activities provided by ARL for MSN. Topics discussed were system administration support, software patching, security compliance and support desk activities.

This presentation was written by me and reviewed by [redacted] and [redacted] prior to the PMTR. Once the presentation was completed, [redacted] stored it electronically.

--
[redacted]
APPLIED RESEARCH LABORATORIES
THE UNIVERSITY OF TEXAS AT AUSTIN
[redacted]

FOIA(b)(6)

From:
Sent: Friday, June 22, 2012 11:22 AM
To:
Subject: FW: PMTR Presentation of Feb 2012
Signed By:

FYI...

-----Original Message-----
From:
Sent: Friday, June 22, 2012 10:56 AM
To:
Cc:
Subject: PMTR Presentation of Feb 2012

Hi
Back in February of this year I created a presentation called "IT/IS Migration" for our PMTR meeting. This presentation was created solely by me. The purpose of this presentation was to give an overview of what it will take to migrate our Solaris environment to a virtual environment. The presentation listed things such as goals for migration, a schedule of the servers that will be migrated, and other pertinent information such as action items and funding. There was no specific details in my presentation that can be considered classified.

After I created a presentation, I have the tendency of sending it out to a couple of people for review. This presentation was sent to two managers and one of them happens to be our ISSO for the department and neither one of them saw anything classified on this document. If any changes need to be made, I make the modifications and send it back for a final review. Once it gets final approval, its then put online in a folder where only specific people can view them. My presentation was 1 out of 19 presentations in that folder for February.

Please let me know if you need any further information or clarification regarding this presentation.
regards,

FOIA(b)(6)

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

From:
Sent: Friday, June 15, 2012 10:13 AM
To:
Cc:
Subject: Security incident
Signed By:

I've left several voicemails not realizing you were TDY. I wanted to make sure you received the information you requested during our last conversation on 31 May 2012 and also inform you I have not received the information I requested during that same conversation. The email I sent contains the final decision from on your request to have the information in question re-evaluated. With the final determination rendered, please proceed according to ARL-UT policies and procedures concerning an event of this type. I also request a copy of the final report as I will need to include it in my report. Please let me know if you have any questions.

r/

b)(6)

From:
Sent: Tuesday, May 08, 2012 10:42 PM
To:
Cc:
Subject: Re: Security Violation (Classified Spillage)

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

The summary of the situation is that we have gotten conflicting information from NGA and have not received information from NGA regarding what (if anything) is classified. Without that information, we cannot be sure we actually sanitize any systems. The following paragraphs detail what we know and what has happened to date.

At the end of February (27th or 28th), I received information about an "incident" from NGA that occurred at a program and technical review (PMTR) that happened on Jan 25th. The information I received from NGA in discussions with and was that the NGA security office determined that if two of the presentation from the PMTR were aggregated, the aggregation would contain classified information. They did say that individually each presentation was unclassified. provided verbal direction on the actions we were to take and provided it in writing in a SIPRnet email on 2/29. The instructions were to delete soft copies of the presentation, destroy hard copies, overwrite the index of backup tapes but keep them in the rotation, delete emails (from all folders including trash), and inform external organizations that got copies of the presentations to destroy/delete them as well. We completed the actions by 2/29.

On 3/19, I saw a SIPRNet email from of NGA asking for a report about the incident and indicated it was classified. This was the first time we heard that it was actually classified instead of having the potential to be classified if aggregated. I asked for clarification about what was classified and he referred me to and noted the incident number is 3325. After several attempts on the phone, I was finally able to reach on either the 6th or 9th of April. I received an email on April 10th that provided a couple of sentences that stated the information was SECRET/NF and provided the general category of information. She did not indicate if this was in aggregate or in a single presentation.

I reviewed the information provided and compared it to the NGA security classification guide and the copies of the two presentations. (We retained one hardcopy of each presentation we have marked as classified.) In examining the presentations, I did not find and of the information she referenced in the email that was classified. This review was also done by and later by They both agreed that the referenced information was not in either presentation or in aggregate. On April 13th, I sent an email referencing the relevant sections of the NGA SCG, explained that none of the presentations contained the listed information, listed the information the presentation did contain, and asked her to describe what was classified based on the SCG or to reverse the ruling.

Since that email, we have not received a response. I did talk to her on April 13th and told her I sent her this email. I have left several voice mails for her but have yet to get a call back or email clarification on the ruling. Messages were left during the week of April 16th and April 23th I believe. Also during the week of April 23rd, I asked our sponsors to see if they could get a response from

did talk to on April 26th about the incident and said that she could not provide answers to questions about the classification that Joe believes she should be able to answer as a classifier. At this point requested information from NGA regarding who is the supervisor in this office to see if contacting them would help bring closure to the situation. contacted on May 3rd about this issue. has also tried to contact her by phone but with no success.

Subject: Fwd: ACTION REQUIRED from the January 2012 MSN PMTR at Austin

You can see in the To and CC below the list of people/organizations that the original link was sent to and this is the same list that the delete instructions were sent to in the email below.

Does that sufficiently allow you to answer the question you posed this morning?

[redacted]

-------- Original Message --------

Subject: ACTION REQUIRED from the January 2012 MSN PMTR at Austin

Date: Wed, 29 Feb 2012 12:42:11 -0600

From: [redacted]

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

CC: FOIA(b)(6)

[redacted]

NGA has requested that the following unclassified presentations be deleted if you have electronic copies or destroyed if you have hard copies.

- Presentation #6 titled "IT/IS Migration" by [redacted] File name 06-ITIS-MigrationV2.pdf
- Presentation #10 titled "MSN OPS Support" by [redacted] File name 10-Jan2011-Ops Support-final.pdf

Please contact me or [redacted] with any questions.

Thanks,

[redacted]

On 1/19/2012 3:12 PM, [redacted] wrote:
We have just posted the read ahead material for the meeting next week Wednesday and Thursday (Jan 25 -26). The only presentations that are missing are for a couple of the side sessions on Thursday (note, not all side sessions have material). You can download the presentation information in a zip file called MSN_PMTR_2012_Jan.zip located at:

https://ftp.arlut.utexas.edu/arl_web_ftp/ftp/ftproot/priv/SGL/bqstaging/January2012PMTR

I will send the password and username in the next email.

Dial in information will be available for the meeting and is as follows:

Call 512-873-5432.
Conference number is 3644#
Passcode is 44121#

We will attempt to host a web meeting as well but this may or may not happen due to recent issues with the web meeting server. If we are successful, the address for the web meeting is:

https://meeting.arlut.utexas.edu/msnpmtr/

Lunch will be provided each day to facilitate the flow of the meeting.

Please let me know if you have any questions. We are looking forward to the discussion next week.

[redacted]

On 1/10/2012 5:49 PM, [redacted] wrote:

FOIA(b)(6)

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

Based on some feedback, I have several updates I want to distribute. The updated agenda is attached. Changes from the previous are:

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

1. Additional talk by [redacted]
2. Several new side sessions resulting in a new end time on Thursday, 26 Jan of 1400. (Note that the ordering of side sessions has not been set and will be varied based on interest and travel schedules of participants.)
3. Due to the number of participates, the main PMTR session (25 Jan) will be held in the main auditorium just behind the ARL lobby.

I will be emailing out a link to the electronic copy of the meeting next week, along with dial in information. I also plan on mailing hard copies of the presentation. If you are interested in a hard copy to support remote participation, please email me the number of copies and an address to send to.

[redacted] FOIA(b)(6)

On 1/3/2012 5:04 PM, Rick Mach wrote:

As of today, I have the following people who have noted they will or may come (see end of email). If there are others, please let me know this week. You can find information about visiting ARL at:

http://www.arlut.utexas.edu/visiting/index.html

and information about submitting a clearance at:

http://www.arlut.utexas.edu/visiting/entry.html

While most of the meeting will be held at the unclassified level, we may have certain sessions or discussion at the SECRET level.

[redacted]

NGA:

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

NSWC: [redacted] FOIA(b)(6)

USAF: [redacted] FOIA(b)(6)

On 12/14/2011 3:56 PM, [redacted] wrote:

The agenda for the MSN portion (on the 25th and 26th of January) is attached. Two requests:

1. If you plan on attending in person, please let me know by Friday, 6 January 2012. This is needed so I can plan for food and ensure security paperwork is in place for the visit.

2. I believe I have incorporated all the suggestions for agenda/side session topics. If you have any comments/additions/changes, please let me know in the next few days so I can work them into the agenda.

[redacted] FOIA(b)(6)

All,

We've settled on dates for the next program management and technical review of NGA tasks in progress at ARL:UT and NSWC.

These meetings will be in Austin, TX.

January 24, 2012 (Tuesday) - NSWC PMTR & side sessions (full day)
January 25th, 2012 (Wednesday) - ARL MSN

PMTR (full day)
January 26th, 2012 (Thursday) - ARL MSN side sessions (partial day)

I will send out a draft for the MSN portion next week. Please let me know now if you have any topic or side meeting suggestions.

[redacted] FOIA(b)(6)

FOIA(b)(6)

From:
Sent: Friday, July 13, 2012 5:32 PM
To:
Cc:
Subject: Re: FW: ACTION REQUIRED from the January 2012 MSN PMTR at Austin
Signed By:

I was instructed by NGA to not bring attention to the fact of a potential aggrigation issue when passing it along and definitely not that it was actually classified. If the question came up I was just to note that the information was "sensitive".

On 7/13/2012 3:17 PM, Neil Fox wrote:

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

In your email of Thu 7/12/2012 11:29 AM you requested:

"Please provide additional information regarding security violation no. 55354-20120531-C1. You mentioned in your report that on 2/29/2012 contacted the external organizations that got copies of the two presentations that when aggregated became classified to notify those organizations of the need to destroy/delete per the instructions that had provided to I need to know what organizations were notified. If contractor organizations were notified I need to know the contractor name and CAGE Code as well as the POC name. I am required to notify the IS Rep of any contractor organization that was affected by the violation. If the external organizations were all government organizations, then please just provide the organization name and POC notified. Please provide this list as soon as possible, but no later than 7/19/2012."

I went out to and asked him for the information. You can read his response. Apparently he just passed along the deletion guidance he initially received from the sponsor and did not follow up specifically informing the recipients that the information was considered classified. Do you want us to follow up and inform the recipients that the slides were classified? I will ask to provide the full name and location of the facility where he sent the emails; it will take some time to determine the CAGE Codes of those facilities.

From:
Sent: Friday, July 13, 2012 2:10 PM
To:
Cc:
Subject: Re: ACTION REQUIRED from the January 2012 MSN PMTR at Austin

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

[redacted] FOIA(b)(6)

On 7/13/2012 1:52 PM, [redacted] wrote:

Can you tell me who it was mailed to and the address?

From: [redacted]
Sent: Friday, July 13, 2012 1:49 PM
To: [redacted]
Cc: [redacted]
Subject: Re: ACTION REQUIRED from the January 2012 MSN PMTR at Austin

As for the physical shipment, all I can find is that we mailed a copy to NGA in St. Louis.

[redacted]

On 7/13/2012 1:40 PM, [redacted] wrote:

[redacted]

To clarify, I didn't notify people of a spill. The information was that there was the potential to create a spill and to delete these presentations to remove the potential.

I do not know CAGE codes and appropriate security POCs for these organizations. The best I can provide is the list of people and organizations to which we emailed the link (which you can see in the email below). I'm also in the process of determining who we mailed copies to as well. Do I need to contact each person and ask for a CAGE code and a security POC? Is there a way the security office at ARL can lookup that type information?

[redacted]

On 7/13/2012 12:45 PM, [redacted] wrote:

[redacted]

I would like for you to answer the question; not me since you are the one who notified the folks that there was a spill. Please provide one or two short paragraphs delineating what organizations were notified and if they were contractor organizations, their CAGE Code as well as a POC for each organization. If they were just government organizations then the organization name and POC is all.

Thanks

[redacted]

From: [redacted]
Sent: Friday, July 13, 2012 9:51 AM
To: [redacted]
Cc: [redacted]
Subject: Fwd: ACTION REQUIRED from the January 2012 MSN PMTR at Austin

FOIA(b)(6)

You can see in the To and CC below the list of people/organizations that the original link was sent to and this is the same list that the delete instructions were sent to in the email below.

Does that sufficiently allow you to answer the question you posed this morning?

[redacted]

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

-------- Original Message --------

Subject: ACTION REQUIRED from the January 2012 MSN PMTR at Austin
Date: Wed, 29 Feb 2012 12:42:11 -0600
From: [redacted]
To: [redacted]

"Sch

CC: [redacted]

NGA has requested that the following unclassified presentations be deleted if you have electronic copies or destroyed if you have hard copies.

- Presentation #6 titled "IT/IS Migration" by [redacted] File name 06-ITIS-MigrationV2.pdf
- Presentation #10 titled "MSN OPS Support" by [redacted] File name 10-Jan2011-Ops Support-final.pdf

FOIA(b)(6)

Please contact me or [redacted] with any questions.

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

Thanks,

[redacted]

On 1/19/2012 3:12 PM, [redacted] wrote:
We have just posted the read ahead material for the meeting next week Wednesday and Thursday (Jan 25 -26). The only presentations that are missing are for a couple of the side sessions on Thursday (note, not all side sessions have material). You can download the presentation information in a zip file called MSN_PMTR_2012_Jan.zip located at:

https://ftp.arlut.utexas.edu/arl_web_ftp/ftp/ftproot/priv/SGL/bqstaging/January2012PMTR

I will send the password and username in the next email.

Dial in information will be available for the meeting and is as follows:

Call 512-873-5432.
Conference number is 3644#
Passcode is 44121#

We will attempt to host a web meeting as well but this may or may not happen due to recent issues with the web meeting server. If we are successful, the address for the web meeting is:

https://meeting.arlut.utexas.edu/msnpmtr/

Lunch will be provided each day to facilitate the flow of the meeting.

Please let me know if you have any questions. We are looking forward to the discussion next week.

[redacted] FOIA(b)(6)

On 1/10/2012 5:49 PM, [redacted] wrote:

Based on some feedback, I have several updates I want to distribute. The updated agenda is attached. Changes from the previous are:

1. Additional talk by [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)
2. Several new side sessions resulting in a new end time on Thursday, 26 Jan of 1400. (Note that the ordering of side sessions has not been set and will be varied based on interest and travel schedules of participants.)
3. Due to the number of participates, the main PMTR session (25 Jan) will be held in the main auditorium just behind the ARL lobby.

I will be emailing out a link to the electronic copy of the meeting next week, along with dial in information. I also plan on mailing hard copies of the presentation. If you are interested in a hard copy to support remote participation, please email me the number of copies and an address to send to.

[redacted]

On 1/3/2012 5:04 PM, [redacted] wrote:

As of today, I have the following people who have noted they will or may come (see end of email). If there are others, please let me know this week. You can find information about visiting ARL at:

http://www.arlut.utexas.edu/visiting/index.html

and information about submitting a clearance at:

http://www.arlut.utexas.edu/visiting/entry.html

While most of the meeting will be held at the

unclassified level, we may have certain sessions or discussion at the SECRET level.

[redacted] FOIA(b)(6)

NGA:

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

NSWC:

[redacted] FOIA(b)(6)

USAF:

[redacted] FOIA(b)(6)

On 12/14/2011 3:56 PM, [redacted] ~~wrote:~~ FOIA(b)(6)

The agenda for the MSN portion (on the 25th and 26th of January) is attached. Two requests:

1. If you plan on attending in person, please let me know by Friday, 6 January 2012. This is needed so I can plan for food and ensure security paperwork is in place for the visit.

2. I believe I have incorporated all the suggestions for agenda/side session topics. If you have any comments/additions/changes, please let me know in the next few days so I can work them into the agenda.

[redacted] FOIA(b)(6)

All,

We've settled on dates for the next program management and technical review of NGA tasks in progress at ARL:UT and NSWC.

These meetings will be in Austin, TX.

January 24, 2012 (Tuesday) - NSWC PMTR & side sessions (full day)
January 25th, 2012 (Wednesday) - ARL MSN PMTR (full day)
January 26th, 2012 (Thursday) - ARL MSN side sessions (partial day)

I will send out a draft for the MSN portion next week. Please let me know now if you have any topic or side meeting suggestions.

[redacted] FOIA(b)(6)

[redacted]

From: [redacted]
Sent: Friday, April 27, 2012 5:46 PM
To: [redacted]

Cc: [redacted]
Subject: RE: security issue
Signed By: [redacted]

[redacted]

My strategy had been to try to get them to declare the issue closed based on all the mitigation methods already applied, but having them judge that the case was not a spill at all is not something that I had considered. Perhaps that will work.

I will be TDY next week and therefore will have limited capabilities to work with [redacted] and team, but [redacted] will be in and help work the issue.

FOIA(b)(6)

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

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, April 27, 2012 8:33 AM
To: [redacted]
Cc: [redacted]

[redacted]

Subject: RE: security issue
Importance: High

[redacted]

We are having issues with getting an explanation from NGA classification management. [redacted] sent Rick an email via SIPRNET on April 10th citing why the presentation in question here is classified. However, all the information she cited that was classified was not in the briefing so we challenged her ruling in an email response on April 13th and have yet to get a satisfactory answer. We would like to include the Chief of classification management to get this resolved. When I spoke to [redacted] esterday she couldn't provide me with answers to questions she should have known being in he position of a classifier. We have extensively reviewed the SCG and are absolutely certain that there are no violations, spillages, etc. Please assist us in getting this resolved, we appreciate your assistance in this

matter. Thanks.

[redacted]
Information Systems Security Manager
Applied Research Laboratories
University of Texas at Austin
[redacted]

-----Original Message-----
From [redacted]
Sent: Friday, April 27, 2012 7:51 AM
To [redacted]
Cc [redacted]
Subject: Re: security issue

Thanks for pushing this. [redacted] got a call from her yesterday but I have not heard anything. [redacted] was pushing her for resolution and it didn't seem she had good answers. Hopefully we will hear something Monday.

[redacted]

On 4/26/2012 6:21 PM [redacted] wrote:
> [redacted]
> I talked to [redacted] and she should have already called you. I think
> I convinced her that this action needs to be closed, and she is trying to
> contact the investigator to that end.
>
> That said, this is a typical NGA activity, she is on a 4 day work
> week and the investigator has not been in during this week. I think you
> are
> not likely to get this resolved prior to Monday, but I will stay on it.
>
>
>
>
> [redacted]
>
>
>
>
>
> -----Original Message-----
> From: [redacted]
> Sent: Wednesday, April 25, 2012 8:47 AM
> To: [redacted]
> CIV
> Cc: [redacted]
> Subject: security issue
>

FOIA(b)(6)

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

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

> Here is the person that made the ruling. I have called and left a
> message. Would you continue to try and push this person to clarify what
is
> classified because we may have this information elsewhere which will
result
> in a expensive cleanup and then us repeating it again if we get
> clarification a few weeks from now. My security office is feeling under
the
> gun and really needs to get this resolved today.
>
[redacted]
>
>
> Thanks,
[redacted] FOIA(b)(6)
>
> AR: Security contacts:
>
[redacted]

FOIA(b)(6)

From:
Sent: Friday, April 13, 2012 4:24 PM
To:
Cc:
Subject: Re: Security Incident
Signed By:

I talked to about this. I have received the email that identified what was classified from NGA (as I showed you the other day). This morning, I sent off an response that asked for specific clarification to what is classified and provided examples that showed that I didn't believe any of the information the general statement identified was contained in the presentations. Until we receive that clarification, I cannot determine what in (or even if) the presentations were classified. Also without that information, I cannot determine if the same information they are flagging as classified exists in other project documentation.

On 4/13/2012 9:09 AM, wrote:

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

Can you contact this morning and see what the heck is going on and let me know. said this was all put to bed already and wasn't an issue...

From:
Sent: Friday, April 13, 2012 6:46 AM
To:
Cc:
Subject: Security Incident

I received a telephone call from at NGA this morning. He communicated to me that the information was classified and unless you have something in writing to the contrary, we need to complete a security violation report. Joe will be doing the initial draft of the report and he will require statements from you.

Facility Security Officer
The University of Texas System/
The University of Texas at Austin
Applied Research Laboratories

FOIA(b)(6)

From:
Sent: Tuesday, February 28, 2012 5:25 PM
To:
Cc:
Subject: Fwd: PMTR slides

Subsequent email will discuss this one.

-------- Original Message --------
Subject:PMTR slides
Date: Tue, 28 Feb 2012 12:33:47 -0600
From:
To
CC

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

After discussing with please remove last PMTR's presentations hardcopies and from ARL's wiki.

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

Thanks,

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Tuesday, February 28, 2012 5:45 PM
To: [redacted]
Cc:
Subject: NGA contact

Today, I received an email asking status about cleaning up two presentation given at the PMTR. This was the first time I had heard about it so I called and inquired from [redacted] regarding the details and have forwarded you an email from him. He said they required the items to be deleted from computers and have hard copies destroyed. At this point there is no information regarding why these presented and issue so the problem may also exist in other documentation we have. The files were/are at the following places in electronic form: FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)

SGL file server
ARL FTP site where they were downloaded by various external participants
Laptop used for the presentation
Other computers that sync the SGL file server -- not sure the complete list

What we have done so far this afternoon:

1. [redacted] has removed the files from the SGL file server
2. I have asked for clarification on how to handle the backup tapes
3. I have asked for clarification of what is the issue
4. I have removed the files from my laptop used for the presentation
5. I have turned one hardcopy into document control for future reference as we get clarification

What I still need to do:

1. Email all the people (internally and externally) that may have downloaded copies / have hard copies and ask that they be destroyed
2. Address the tapes after we receive clarification
3. Figure out if there are other issues after we understand the reasons
4. Ask people to delete any emails (inbox, sent, trash, etc) for pre-meeting copies that were email internally for review

We can discuss this further tomorrow.

[redacted]

[redacted] FOIA(b)(6)

From: [redacted]
Sent: Monday, June 25, 2012 8:31 AM
To: [redacted]
Subject: NGA Classification Management POC's
Signed By: [redacted]

Sir,

Here is the information you requested below...

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

[redacted]

FOIA(b)(6)

From:
Sent: Thursday, June 21, 2012 5:54 PM
To:
Cc:
Subject: Re: Review Draft Report
Attachments: ARL Security Violation 55354-20120531-C1_rgm.docx
Signed By:

I have a *significant* concern about this write-up and have included information in the attached document as well. It is written such that I am the only person who committed a security violation and I do *not* agree with that assertion. I didn't write either presentation (they were written by and I didn't do the initial aggregation on the file server (that was done by the two authors). I was only one of several people to review the material after it was written who didn't see this issue (and all of us still don't see what is classified by the NGA guide). My main contribution to this issue is moving the group of presentations around to different places that made them more accessible (printing, shipping, posting to external website).

I have also made some changes (marked with Word change marks) to correct some of the information in the write-up related to this above issue and other issues I noted. In addition to the changes, I did insert several comments where I was unsure how to change this text and described my concern.

FOIA(b)(6)

By the time I got to this review and saw this issue an hour or so ago, I tried to find both of you but you were gone for the day. I am going on vacation and will be out of the office until next week Thursday. You could reach me at home before 10 AM tomorrow at if you want to discuss this before I get back. I have CCed who is aware of the situation and could help answer questions and review any changes if this needs to get finished prior to my return.

PS: I know you asked for me to make the changes to what they should be w/o change marks. I didn't do that since I can't finalize the document and there are open questions. The change marks and the word comments were the best way I had to communicate the comments before I left for vacation.

On 6/21/2012 2:41 PM, wrote:

> Please take a look at the draft report. I am concerned about specifics as far as who contacted whom, when, and that the sequence of events is correct. If something needs to removed, added, or corrected, please let me know.
>
> Thanks

Facility Security Officer
The University of Texas System/
The University of Texas at Austin
Applied Research Laboratories

FOIA(b)(6)

From: [redacted]
Sent: Wednesday, June 27, 2012 9:45 AM
To: [redacted]
Cc: Joe Landry; [redacted]
Subject: 2ARL Security Violation 55354-20120531-C1_rgm.docx
Attachments: 2ARL Security Violation 55354-20120531-C1_rgm.docx
Signed By: [redacted]

[redacted]

Attached is a Final Report of an alleged security violation that occurred at ARL back in February. We have been trying (without success) to get specific information regarding the determination that unclassified information was "aggregated" and that the aggregation resulted in a security violation. I do not agree with NGA's determination; not the fact that aggregated unclassified information may be considered classified but the fact that the information contained on the two slide can be considered aggregated . You will see in my report that I am asking DSS to obtain that information from NGA. If you have any questions regarding the report or require additional information please let me know.

Thank you.

[redacted]

ARL
The University of Texas at Austin

27 June 2012

55354-20120228-C1
Final Report

Applied Research Laboratories
The University of Texas at Austin
10000 Burnet Road
Austin, Texas 78758-4423

CAGE Code: 55354
Facility Clearance: Top Secret
Facility Safeguarding Level: Top Secret
Contract No.: N00024-07-D-6200-5-74 and 5-46.
Program Name: Monitor Station Network

1. As directed by the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M, paragraph 1-303. a., a preliminary inquiry was conducted by the Applied Research Laboratories' (ARL), Facility Security Officer (FSO), [redacted] at ARL during the period 28 Feb 2012 - 20 Jun 2012 to consider the facts and circumstances surrounding an alleged security violation that occurred on 28 February 2012. This final report is being submitted late; an extension was granted by DSS, ISR [redacted] on 6 June 2012.

FOIA(b)(6)

2. ESSENTIAL FACTS:

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

What is alleged to have happened?

In early January of 2012, in preparation for an upcoming Program and Technical Review (PMTR) that occurred on 25 January at ARL: UT, several ARL employees developed unclassified presentations for the meeting. These presentations were emailed, inside ARL: UT, saved on ARL: UT servers, saved on various desktop and laptop computers, printed at the ARL: UT media center, mailed to external participants, and posted to a password protected externally visible website for download by external participants. [redacted] coordinated the posting and distribution of the presentation done by the ARL: UT team members. On 28 February, approximately one month after the PMTR, [redacted] received a telephone call from [redacted] at NGA (the sponsoring agency for most of the work) informing him that two of the presentations, one written by Jose Acevedo and one written by Richard Campbell from the PMTR contained "very sensitive" information. [redacted] handles the interfacing with NGA security for the NGA team as well as ARL: UT.) [redacted] communicated to [redacted] that individually each presentation was unclassified but if the information on the slides

were "aggregated", it had the "potential" to be classified. [redacted] then provided verbal direction on the actions to be taken and provided it in writing in a SIPRNet email on 2/29. He instructed [redacted] to delete soft copies of the presentation, destroy hard copies, overwrite the index of backup tapes but keep them in the rotation, delete emails (from all folders including trash), and inform external organizations that got copies of the presentations to destroy/delete them as well. This was completed on 29 February.

How was the violation discovered, and who reported it? To whom was it reported and when?

On 28 February [redacted] reported what he had discussed with [redacted] to the ARL ISSM, [redacted] and the ARL FSO, [redacted] When queried, [redacted] communicated to the FSO that the information contained in the individual presentations was not classified and that based upon his conversation with the sponsor [redacted] he [redacted] did not believe that the sponsor considered the information to be classified since the information was not aggregated.

On 19 March confirmation of a security violation was initially communicated to [redacted] (ARL Program Manager/ISSO) while reviewing a SIPRNet email sent by [redacted] asking for a copy of the security report [redacted] communicated that an initial classification ruling had been made by NGA regarding the aggregation of the two unclassified presentations. [redacted] relayed this information to the ARL security office. In response to [redacted] email, [redacted] requested a copy of the initial classification ruling that was made by NGA Classification Management – [redacted]

After repeated attempts, [redacted] was finally able to reach [redacted] on either the 6th or 9th of April. He received an email on April 10th that provided a couple of sentences that stated the information was SECRET/NF and provided the general category of information. She did not indicate if this was in aggregate or in a single presentation.

[redacted] reviewed the information [redacted] provided and compared it to the NGA security classification guide and the copies of the two presentations. (ARL retained one hardcopy of each presentation and marked them as classified.) In examining the presentations, [redacted] could not find any of the information she referenced in the email that was classified. This review was also done by ARL employee [redacted] and later by ARL ISSM [redacted] and the ARL FSO, [redacted] They all were each, unable to identify the referenced information in either presentation or in aggregate. On April 13th, [redacted] sent [redacted] an email referencing the relevant sections of the NGA SCG, explaining that none of the presentations contained the listed information; he listed the information the presentation did contain and asked her to describe what was classified based on the SCG or to reverse the ruling.

Since that email, ARL has not received a response. [redacted] spoke with [redacted] on April 13th and voiced his concerns referencing the email he had sent her. Since then [redacted] has called [redacted] and left several voice mails for her but has yet to receive a call back or an email clarification on the ruling. Messages were left during the week

of April 16th and April 23th. Also during the week of April 23rd, asked his sponsors to see if they could get a response from

discussed with on April 26th the incident. She was unable to provide answers to questions about the classification determination that believes as a classifier, should have been able to answer. requested contact information from NGA for the supervisor in the NGA classification office. The name he was given was attempts by both the ARL ISSM and the ARL FSO to contact have been unsuccessful.

Although ARL has not received a response from did receive a telephone call from on May 31, who stated he had received an email from and that she had made a final classification ruling in response to the challenge. He indicated that she was in agreement with original classification ruling i.e. that the two presentations when aggregated were in fact classified. communicated that he would forward email via SIPRNet to and he also requested ARL send him an email summary of all actions that were taken in regards to computer sanitization so the incident could be closed out. received email from however, it did not address the details about what information was classified, only that a final classification ruling had been made.

What information was involved, and what is its classification? (Obtain a listing of the material, if appropriate.)

The classified material is considered to be "aggregate" Secret/NF information that can be derived from two unclassified PowerPoint presentations that were created separately by and (ARL) on their unclassified desktop computers and distributed to a number of locations as described in the first paragraph of section 2 above.

Identify the GCA and associated prime/subcontractors who originated the classified information.

The NGA GCA regarding security matters for this TD is

Identify the GCA or prime contractor that released the classified information to the contractor and the associated contract numbers.

The ARL contract N00024-07-D-6200-5-74 and 5-46. The NGA GCA for security matters is

Identify specific NISPOM provisions violated. Indicate whether the company was required to have a Standard Practice Procedure (SPP), its level of adequacy, and whether the company complied with the SPP. If applicable, attach a copy of the applicable portions of the SPP that

reflect promulgation of the rules and regulations of the SPP and/or NISPOM to employees authorized for access.

ARL employee [redacted] violated provision 8-102 of the NISPOM that states "The CSA is the DAA responsible for accrediting information systems used to process classified information in industry." [redacted] posted unclassified information on an external web page that could be considered classified if aggregated; albeit, he didn't know the aggregation of the information was considered classified. Also, this is a violation of the NISPOM paragraph 4-213, "Marking Compilations" whereas certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the compilation shall be conspicuously affixed. The ARL SPP for Security paragraphs A-B. 9. and X-B. adequately covers these areas.

OIA(b)(6)

3. CORRECTIVE ACTIONS:

What actions were taken to protect the classified information prior to the inquiry (e.g., inventories, securing material, changing container combinations)? When were these actions taken and by whom?

Prior to notification from NGA that the information contained on the two unclassified presentations was "potentially" classified if aggregated, no action was taken to protect the information. By definition the information contained in the individual briefings is unclassified. Lacking prior knowledge that the aggregation of the information contained in the two briefings would be considered classified, ARL employees took no unusual measures to protect it.

Will the contractor take disciplinary action against the individual? If not, why not? Include any follow-up actions.

The ARL employee responsible for the security violation is ARL employee [redacted] (ARL Program Manager/ISSO). The importance of determining classification prior to creating and/or posting program information was discussed with [redacted] by the FSO. Prior to posting the slide presentations [redacted] did in fact review the classification guidance and took steps to ensure that the information was unclassified.

[redacted] understands the classification guides; he is thoroughly familiar with the information contained in the unclassified presentations and he understands the concept of unclassified information becoming classified based upon aggregation of the information. He was unaware that when he posted the two unclassified presentations on the external web site that the information contained in the two separate slides in the two different presentations could be considered aggregated and/or classified when aggregated.

Include an evaluation of the corrective actions taken by the contractor to preclude future violations.

The circumstances surrounding this incident have been promulgated to all cleared ARL employees.

4. CONCLUSIONS:

When, for how long, and under what circumstances was the classified information vulnerable to unauthorized disclosure?

When the sponsor notified [redacted] (ARL Program Manager/ISSO) that the aggregation of the two presentations could possibly be considered classified information, he immediately took action and contacted the security office to minimize the incident. [redacted] along with the ARL IT department followed the sanitization guidance provided by the sponsor (NGA) to delete all electronic soft copies, destroy all hard copies, overwrite the index of backup tapes but keep in rotation, delete all emails that contain these presentations, and inform personnel that got copies to destroy/delete them. The information was available to unauthorized disclosure from the time the presentations were created sometime in mid-January until all sanitizations procedures were completed as directed by the sponsor on 29 Feb 2012. During that time the information was stored electronically on the ARL/SGL File Server, ARL FTP Site, ARL Email Server, ARL desktop/laptop computers, other computers that sync the ARL/SGL server, mailed to external organizations, and downloaded by external organizations. There is no indication that any unauthorized individuals accessed the information.

FOIA(b)(6)

If an unauthorized person gained knowledge of classified information, describe how the knowledge was gained and provide identifying data about the unauthorized person to include current and previous eligibility and access information.

N/A

Are there other security violations at this facility pertaining to this contract, technology, or information? If so, is there a pattern? Does the pattern include foreign nationals/visitors?

None

Have foreign nationals expressed an interest in the contract, technology, or information at the facility? If so, is there a pattern?

None

The individuals interviewed in connection with the violation are to be identified. Interviews for each person should be recorded in a narrative format, reflecting their position at the facility and the date of the interview.

[redacted] Program Manager/ISSO/Questioned 29 February and sent a statement via e-mail on 11 May 2012 by the FSO [redacted]

Your conclusion regarding the loss or compromise of the classified information is to be included.

Given the fact that the two documents in question (two separate unclassified PowerPoint slides in two separate slide presentations) are both unclassified and created by ARL employees [redacted] and [redacted] that they were created as unclassified documents and therefore contain no classified marking; that they were placed separately on a password protected, external ARL web page along with multiple (19) other unclassified presentations; and that the slides containing information that, when aggregated, could be considered classified, were in different presentations; the chances of an unauthorized person accessing the web page, accessing the two slides from the different presentations and aggregating the information is very remote. Even though there is no indication that the information contained in the two unclassified presentations was accessed by unauthorized individuals, because the presentations resided on the external web page for approximately 30 days, the possibility of compromise, though remote, exists. FOIA(b)(6)

Additionally, because the information was contained on two separate slides on two separate presentations, each individually accessed; the ARL FSO questions the determination by NGA that the information can be considered "aggregated". Analogous to this would be technical information contained in volumes residing on the shelves of a technical library. If the two unclassified presentations in question were on separate tables is the same room would they still be considered aggregated; if the two presentations were in different rooms in the same building would they still be considered aggregated? Absent specific definition and/or handling guidance, unless the information is truly aggregated, i.e. unclassified information on the same slide or unclassified information contained within the same briefing it cannot be considered aggregated.

5. DETERMINATION OF CULPABILITY

Provide identifying data (name, title/position, Social Security number, date and place of birth, access level) of the individual who was/is responsible for the incident.

Name: [redacted]
Job Title: Project Manager/ISSO
Employees SSN: (will be provided telephonically upon request)
Date of Birth: [redacted]
Place of Birth [redacted]
Clearance Level: [redacted]
Date of Last Security Briefing: [redacted]

ARL Telephone Number: [redacted]
Statement Obtained: YES

FOIA(b)(6)

The interview of the responsible individual must stress the following:

- Individual's level of awareness of the NISPOM and associated security regulations. Include when and how the individual became aware of the classified information.

  The employee [redacted] involved in this incident is familiar with his individual security requirements under the NISPOM and the ARL SPP for Security. Because [redacted] was the employee responsible for posting the presentations on the external web page he is technically responsible for creating the security violation; however, there is no degree of guilt or blame to assign.

FOIA(b)(6)

- Details of all prior security briefings, seminars, etc., contributing to the individual's knowledge of security requirements.

  ARL New Employee Security Briefing
  Annual Security Awareness Training
  Semi Annual Security Briefings

- Individual's knowledge of security requirements and awareness of the company's practices and how he or she became aware of them. Provide a description of the facility's security education and training program. Attach copies of any and all records concerning security briefings (written and oral) provided to the individual to prove the extent of individual's knowledge of the requirements for the proper handling of classified information. If available, include dates, times, and information provided in the security briefings, as well as copies of any debriefing statements.

  (on file)

- A detailed review of each document, item, or system involved in the violation to include the individual's knowledge of where they came from; where each was found and under what circumstances; why each was found where it was located; whether each was in the classified document information management system; and whether they contained prominent classification markings. Conduct follow-up questioning on disparities between the individual's statement and known facts.

  The two documents in question (two separate unclassified PowerPoint slide presentations) are both unclassified; created by ARL employees [redacted] and [redacted] They were created as unclassified documents and therefore contain no classified marking; no classification markings are required. They were placed separately on an external ARL web page by [redacted] along with multiple (19) other unclassified presentations. The two slides containing information that, when aggregated, could be considered classified, were in different presentations.

- The reasons the individual acted as he or she did in this particular incident.

  The individual acted in accordance with established ARL procedures.

- Whether the individual was aware that he or she was violating security guidelines at the time of the incident

  ARL employees were unaware that creating and posting the unclassified presentations could be viewed as violating security guidelines at the time of the incident; it was neither deliberate nor intentional.

- The individual's future intentions regarding the handling and safeguarding of classified material.

  There is no reason to suspect that ARL employees will do anything other than follow the proscribed rules and guidelines given to them; they have demonstrated that they are aware of their individual responsibilities.

- Your evaluation of the individual's culpability.

  The employees are culpable only to the extent that it was determined by NGA Classification Management Office that the aggregation of the two unclassified presentations would create classified information. There was no mention or concern by the program sponsor during the PMTR and it was only a month after the PMTR that a classification determination was made. ARL employees fully cooperated with the Security Office and followed sponsor (NGA) guidance when they initially became aware of the possibility that the two presentations, if aggregated, would contain classified information, they are aware of their responsibilities to protect classified information and to report any security violations.

6. RECOMMENDATIONS:

The NGA Classification Management Office has determined that the aggregate of the two unclassified presentations are classified at the Secret/NF level; however, ARL has yet to receive any official guidance about what exactly is classified and has requested from NGA this information. As such, ARL does not agree with NGA's classification determination. IAW NISPOM 4-104, ARL herein requests that the CSA (DSS) provide assistance in obtaining a satisfactory response; specifically what information in the two unclassified presentations prepared by [redacted] and [redacted] when aggregated, is classified; more specifically, why the information is considered classified. This is in an effort to preclude this from happening again. NGA POC(s) are [redacted]

FOIA(b)(6)

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

7. FOLLOW-UP:

IAW NISPOM 4-104, absent a 120 day response from the CSA, the classification challenge will be forwarded to the Interagency Security Classification Appeals Panel (ISCAP) through the ISOO.

Table of Contents

(U) Summary Statement

(U) Clear and direct guidance on the exact nature of what Classified information is in the Exhibits was never provided despite repeated requests from both ARL:UT and from DSS to the original classifier, her direct supervisor, and other members of the NGA Security Office. The NGA SCG was reviewed by [redacted] ARL:UT, [redacted] ARL:UT, [redacted] ARL:UT, and [redacted] ARL:UT. After careful inspection of Exhibits A and B, all four are unanimous that none of the slides contain Classified information, nor is there any risk of Classified by Aggregation. As such, it is impossible for ARL:UT to know which information was Classified without additional information.

FOIA(b)(6)

(U) Clear and direct statements as to what constitutes "aggregation" were never provided. ARL:UT requires a specific definition in order to prevent future violations by aggregation. Note that, historically, two separate hardcopies existing in the same desk have not been considered "aggregated". In the modern era, should two electronic files stored on the same hard drive be considered aggregated? For the analysis described above, ARL:UT operated under the assumption that aggregation meant the two files were considered as a single file (even though they never existed in this state).

(U) The limited guidance received was in conflict – in some cases the Exhibits were referred to as Classified individually, in other cases, only in aggregate.

(U) Purpose of Request

(U) The NGA SCG ARL:UT is contractually obligated to follow does not contain any information from which a reasonable person would conclude a violation occurred. As such we believe either the SCG is in error or the classifying agency is in error. The original ruling should be reversed or the SCG should be updated and new classification guidance provided to ARL:UT.

(U) Request

(U) ARL:UT requests complete and full details on which exact information in both Exhibits is Classified and for what reasons with references to specific paragraphs and/or table line numbers of appropriate classification guides.

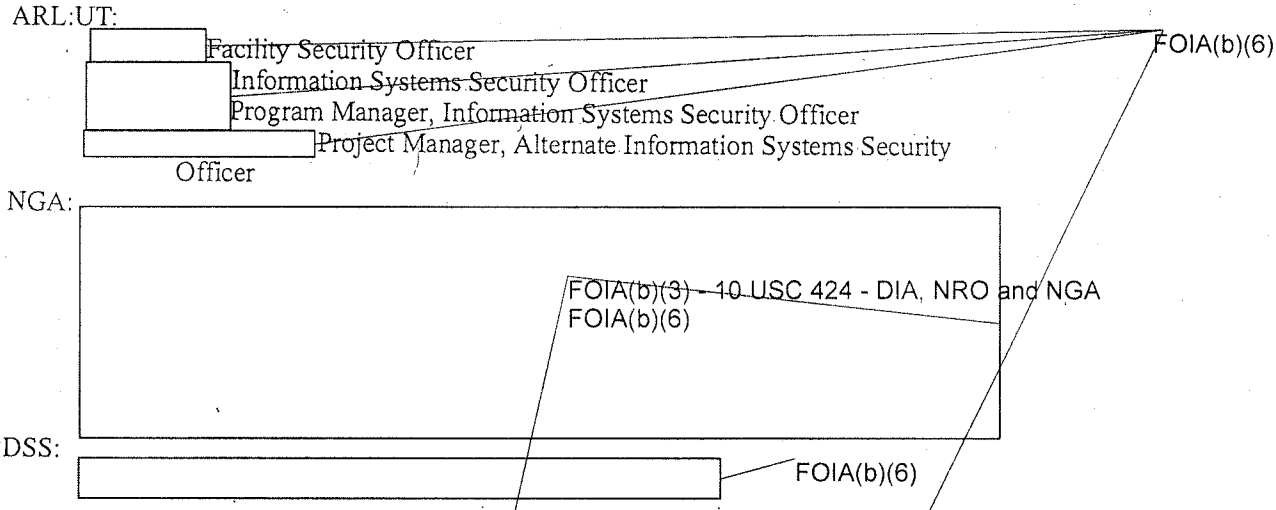
(U) ARL:UT requests complete and full details on what constitutes 'aggregated' in the case of electronically stored documents.

(U) Chronological Timeline of Relevant Communication

(U) The majority of paragraphs below refer to email correspondence. Those items taken from phone calls are indicated as "by phone". All emails used to develop this summary are included as part of this packet.

(U) Organizations Listed:
ARL:UT: Applied Research Laboratories, The University of Texas at Austin
NGA: National Geospatial-Intelligence Agency
DSS: Defense Security Service
ISCAP: Interagency Security Classification Appeals Panel

(U) Personnel Listed:



Timeline:

(U) 25 January 2012: Program Management and Technical Review held at ARL:UT. The two presentations in question (hereafter referred to as Exhibit A and B) were presented at this meeting. The majority of this meeting was held at the Unclassified level.

(U) 28 February 2012: [redacted] NGA requested that [redacted] ARL:UT remove electronic Unclassified access to the Exhibits and destroy all hardcopies.

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

(U) 27 June 2012: [redacted] ARL:UT sent the final report to [redacted] DSS, restating that requests for specific information had not been answered, and stating his opinion that a portion of the NGA ruling was in error, specifically, that two separate presentations could be considered aggregated. His report also asked DSS to assist in obtaining the specific information requested from NGA.

FOIA(b)(6)

(U) 5 July 2012: [redacted] NGA acknowledged receipt of final report and of the fact that ARL:UT would be challenging the ruling.

(U) 23 July 2012: Defense Security Service acknowledged receipt of a final report, dated 27 June 2012, regarding this security violation and confirmed that mitigation efforts (as referenced in 29 February email) taken by ARL:UT were sufficient.

(U) 14 December 2012: [redacted] RL:UT prepared and sent to ISCAP a formal challenge of the Classification ruling highlighting that ARL:UT is seeking detailed and specific explanations on what was Classified to avoid future incidents.

(U) 20 December 2012: The Interagency Security Classification Appeals Panel acknowledged receipt of ARL:UT's classification challenge and requested further information.

(U) List of Attachments

(U) Exhibit A: Presentation: MSN Ops Support (~~S//NF~~)

(U) Exhibit B: Presentation: IT/IS Migration (~~S//NF~~)

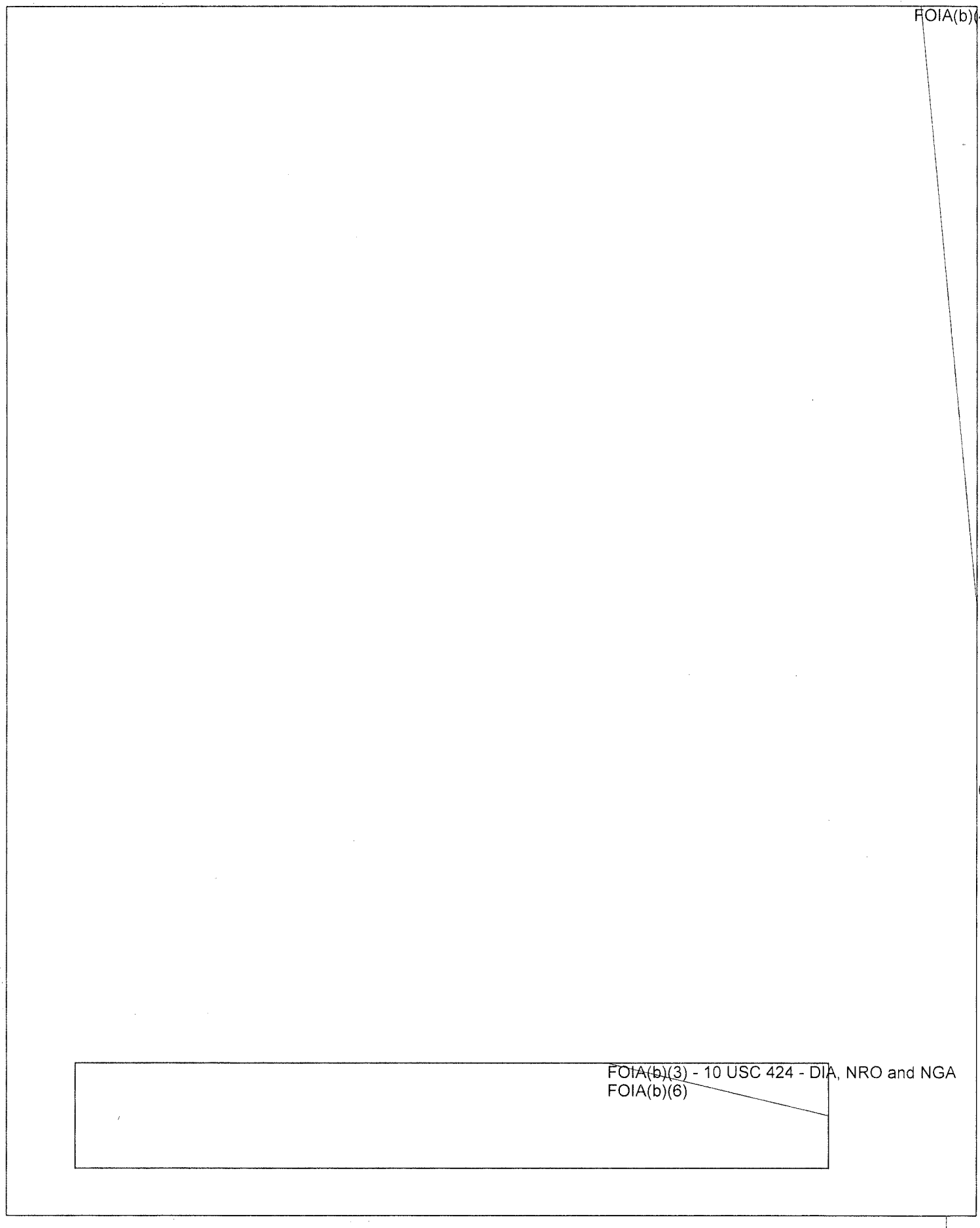
(U) NGA Security Classification Guide (March 25, 2008 version)

(U) Final report to DSS from ARL

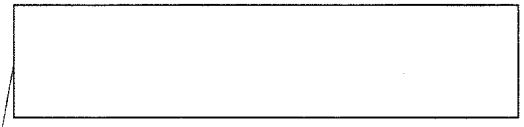
(U) SIPRnet Email collection (~~S//NF~~)

(U) Unclassified Email collection

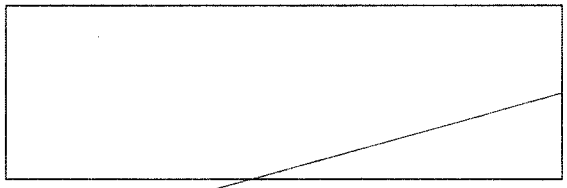
(U) Unclassified Mail collection



FOIA - b(1)



FOIA(b)(3) - 10 USC 130b - PII for armed forces
FOIA(b)(6)



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

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

APPLIED RESEARCH LABORATORIES
THE UNIVERSITY OF TEXAS AT AUSTIN

P. O. Box 8029 · Austin, TX 78713-8029 · (512) 835-3200 · Fax: (512) 835-3259

This cover letter is unclassified upon removal of classified enclosures.

31 January 2013
ISCAP No. 2013-030

TO: Interagency Security Classification Appeals Panel
700 Pennsylvania Avenue, N.W., Room 100
Washington, D.C. 20408

ATTN: Mr. William Carpenter

FROM Dr. Clark S. Penrod
Executive Director

SUBJECT: Challenge to Classification Determination (U)

REF: (a) (U) NISPOM 4-104.
(b) (U) ISCAP Executive Secretary ltr. 20 December; ISCAP No. 2013-030

ENCL: (1) (U) Summary and Supporting Material in support of ISCAP No. 2013-030 (S/NOFORN)
(2) (U) "IT/IS Migration" PowerPoint Slide Presentation prepared by Jose Acevedo, Exhibit (A); "MSN OPS Support" PowerPoint Slide Presentation prepared by Richard Campbell, Exhibit (B)
(3) (U) National Geospatial-Intelligence Agency (NGA), Security Classification Guide, dtd. 25 March 2008 (S/NOFORN)
(4) (U) Classified Emails between NGA and ARL: UT personnel. (S/NOFORN)
(5) (U) Unclassified Emails between NGA and ARL: UT personnel.
(6) (U) ARL: UT Security Violation 55354-20120228-C1 dtd. 27 June 2012

1. (U) In accordance with reference (a) as directed by reference (b) a challenge by the University of Texas, Applied Research Laboratories (ARL) regarding a Government classification determination is herein submitted.

2. (U) Enclosure (1) is a classified, chronological sequence outlining events and communications between the NGA and ARL as they pertain to an alleged security incident that occurred in January 2012.

3. (U) In preparation for an NGA Program Management and Technical Review (PMTR) conference being held at ARL on 25 January 2012 [redacted] and [redacted] each, independently, prepared PowerPoint slide presentations; enclosure 2, Exhibit A and enclosure 2, Exhibit B respectively, utilizing NGA Security Classification Guidance (enclosure 3). It was determined by both [redacted] and [redacted] that their individual slide presentations were unclassified and they marked them accordingly. Their slide presentations were turned over to ARL employee [redacted] who posted these presentations, along with 19 other unclassified presentations, on an internal ARL web page. The web page was accessible by authorized NGA personnel and authorized ARL personnel.

4. (U) Enclosures 4 and 5 are classified and unclassified email exchanges between ARL employees and NGA personnel during the period February 2012 through July 2012. The emails are provided to support the sequence of events as outlined in enclosure 1.

5. (U) Enclosure 6 is a copy of the ARL security violation report submitted to the Defense Security Service on 27 June 2012. From the report it can be seen that ARL has tried (without success) to get specific information from NGA regarding the determination that unclassified information was "aggregated" and that the aggregation resulted in a security violation.

6. (U) ARL is challenging the classification determination by NGA; specifically that any of the slides in either [redacted] or [redacted] PowerPoint presentations (enclosure 2, exhibits A and B) are classified. If NGA's classification determination (that one or more of the slides in either of the two presentations is classified) is upheld by the ISCAP, it is requested that the specific information deemed classified be identified and provided to ARL, and that the reason for the classification as outlined in the NGA classification guide (enclosure 3) also be specifically identified and provided to ARL.

7. (U) If the ISCAP determines that the information contained in both [redacted] and [redacted] presentations is unclassified but further determines that the aggregation of that information constitutes a security violation, it is requested that the specific information deemed classified be identified and provided to ARL and that the specific reason for the classification, as outlined in the NGA classification guide (enclosure 3), also be identified and provided to ARL.

   (U) Additionally, if the ISCAP determines that the information contained in both [redacted] and [redacted] presentations is unclassified but further determines that the aggregation of that information constitutes a security violation, it is requested that the ISCAP provide specific guidance on aggregation

FOIA(b)(6)

and/or confirmation that information contained in two distinct files on the same (electronic) system can indeed be considered "aggregated."

8. (U) Your consideration and timely action in this matter is appreciated. While erring on the side of caution, ARL continues to use a classification guide whereas we are unsure of the guidelines; without an explanation of why NGA determined that a security violation had occurred, we may inadvertently misinterpret the SCG again.

9. (U) If you require additional information or have any questions regarding this matter the ARL, POC is our Facility Security Officer, [redacted] His telephone number is [redacted] FOIA(b)(6)

Neena Sachdeva

From: William C. Carpenter [redacted] FOIA(b)(6
Sent: Wednesday, February 13, 2013 11:23 AM
To: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
Cc: [redacted] Neena Sachdeva FOIA(b)(6)
Subject: (U) Classification Challenge Appeal to ISCAP: ARL:UT, Appeal No. 2013-030 (S/NF)
Attachments: 2013-030 Composto Material Request (U).pdf; 2013-030 Incoming Challenge Appeal (S-NF).pdf

Classification: ~~SECRET//NOFORN~~

Classified By: William Carpenter
Reason: 1.4(c), (g)
Declassify On: 20380111
Derived From: ARL:UT Classification Challenge, dated 20130131
==========

[redacted]

(U) The Interagency Security Classification Appeals Panel (ISCAP) has received a classification challenge appeal concerning information classified by the National Geospatial-Intelligence Agency (NGA). The attached Unclassified letter from John Fitzpatrick, the ISCAP Executive Secretary, requests that NGA provide the ISCAP a justification for its decision to classify the information in question. Specifically, the challenge by the Applied Research Laboratories at the University of Texas at Austin (ARL:UT) seeks clarity regarding how the concept of classification by aggregation was applied in this case.

(U) The larger classified attachment consists of the appeal package provided to the ISCAP by ARL:UT. The ISCAP Staff are preparing a briefing book for presentation to the ISCAP membership on March 12 for this appeal as well as for the classification challenge appeal filed with the ISCAP by GeoEye, Incorporated (tracked as ISCAP Appeal No. 2013-035). We hope that we may include NGA's responses in this briefing book, so the ISCAP members may more fully understand NGA's positions for these appeals.

(U) We would be happy to speak with you or your staff about these two appeals in the coming weeks. The adjudication of classification challenge appeals are comparatively rare events for the ISCAP, and the ISCAP Staff must ensure that all sides of the challenge are adequately understood by the ISCAP members. Please contact me, my colleague on the ISCAP Staff Neena Sachdeva, or ISOO Associate Director Bill Cira with questions or concerns.

William Carpenter
Program Analyst, Information Security Oversight Office
National Archives and Records Administration
Secure [redacted] FOIA(b)(7) - (C
Unclassified: 202-357-5466

[Unclassified when removed from classified attachment]

==========

Classification: ~~SECRET//NOFORN~~

INFORMATION PAPER

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

1. (U//~~FOUO~~) **Purpose**. To provide an information paper to DNI and USD(I) on ARL-UT Classification Challenge and Appeal to ISCAP in accordance with Executive Order (E.O.) 13526, "Classified National Security Information," Section 5.3. *Interagency Security Classification Appeals Panel.*

2. (~~S//NF~~) **Content.** FOIA(b)(1) NGA

3. (~~S//NF~~) **Background on NGA's final ruling on ARL-UT materials:** FOIA(b)(1) NGA

CL BY: 1303432
CL REASON: NGA SCG
DECL ON: 20371219

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

Item # 1. Description: (U) An aggregate account of individual items, otherwise unclassified, items that reveal a system, objective, requirement, plan or other aspect of NGA or its mission the disclosure of which would jeopardize NGA organization, functions and organization, functions and capabilities, or U.S. intelligence sources or methods. See remarks. Classification: SECRET, Release: NOFORN, Declass: 25 yrs, Reason: 1.4 (C), Remarks: This is known as classification by compilation.

Item #14. Description: (C)

FOIA(b)(1) NGA

Item #16. Description: (U//~~FOUO~~)

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

Item #17. Description: (U//~~FOUO~~)

b) NGA Classification Management once again used the 25 March 2008, NGA Security Classification Guide (SCG), Version 1.1, Table 1.10 (U)

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

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

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

[redacted] FOIA(b)(1) NGA

5. (U) **Point of contact.** The NGA point of contact for this matter is [redacted] who may be reached at [redacted] or [redacted]

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

EXHIBIT LIST

EXHIBIT A – (2) DD 254 Tasking Order for delivery of classified materials

20110225 – TOP SECRET Tasking Order, Contract Number N00024-07-D-6200

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

(U) Section 15K of this Tasking Order provides a complete list of DoD and NGA mandatory compliance documents, to include security classification guides/guidance.

EXHIBIT B – Statement of Work (SOW) Memorandum of Understanding

EXHIBIT C – PowerPoint Presentation: MSN OPS Support

(S//NF) This Exhibit addresses: FOIA(b)(1) NGA

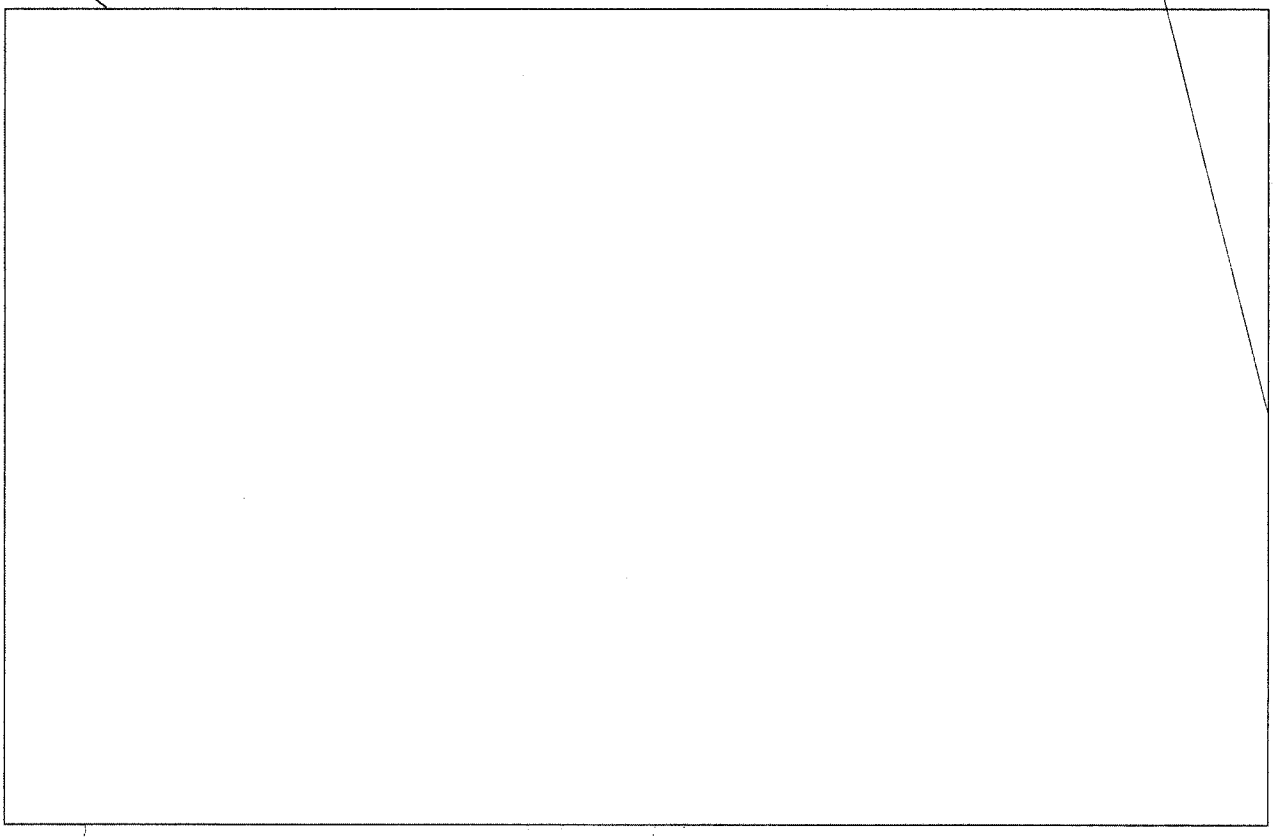


EXHIBIT D – PowerPoint Presentation: IT/IS Migration dated 25 January 2012 (Jose Acevedo)

(U) Refer to pages 3 and 6. This Exhibit lists:

- Migration schedule (p 6)
- Network IP space to NGA managed addresses (p 3)

EXHIBIT E – Executive Order, 12 February 2013, Improving Critical Infrastructure Cybersecurity

APPLIED RESEARCH LABORATORIES
THE UNIVERSITY OF TEXAS AT AUSTIN

P. O. Box 8029 · Austin, TX 78713-8029 · (512) 835-3200 · Fax: (512) 835-3259

This cover letter is unclassified upon removal of classified enclosures.

31 January 2013
ISCAP No. 2013-030

TO: Interagency Security Classification Appeals Panel
700 Pennsylvania Avenue, N.W., Room 100
Washington, D.C. 20408

ATTN: Mr. William Carpenter

FROM Dr. Clark S. Penrod
Executive Director

SUBJECT: Challenge to Classification Determination (U)

REF: (a) (U) NISPOM 4-104.
(b) (U) ISCAP Executive Secretary ltr. 20 December; ISCAP No. 2013-030

ENCL: (1) (U) Summary and Supporting Material in support of ISCAP No. 2013-030 (S/NOFORN)
(2) (U) "IT/IS Migration" PowerPoint Slide Presentation prepared by Jose Acevedo, Exhibit (A); "MSN OPS Support" PowerPoint Slide Presentation prepared by Richard Campbell, Exhibit (B)
(3) (U) National Geospatial-Intelligence Agency (NGA), Security Classification Guide, dtd. 25 March 2008 (S/NOFORN)
(4) (U) Classified Emails between NGA and ARL: UT personnel. (S/NOFORN)
(5) (U) Unclassified Emails between NGA and ARL: UT personnel.
(6) (U) ARL: UT Security Violation 55354-20120228-C1 dtd. 27 June 2012

1. (U) In accordance with reference (a) as directed by reference (b) a challenge by the University of Texas, Applied Research Laboratories (ARL) regarding a Government classification determination is herein submitted.

2. (U) Enclosure (1) is a classified, chronological sequence outlining events and communications between the NGA and ARL as they pertain to an alleged security incident that occurred in January 2012.

3. (U) In preparation for an NGA Program Management and Technical Review (PMTR) conference being held at ARL on 25 January 2012, [redacted] and [redacted] each, independently, prepared PowerPoint slide presentations; enclosure 2, Exhibit A and enclosure 2, Exhibit B respectively, utilizing NGA Security Classification Guidance (enclosure 3). It was determined by both [redacted] and [redacted] that their individual slide presentations were unclassified and they marked them accordingly. Their slide presentations were turned over to ARL employee [redacted] who posted these presentations, along with 19 other unclassified presentations, on an internal ARL web page. The web page was accessible by authorized NGA personnel and authorized ARL personnel.

4. (U) Enclosures 4 and 5 are classified and unclassified email exchanges between ARL employees and NGA personnel during the period February 2012 through July 2012. The emails are provided to support the sequence of events as outlined in enclosure 1.

5. (U) Enclosure 6 is a copy of the ARL security violation report submitted to the Defense Security Service on 27 June 2012. From the report it can be seen that ARL has tried (without success) to get specific information from NGA regarding the determination that unclassified information was "aggregated" and that the aggregation resulted in a security violation.

6. (U) ARL is challenging the classification determination by NGA; specifically that any of the slides in either [redacted] or [redacted] PowerPoint presentations (enclosure 2, exhibits A and B) are classified. If NGA's classification determination (that one or more of the slides in either of the two presentations is classified) is upheld by the ISCAP, it is requested that the specific information deemed classified be identified and provided to ARL, and that the reason for the classification as outlined in the NGA classification guide (enclosure 3) also be specifically identified and provided to ARL.

7. (U) If the ISCAP determines that the information contained in both [redacted] and [redacted] presentations is unclassified but further determines that the aggregation of that information constitutes a security violation, it is requested that the specific information deemed classified be identified and provided to ARL and that the specific reason for the classification, as outlined in the NGA classification guide (enclosure 3), also be identified and provided to ARL.

(U) Additionally, if the ISCAP determines that the information contained in both [redacted] and [redacted] presentations is unclassified but further determines that the aggregation of that information constitutes a security violation, it is requested that the ISCAP provide specific guidance on aggregation

FOIA(b)(6)

and/or confirmation that information contained in two distinct files on the same (electronic) system can indeed be considered "aggregated."

8. (U) Your consideration and timely action in this matter is appreciated. While erring on the side of caution, ARL continues to use a classification guide whereas we are unsure of the guidelines; without an explanation of why NGA determined that a security violation had occurred, we may inadvertently misinterpret the SCG again.

9. (U) If you require additional information or have any questions regarding this matter the ARL, POC is our Facility Security Officer, [redacted] His telephone number is [redacted] FOIA(b)(6)

~~SECRET//NO FORIEGN~~

(U) Summary and Supporting Material in support of ISCAP No. 2013-030

Classified by: NSA
Reason: 1.4(c), (g)
Declassify On: 11 January 2038
Derived from: NGA SCG AIS-08.11, NGA SCG MET-08.1.1

~~SECRET//NO FORIEGN~~

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

~~SECRET//NO FORIEGN~~

(U) 28 February 2012: [redacted] NGA phoned [redacted] ARL:UT and informed Mr. Mach that Exhibits A and B, if aggregated, had the potential to be considered Classified. [redacted] disputed the fact that these documents, in aggregate, would be Classified, based on understanding of the contents of the March 2008 NGA SCG.

FOIA(b)(6)

(S//NF) [redacted]

(U) 1 March 2012: [redacted] ARL:UT asked for specific guidance from NGA on why Exhibits A and B needed to be cleaned up.

(S//NF) [redacted]

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

(S//NF) [redacted]

FOIA(b)(1) NGA

(U) 19 March 2012: [redacted] ARL:UT stated clean up instructions provided 29 February were executed in full by COB 29 February.

(U) ?? March 2012: [redacted] ARL:UT requested, via phone call, specific clarification on which portions of the Exhibits were Classified, as a careful reading of the NGA SCG indicated that, even if the Exhibits were aggregated, there was nothing Classified.

(U) 10 April 2012: [redacted] NGA responded by repeating the Exhibits were Classified because of discussions about "vulnerabilities to the systems and how it affects NGA's methodology in protecting its assets", and the decision was "consistent with NGA SCG AIS Table, line item." There was no line item specified in this email.

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

~~SECRET//NO FORIEGN~~

~~SECRET//NO FORIEGN~~

(U) 13 April 2012: [redacted] ARL:UT sent a detailed email to [redacted] ARL:UT explaining all sections of the NGA SCG that appeared relevant to previous classification guidance and how those sections did not indicate the Exhibits should be considered Classified. He also requested specific guidance on what, exactly, was Classified so that ARL:UT could update procedures accordingly to reduce risk of future spills and eliminate exiting aggregation of the same information in other project documentation.

(U) 13 April 2012: [redacted] ARL:UT stated that he had received a phone call from [redacted] NGA indicated that the Exhibits were in fact Classified and that ARL:UT should complete a security violation report.

(U) 26 April 2012: [redacted] ARL:UT sent a reminder email to [redacted] NGA, as no response had yet been received to his request for clarification and justification.

(U) 27 April 2012: [redacted] ARL:UT requested assistance from [redacted] NGA to obtain specific guidance from [redacted] NGA, highlighting that her original ruling was challenged by ARL on 13 April and no subsequent response had been received.

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

FOIA(b)(6)

(U) 8 May 2012: [redacted] ARL:UT informed [redacted] ARL:UT that since NGA classification management was not responding to requests for information, [redacted] ARL:UT had to go forward with the original NGA ruling and proceed to treat this as a security violation, and ARL would need to start sanitization procedures.

(U) 8 May 2012: [redacted] ARL:UT provided a report to [redacted] ARL:UT summarizing events, including a note that sanitization procedures, as typically required to clean up spills, could not be carried out until specific guidance on what information was Classified was obtained.

(U) 9 May 2012: [redacted] ARL:UT requested assistance from [redacted] NGA to have either [redacted] NGA or [redacted] NGA contact either the ARL:UT security office or [redacted] ARL:UT directly to discuss what information was Classified. [redacted] stated his own opinion that the Exhibits were sensitive, but not Classified.

(S//NF) 10 May 2012: [redacted] NGA requested a fresh copy of the exact two slides which, in aggregation, led to the violation, from [redacted] NGA.

(S//NF) 10 May 2012: [redacted] NGA replied that he was unsure which parts [redacted] NGA had decided constituted a violation. He asked for more clarification from her.

~~SECRET//NO FORIEGN~~

~~SECRET//NO FORIEGN~~

(S/NF) 10 May 2012: [redacted] NGA stated in an email to [redacted] NGA that his interpretation of Classification guidance was that the Exhibits, even in aggregation, did not constitute classified information, and requested the case be closed as not a spill.

(S/NF) 23 May 2012: [redacted] NGA asked [redacted] NGA as to the status of the classification decision – was it still considered a spill or not.

(U) 30 May 2012: [redacted] NGA informed [redacted] ARL:UT that he should deal with [redacted] NGA directly.

(S/NF) 29 May 2012: [redacted] NGA requested [redacted] NGA step in with a response.

(S/NF) [redacted]

(S/NF) 30 May 2012: [redacted] NGA concurred with [redacted] NGA and stated that ARL:UT should employ appropriate mitigation plans.

(U) 31 May 2012: [redacted] ARL:UT informed [redacted] DSS that NGA had ruled that ARL:UT caused a security violation, and stated that the NGA ruling was the Exhibits were Classified when aggregated. He indicated cleanup procedures were in progress.

(U) 1 June 2012: [redacted] ARL repeated the request to [redacted] NGA on guidance as to which specific parts of the Exhibits were Classified.

(U) 8 June 2012: [redacted] ARL acknowledged receipt of final ruling, and reiterated request for clarification on what information was Classified to avoid future incidents.

(U) 15 June 2012: [redacted] NGA stated the decision had been reviewed by [redacted] NGA and was final and requested a final report.

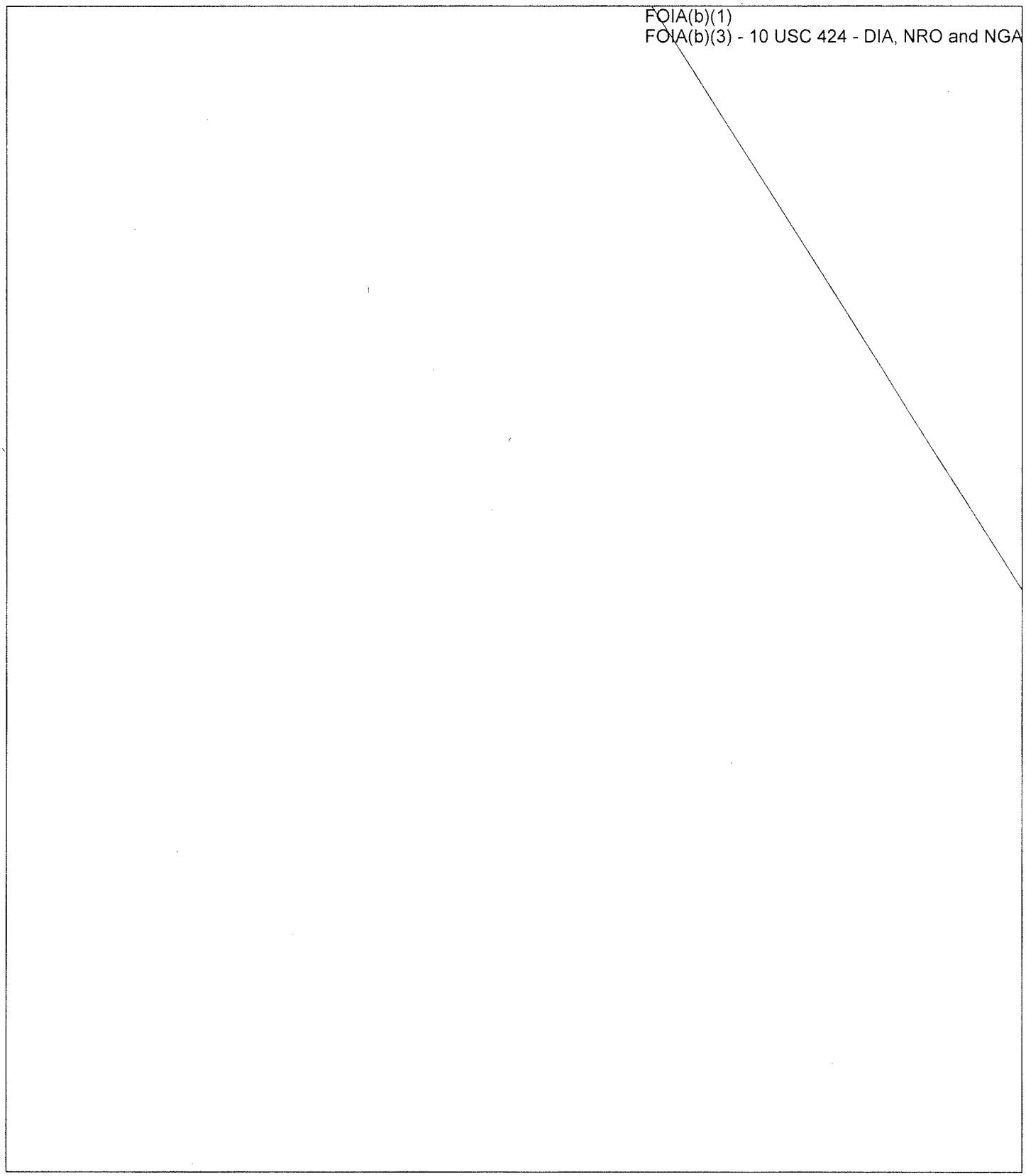
(U) 27 June 2012: [redacted] ARL:UT forwarded to [redacted] NGA the final report as sent to DSS discussing this incident. He again stated that since specific guidance on what was Classified had not been received, and since ARL:UT still did not agree that the Exhibits were classified, that ARL:UT would be asking for DSS assistance in challenging the ruling via ISCAP in accordance with procedures in the NISPOM.

~~SECRET//NO FORIEGN~~

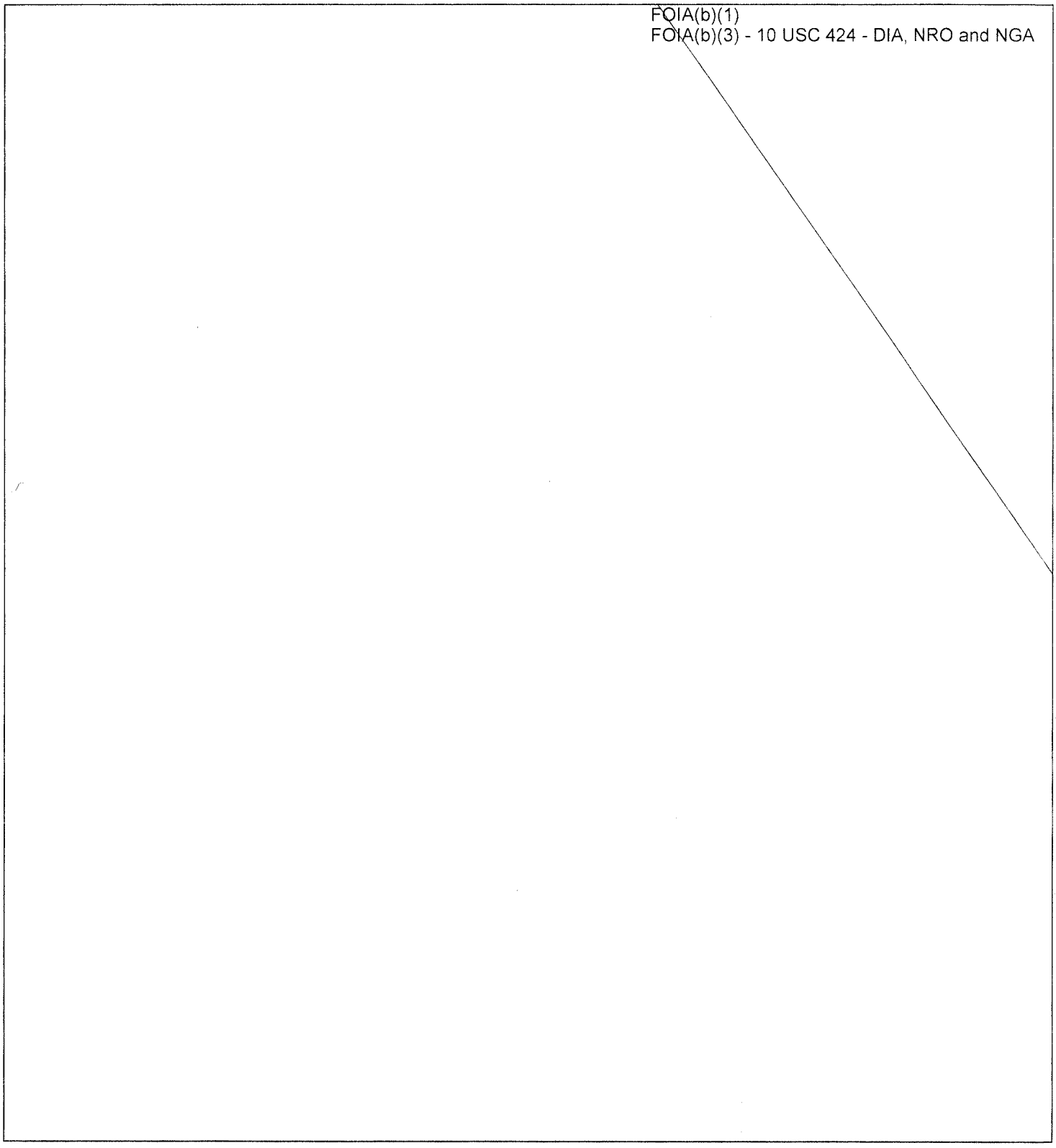
FOIA(b)(3) - 10 USC 424, DIA, NRO and NGA
FOIA(b)(6)

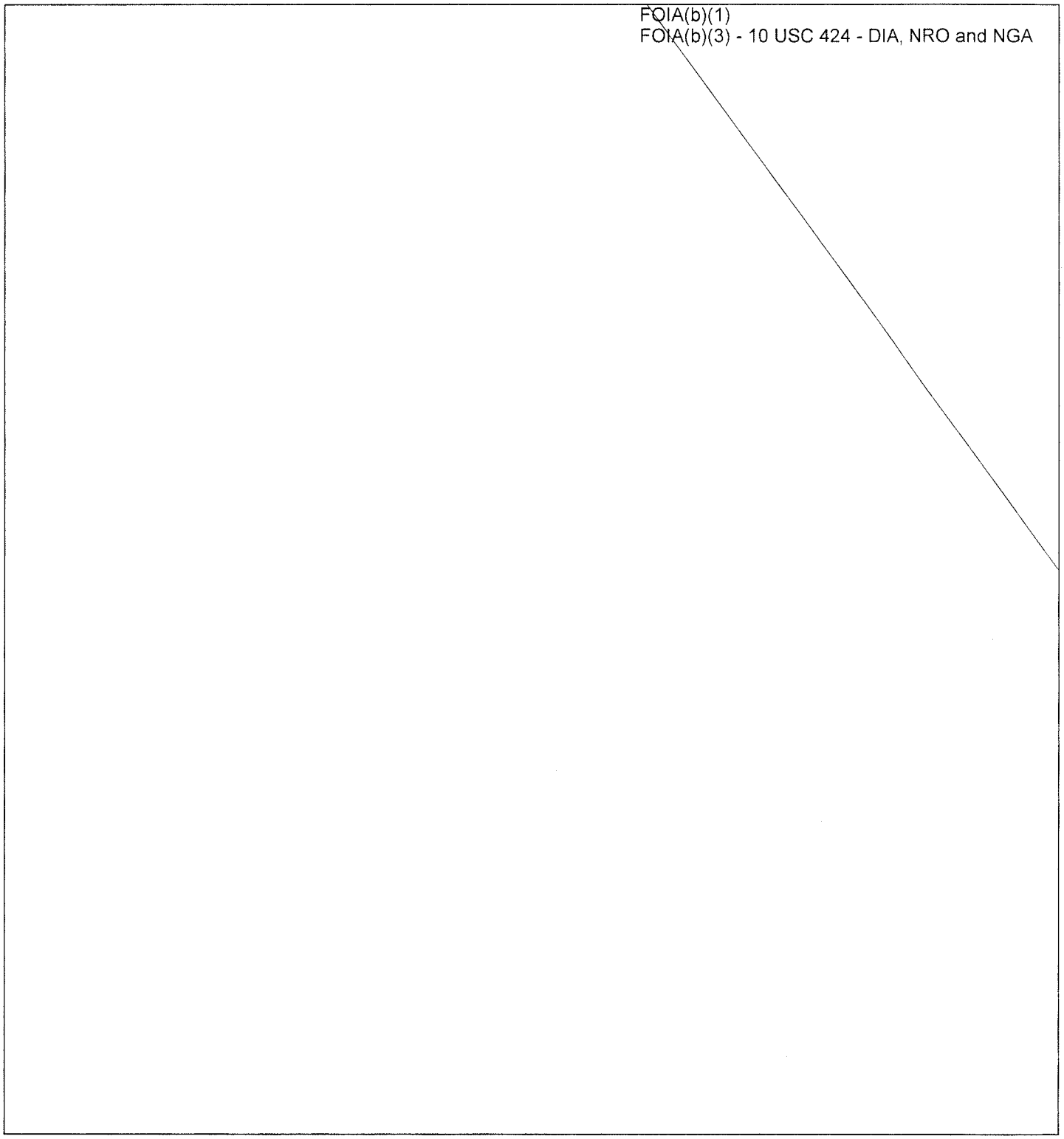
FOIA(b)(1) FOIA(b)(3) 10 USC 424, DIA, NRO and NGA FOIA(b)(6)

FOIA(b)(1) NGA

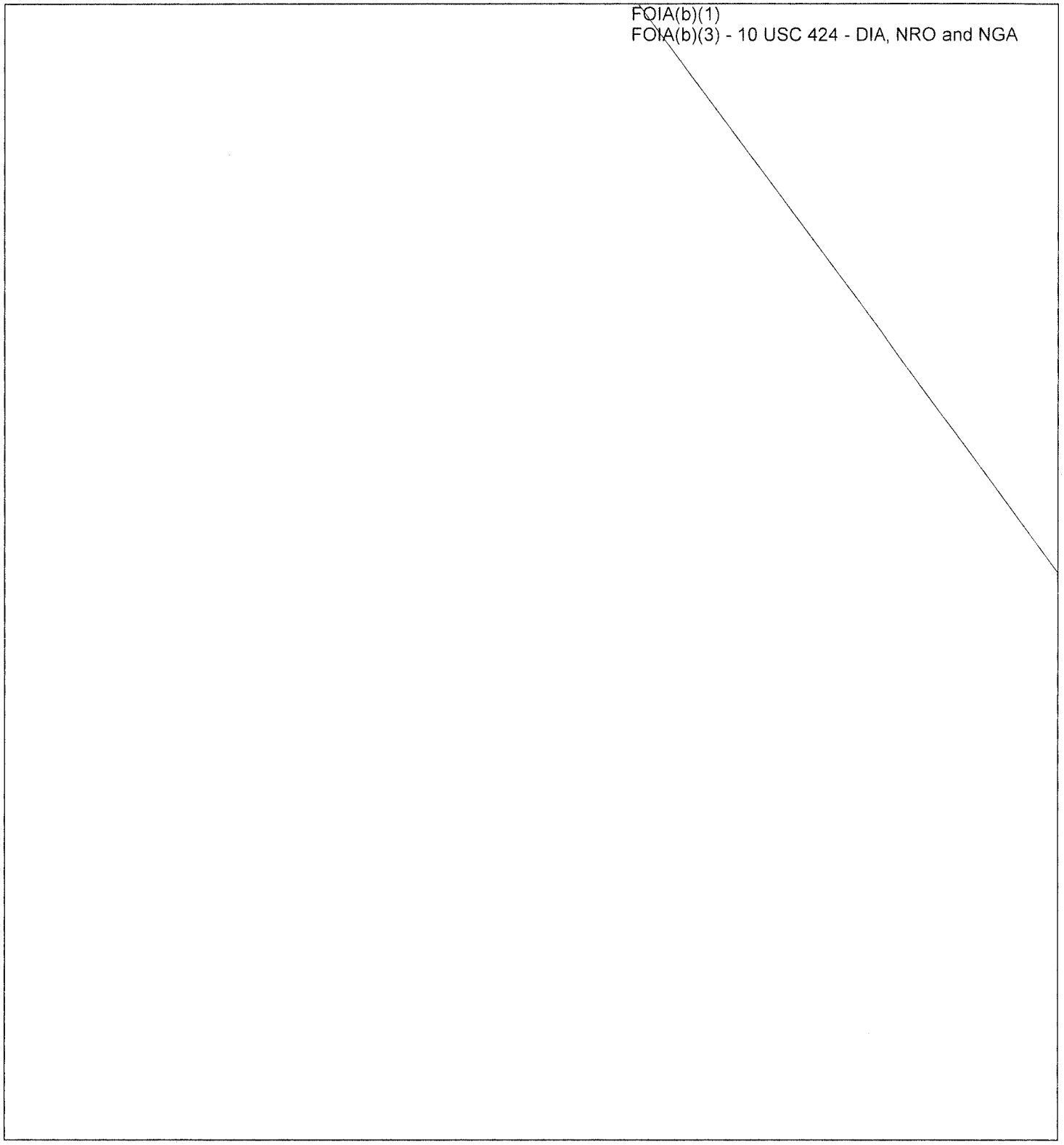


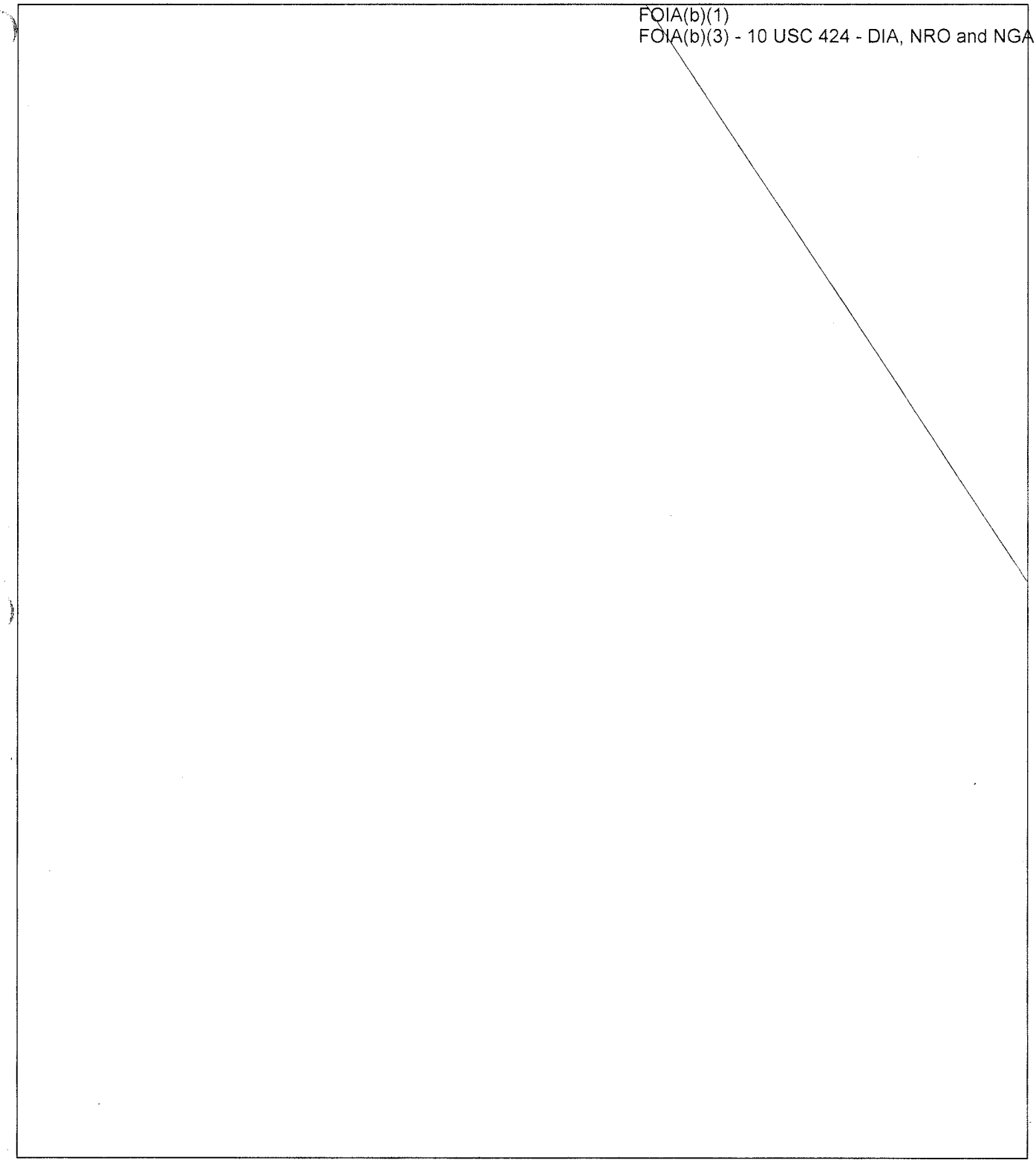
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

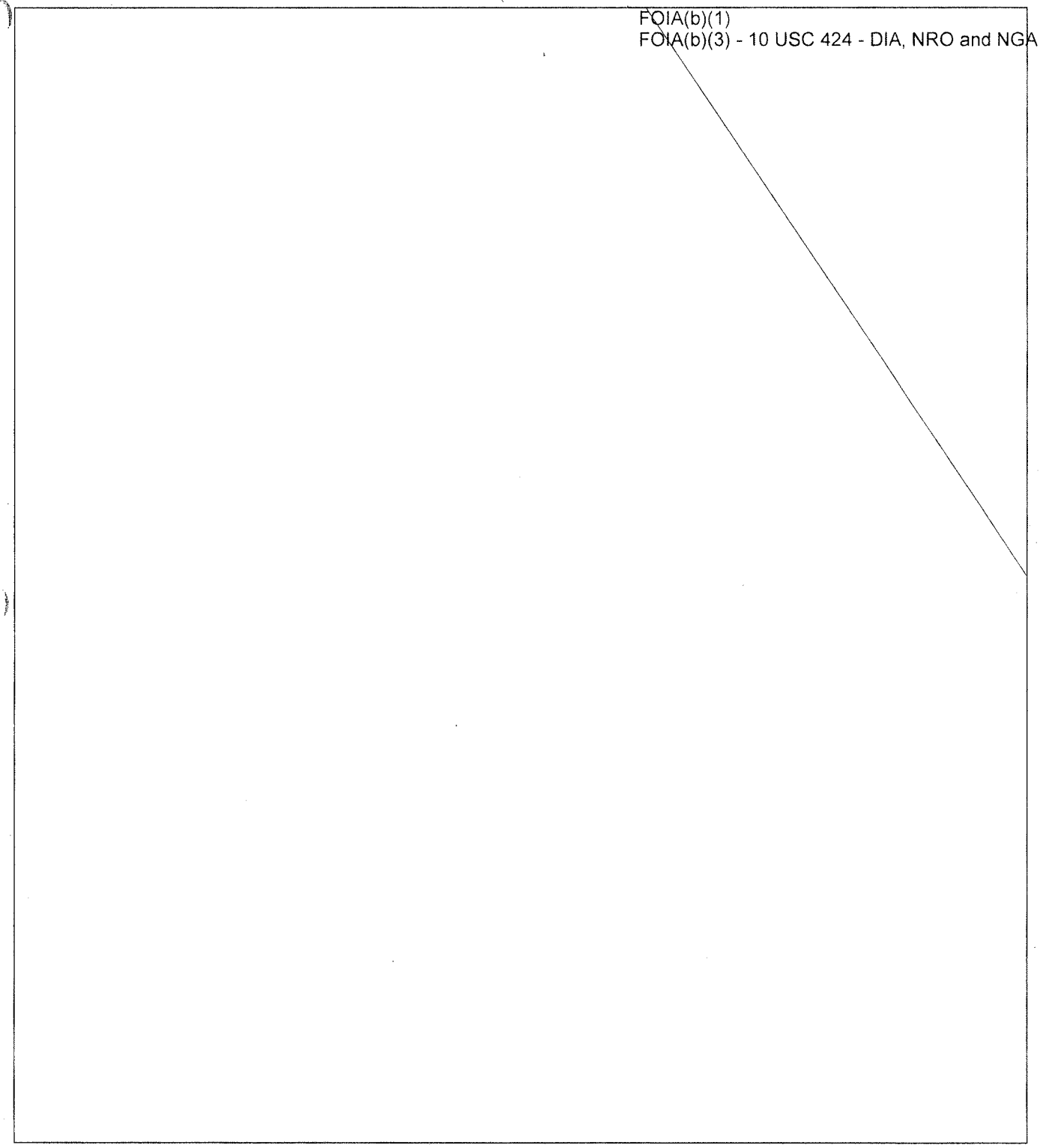


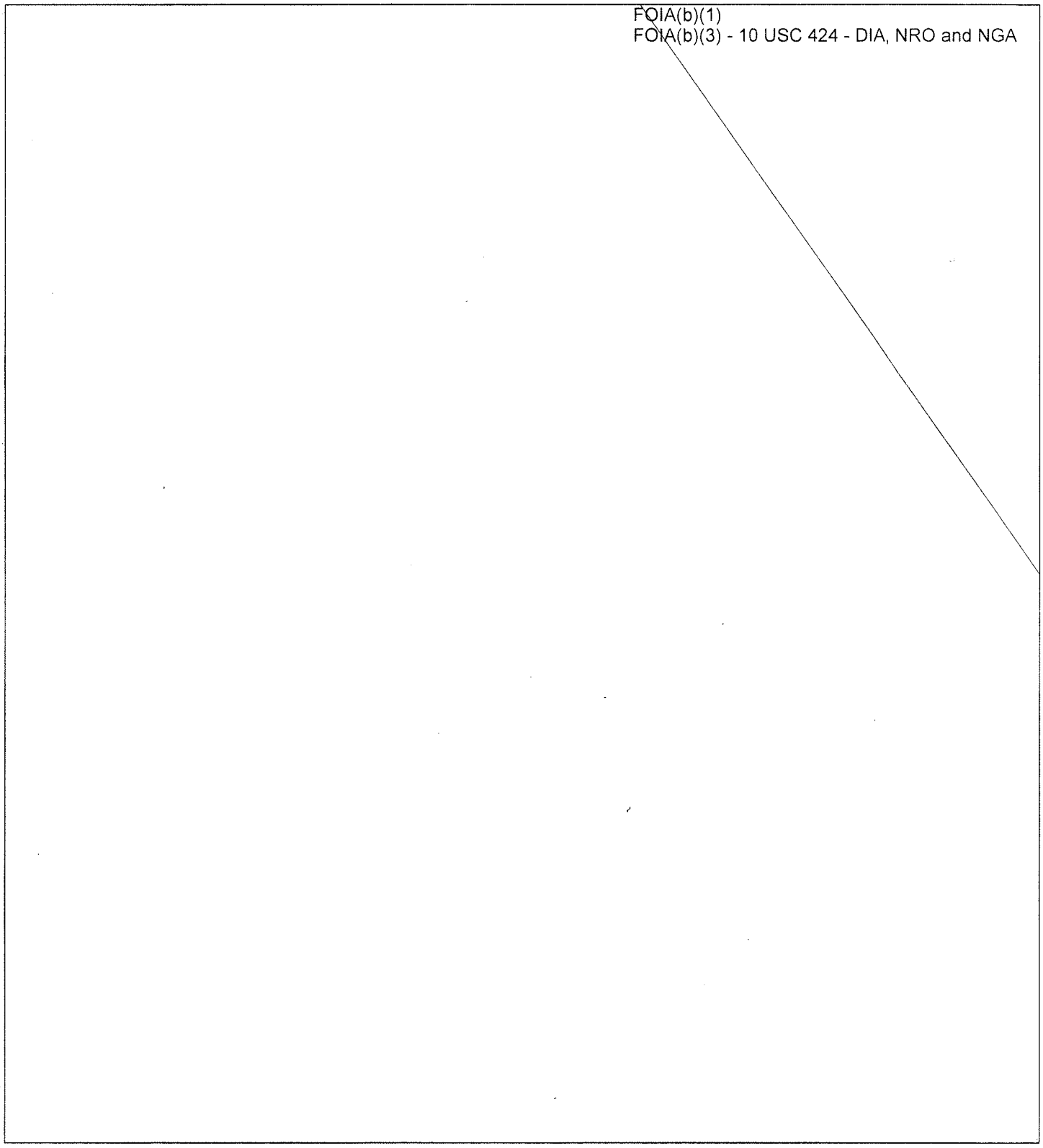

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

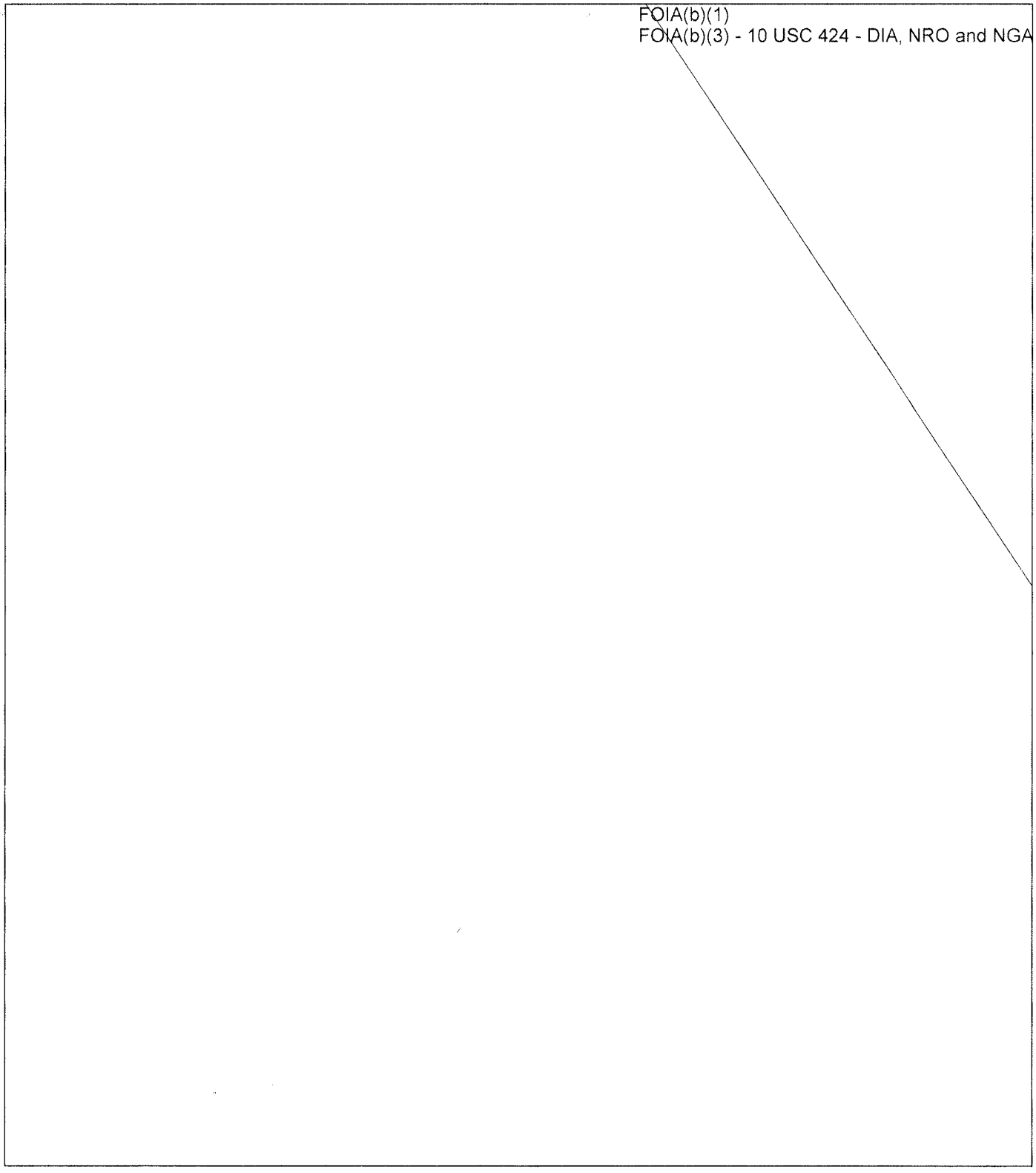
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

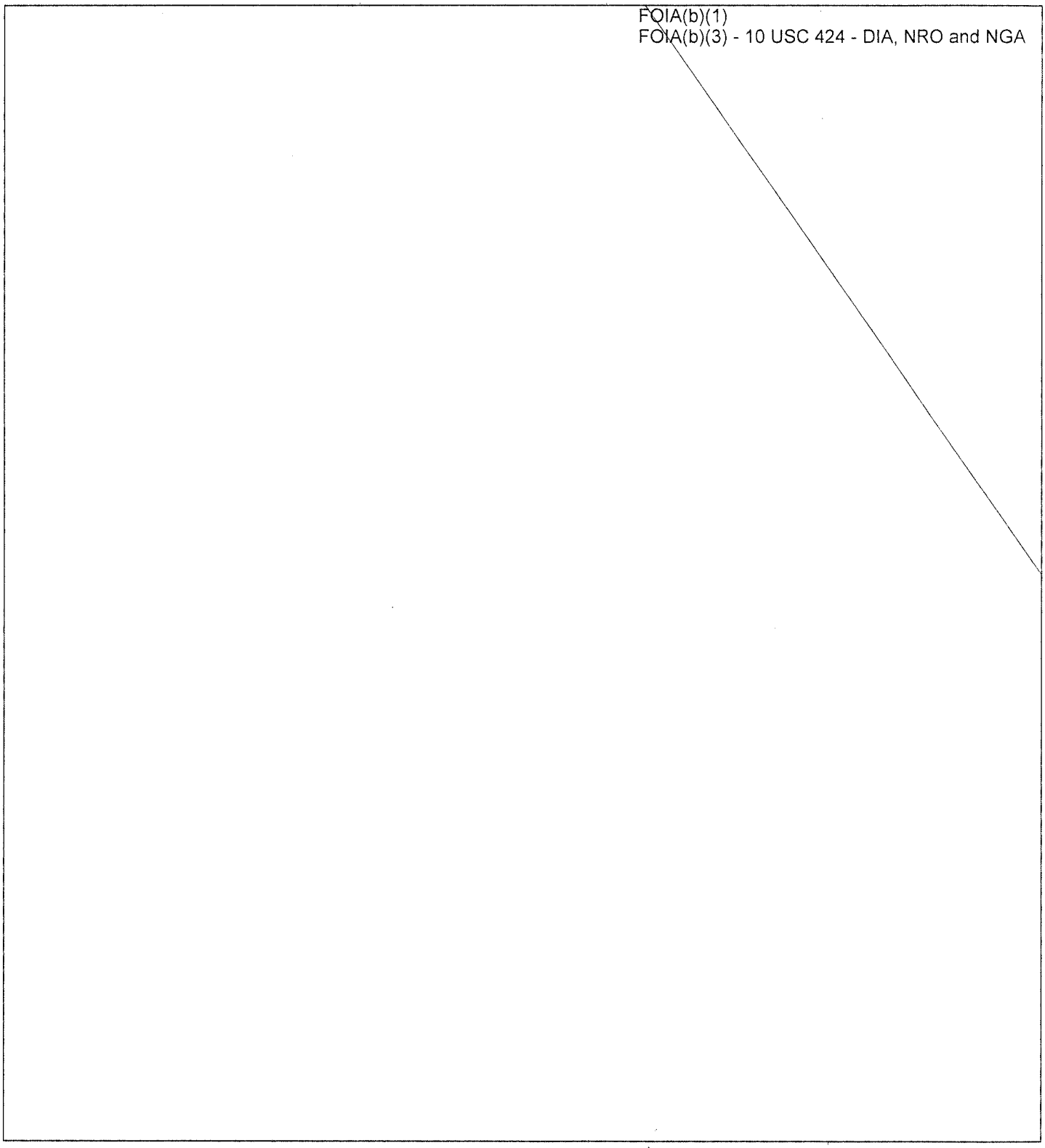





FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

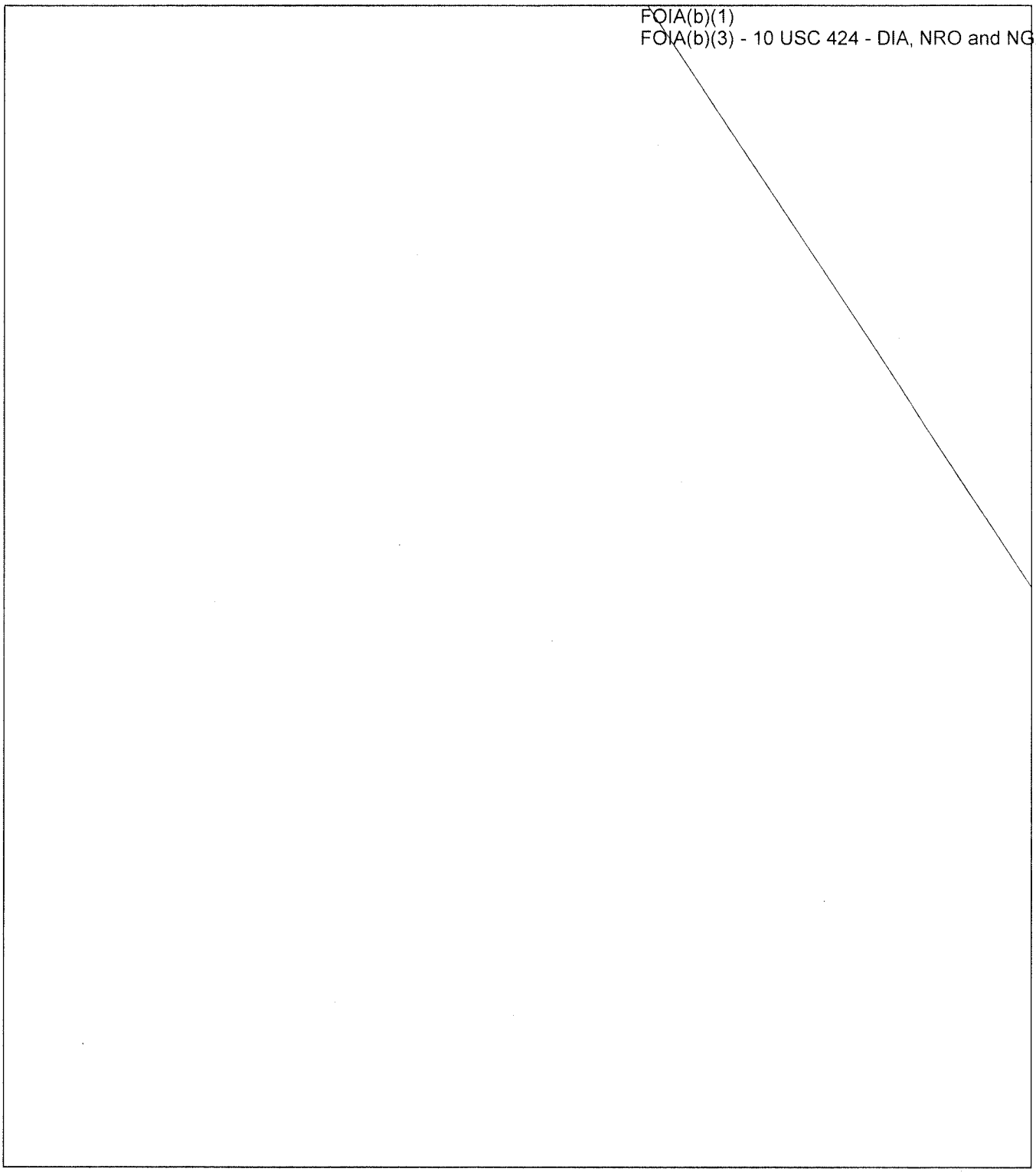

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

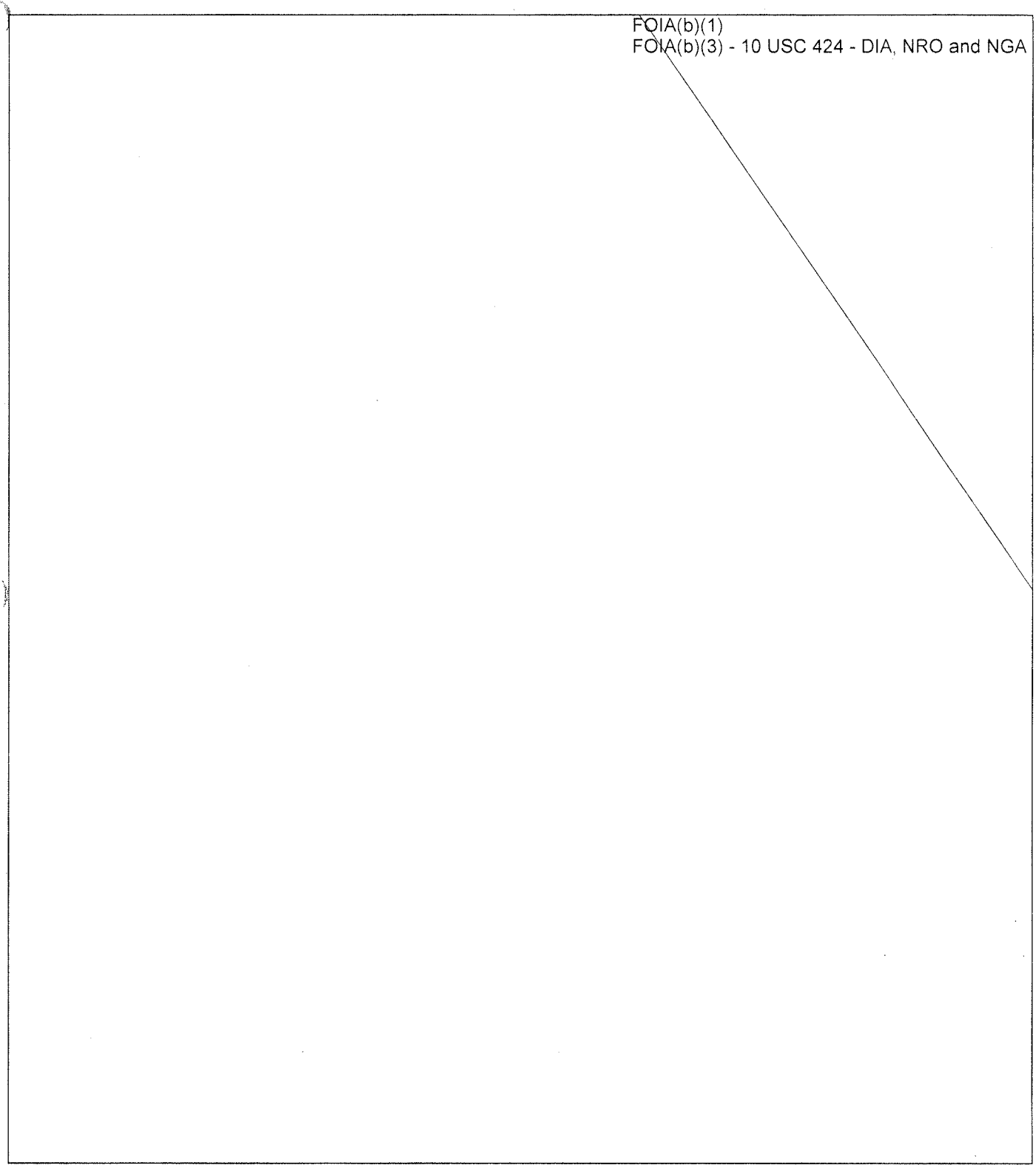

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

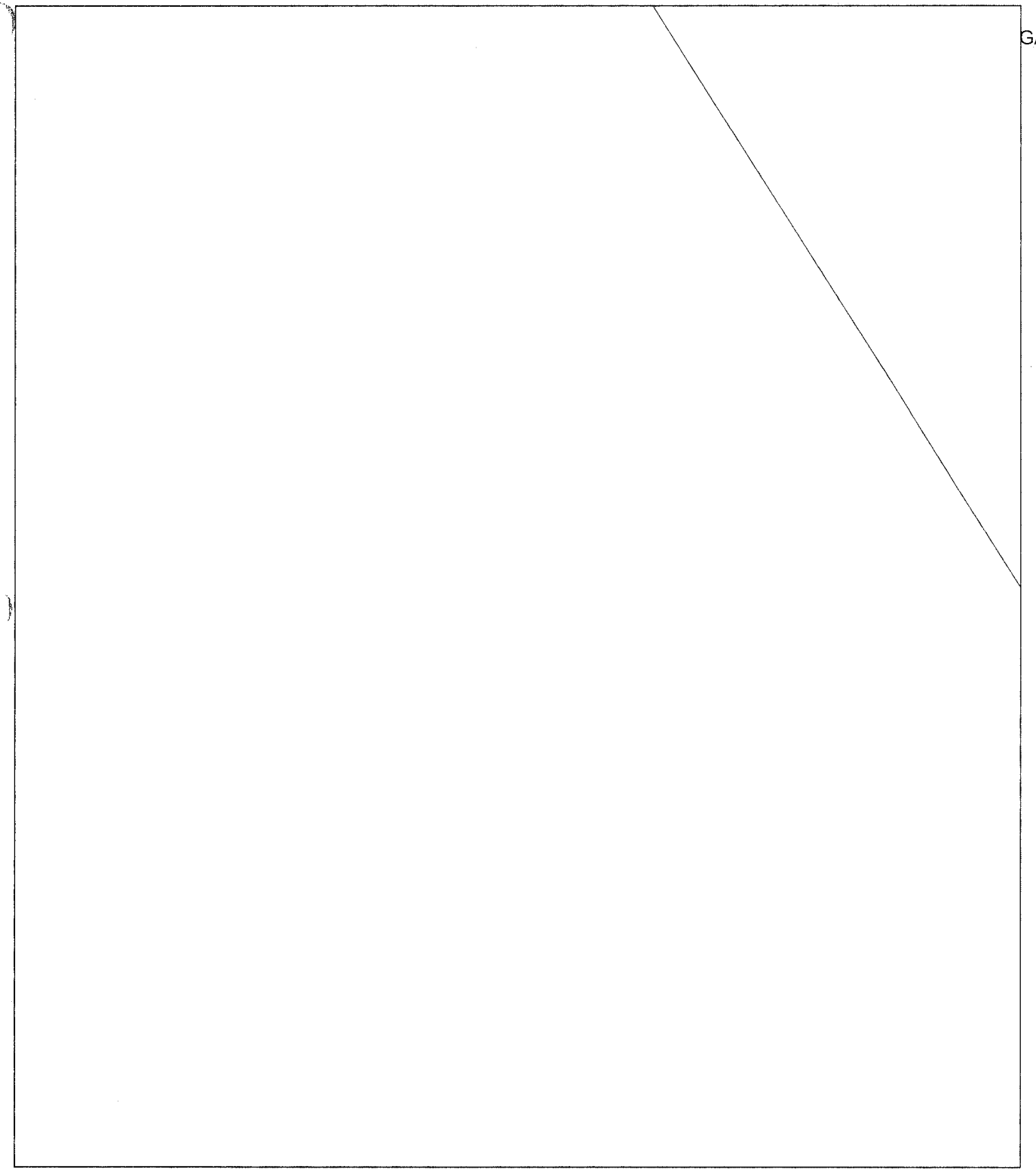


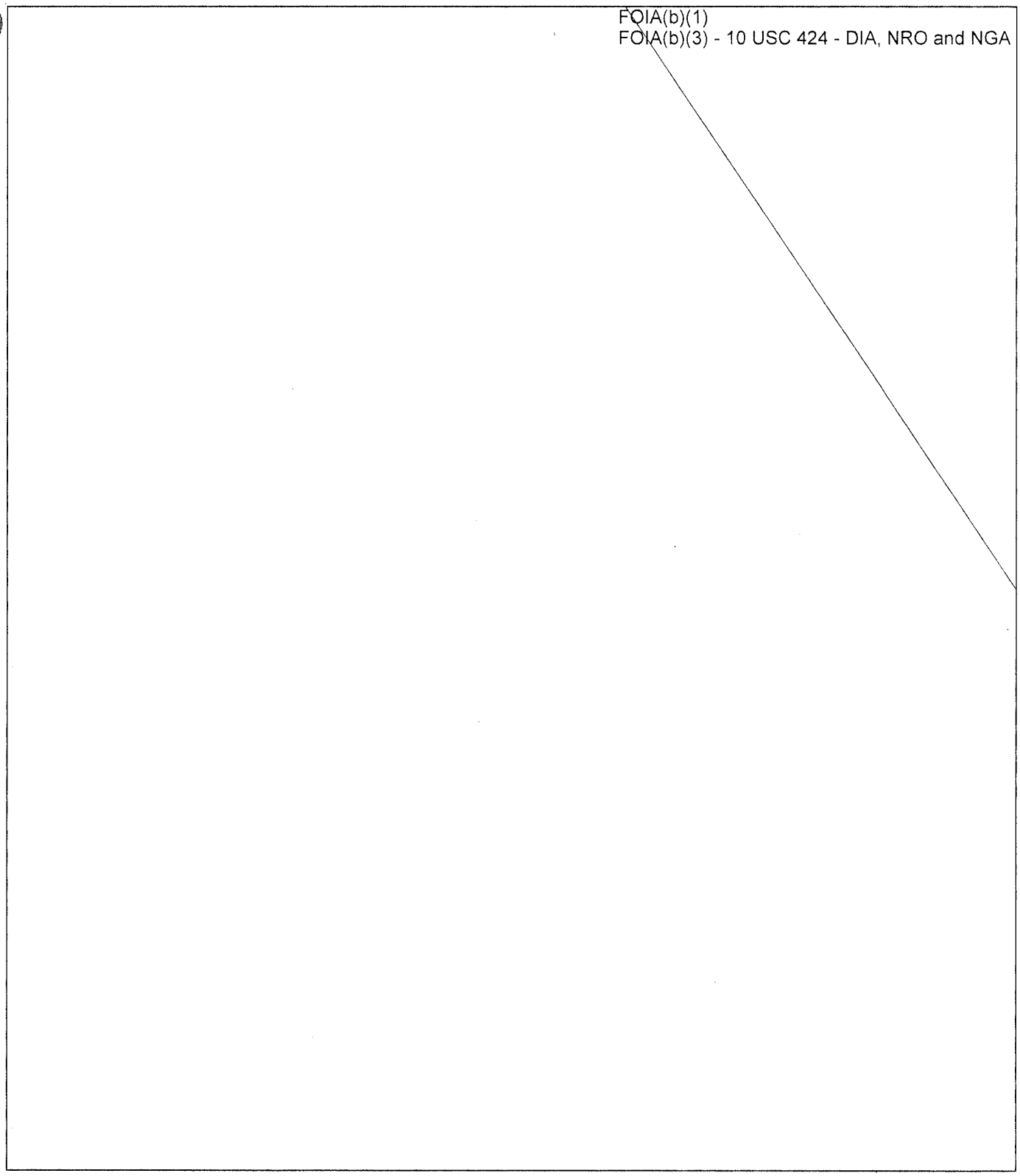
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

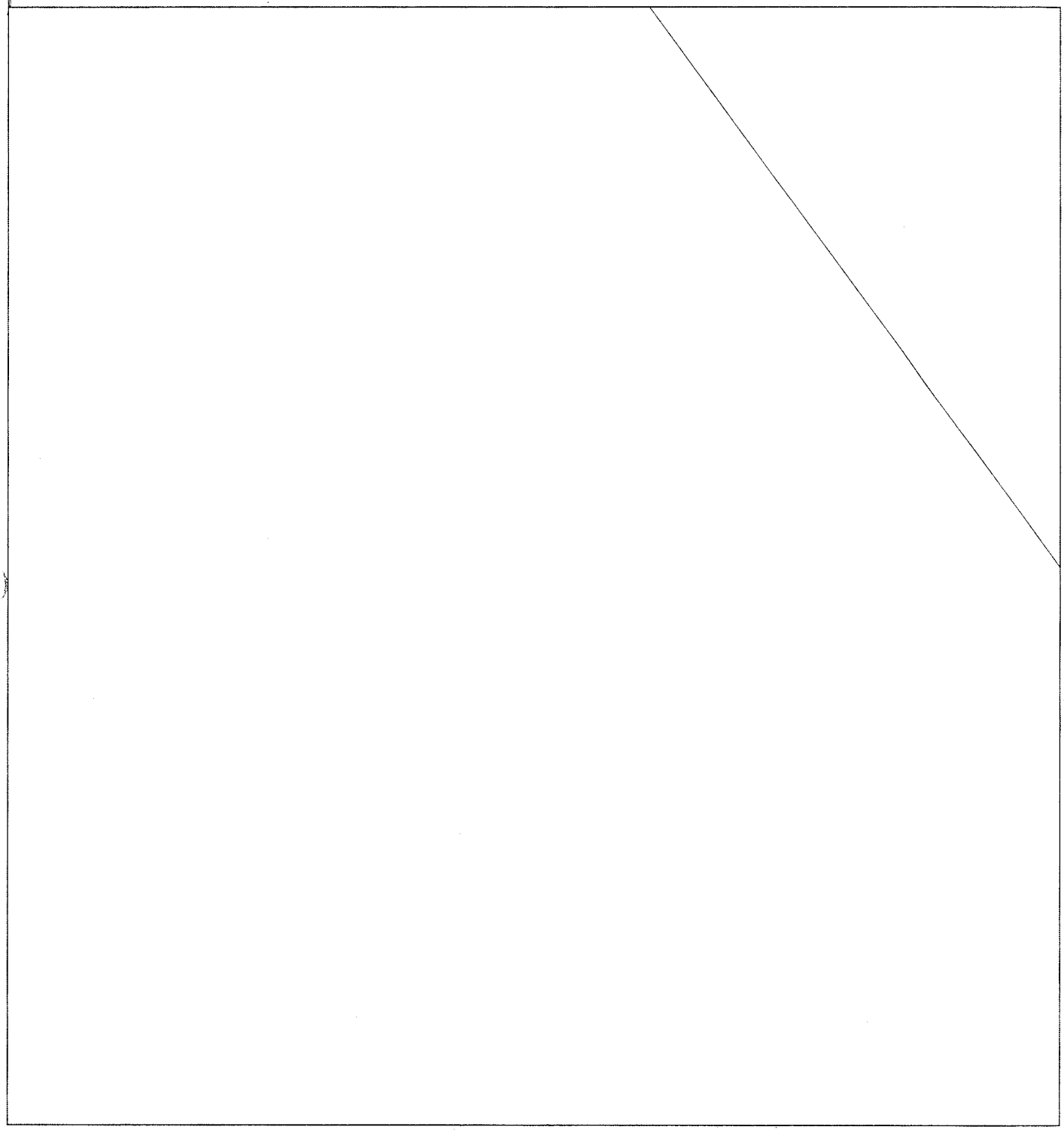
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

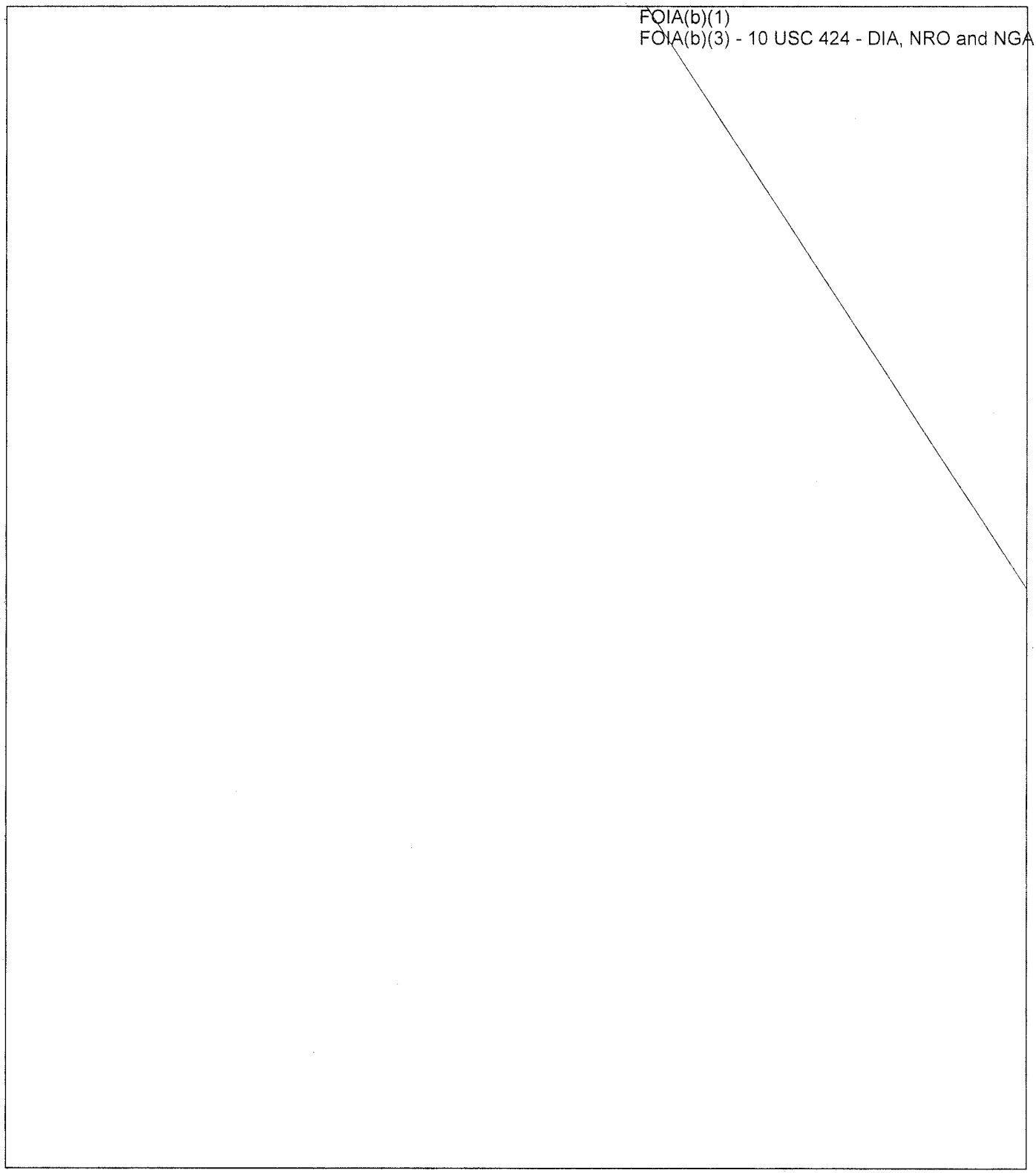

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

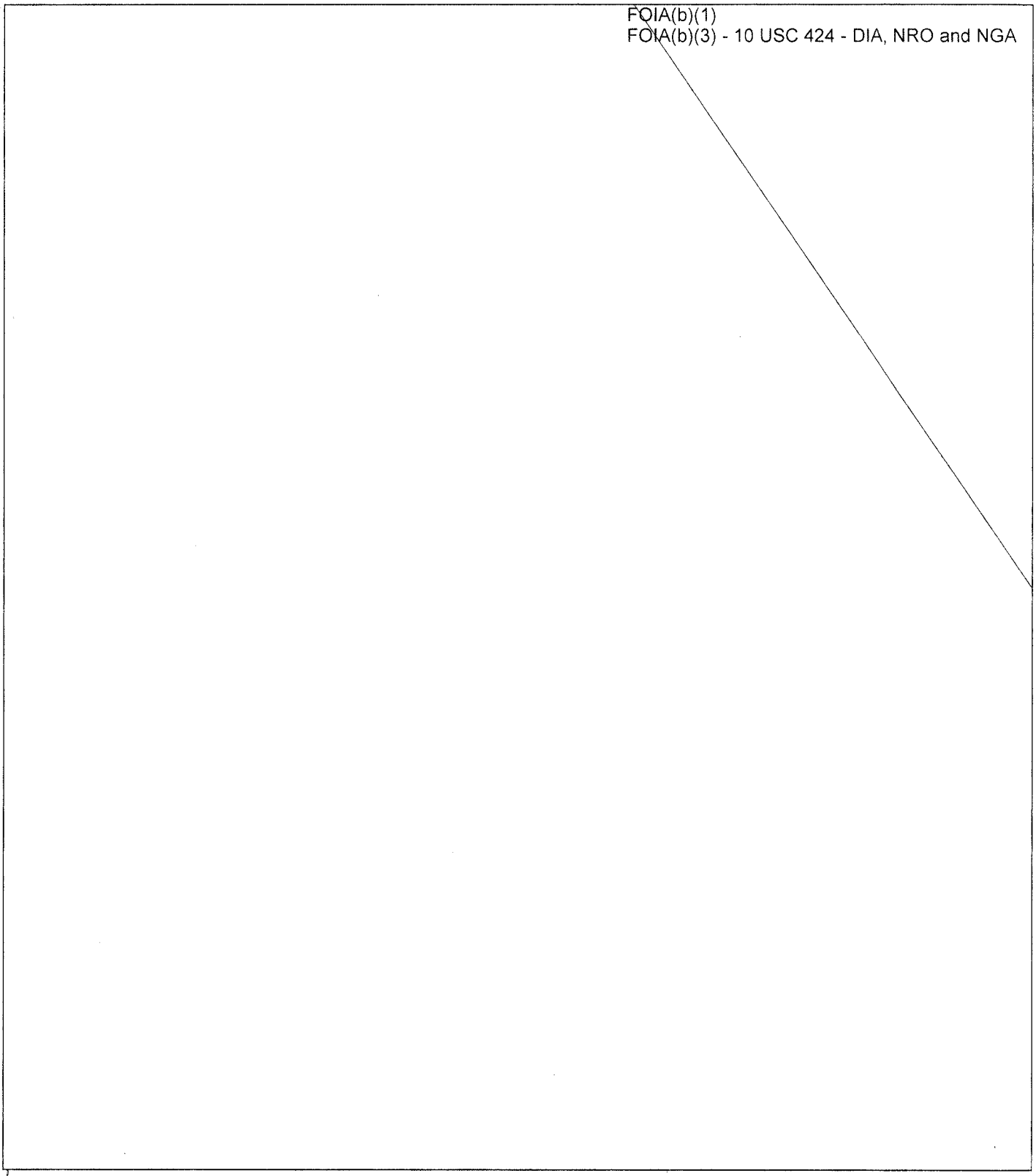

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

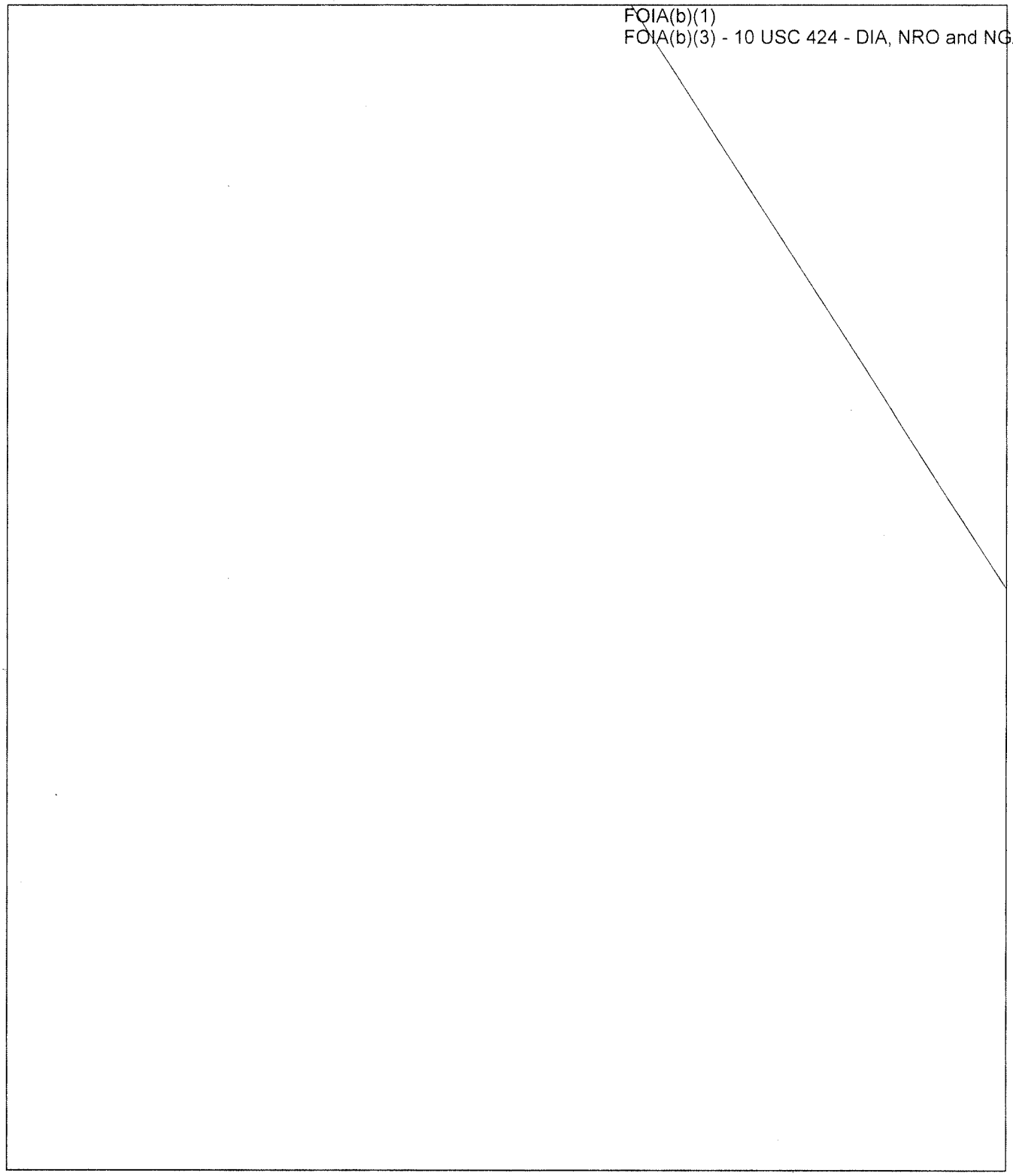


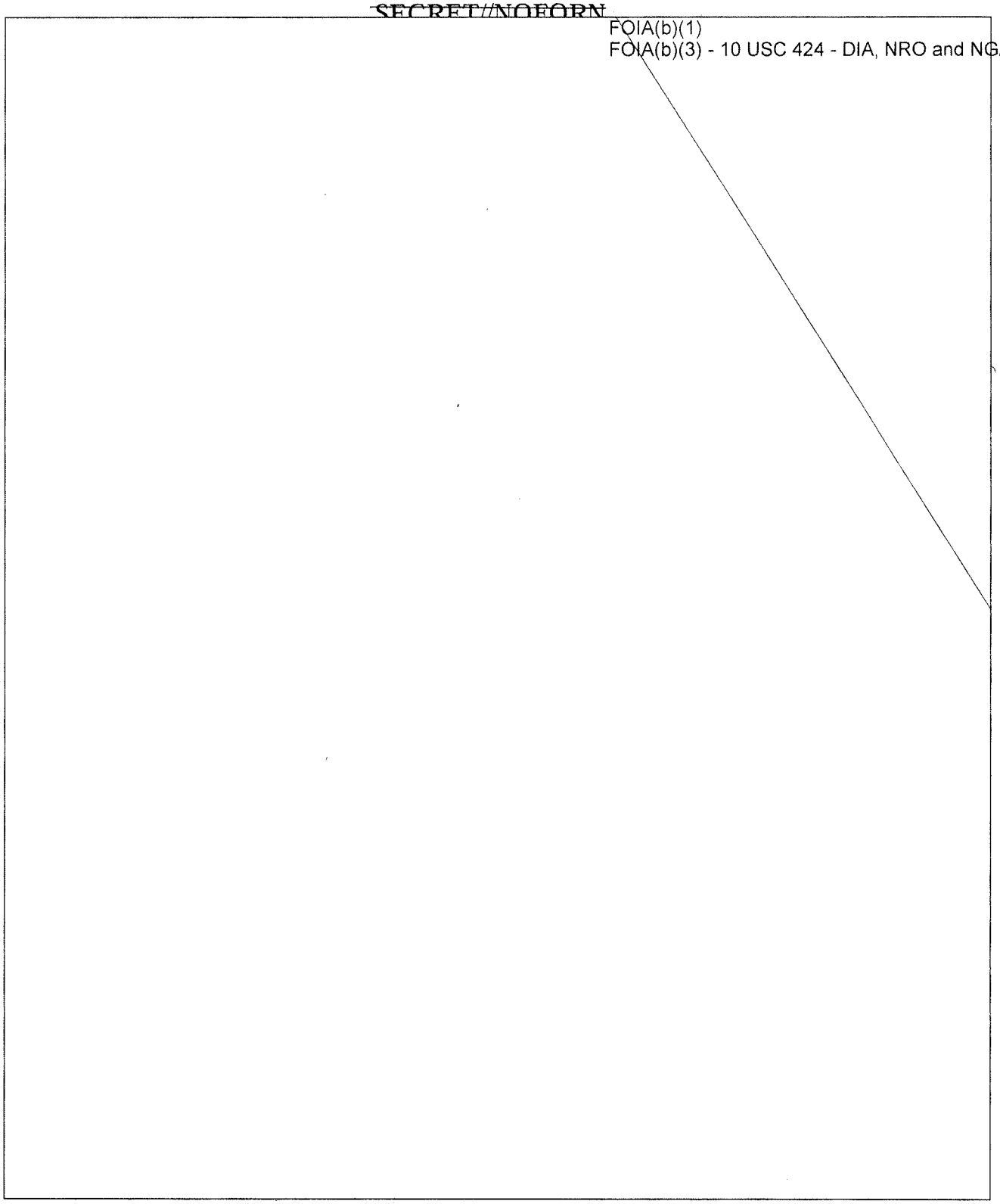

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

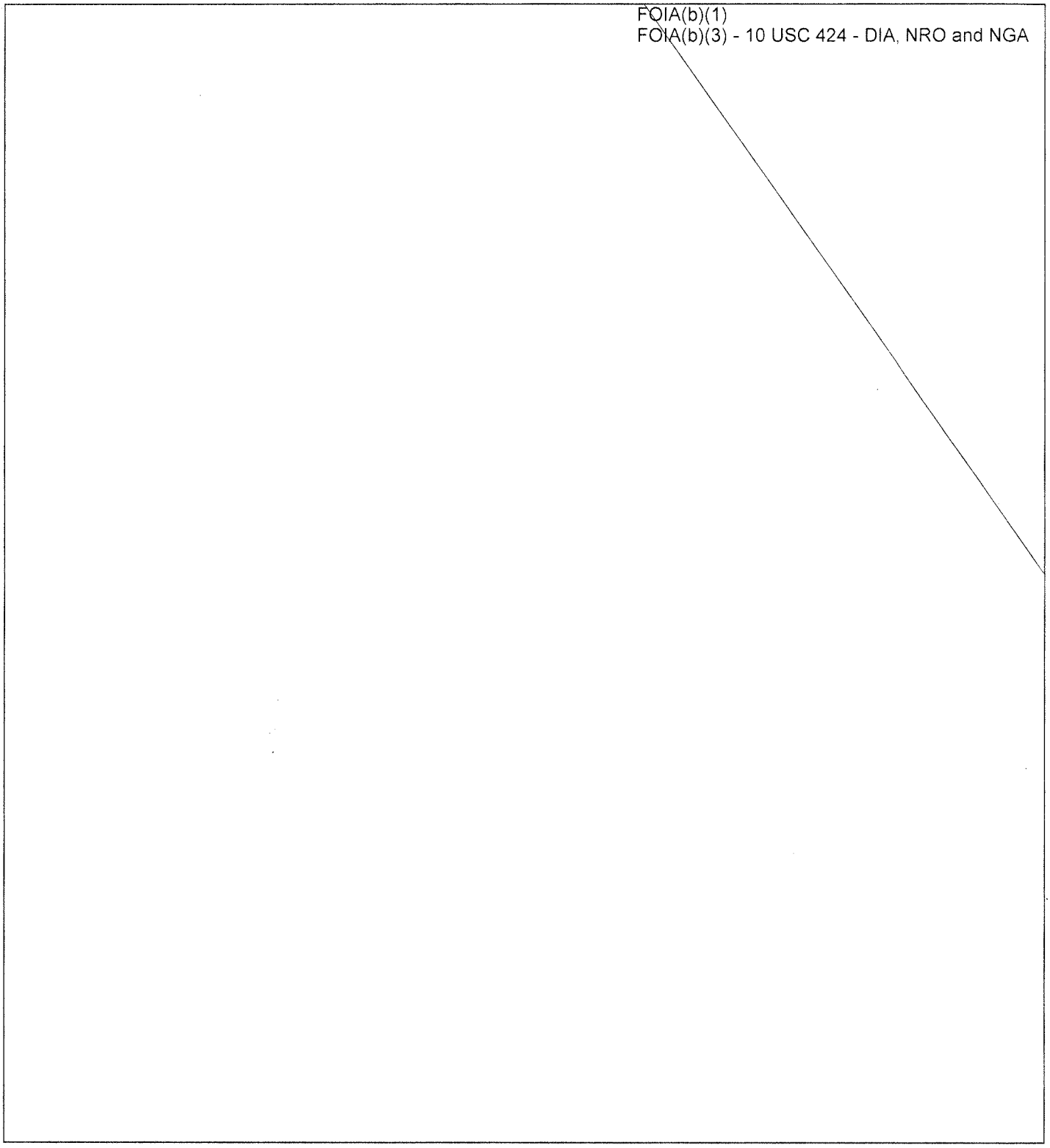




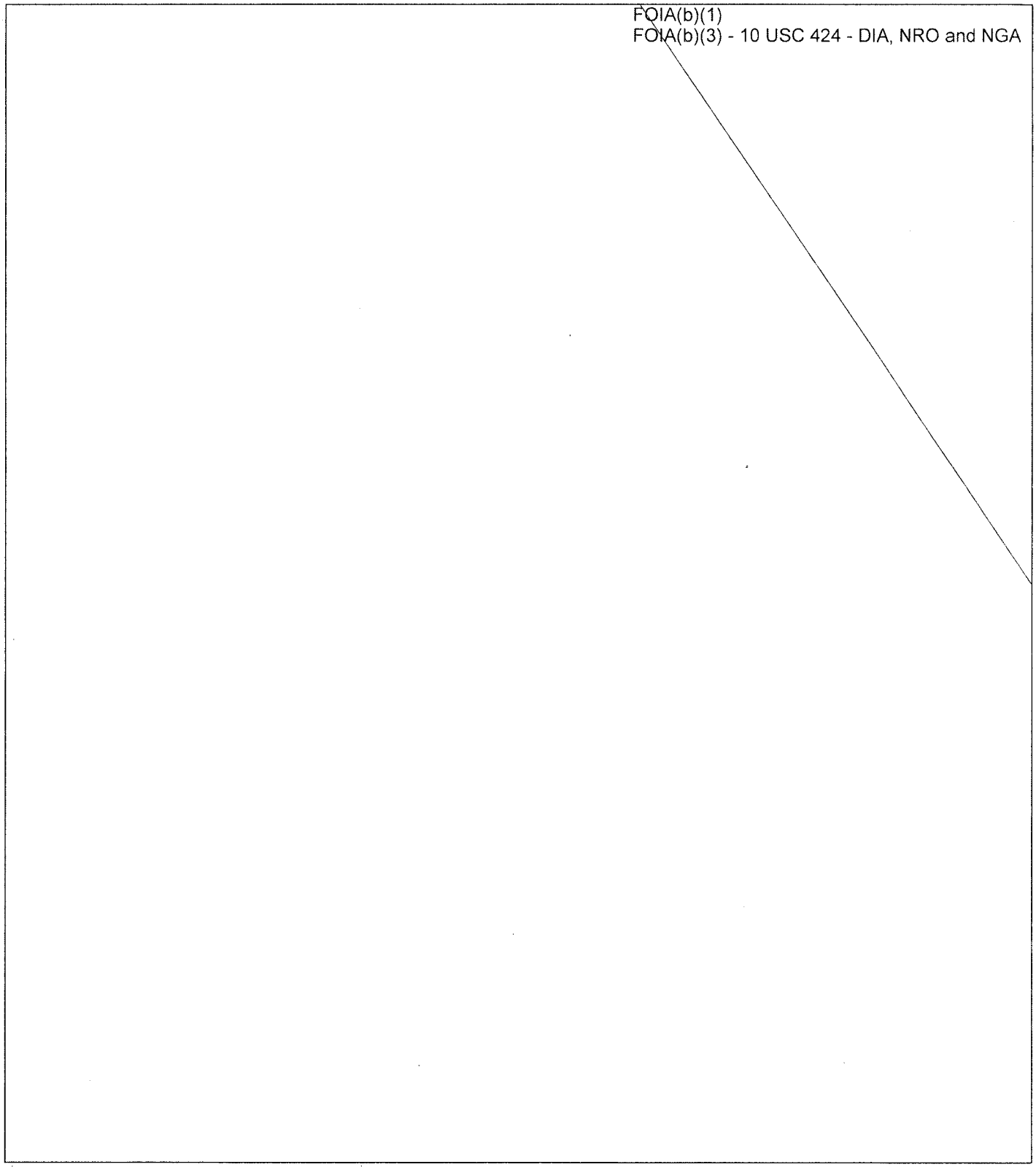

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA


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

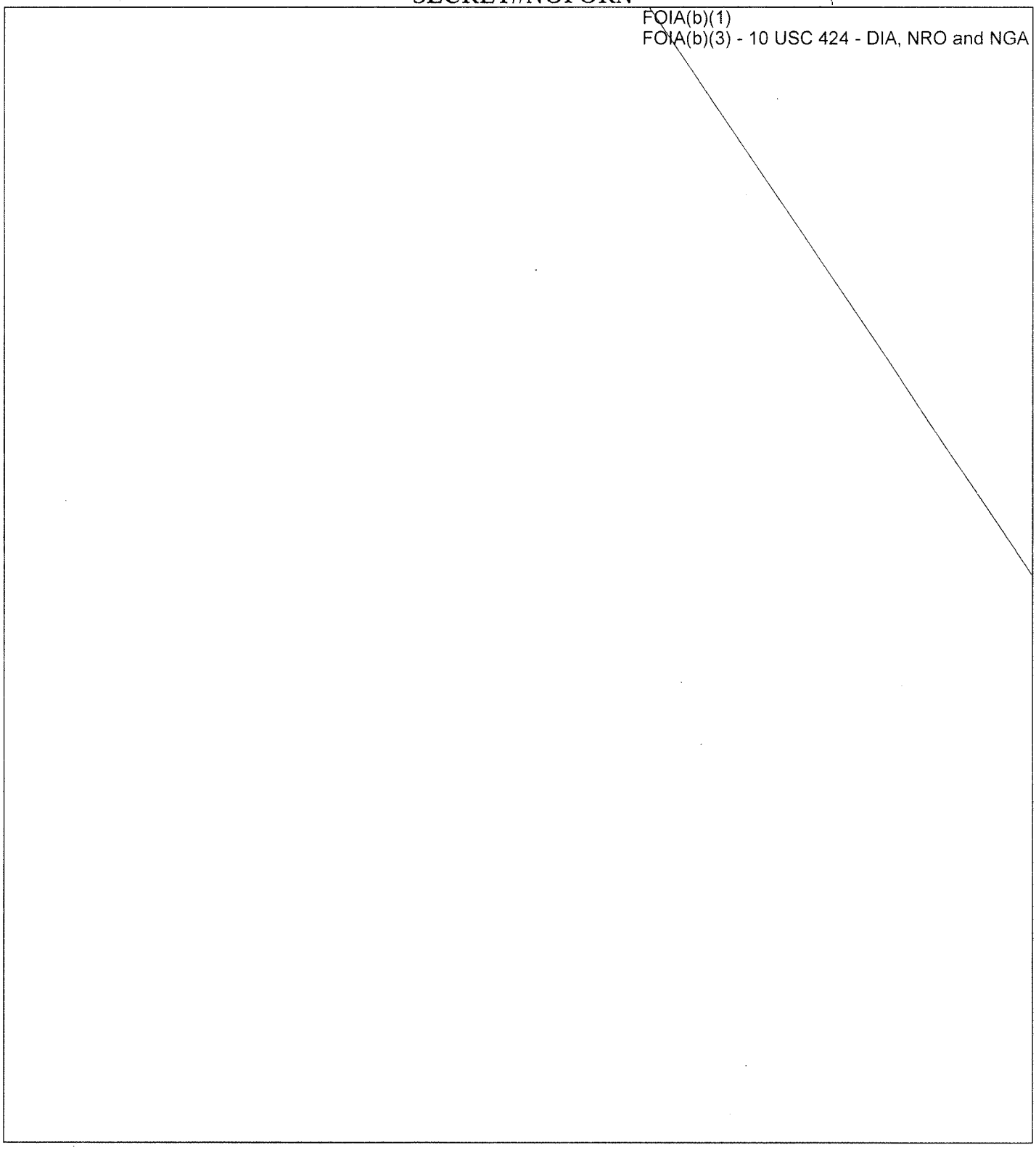



FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

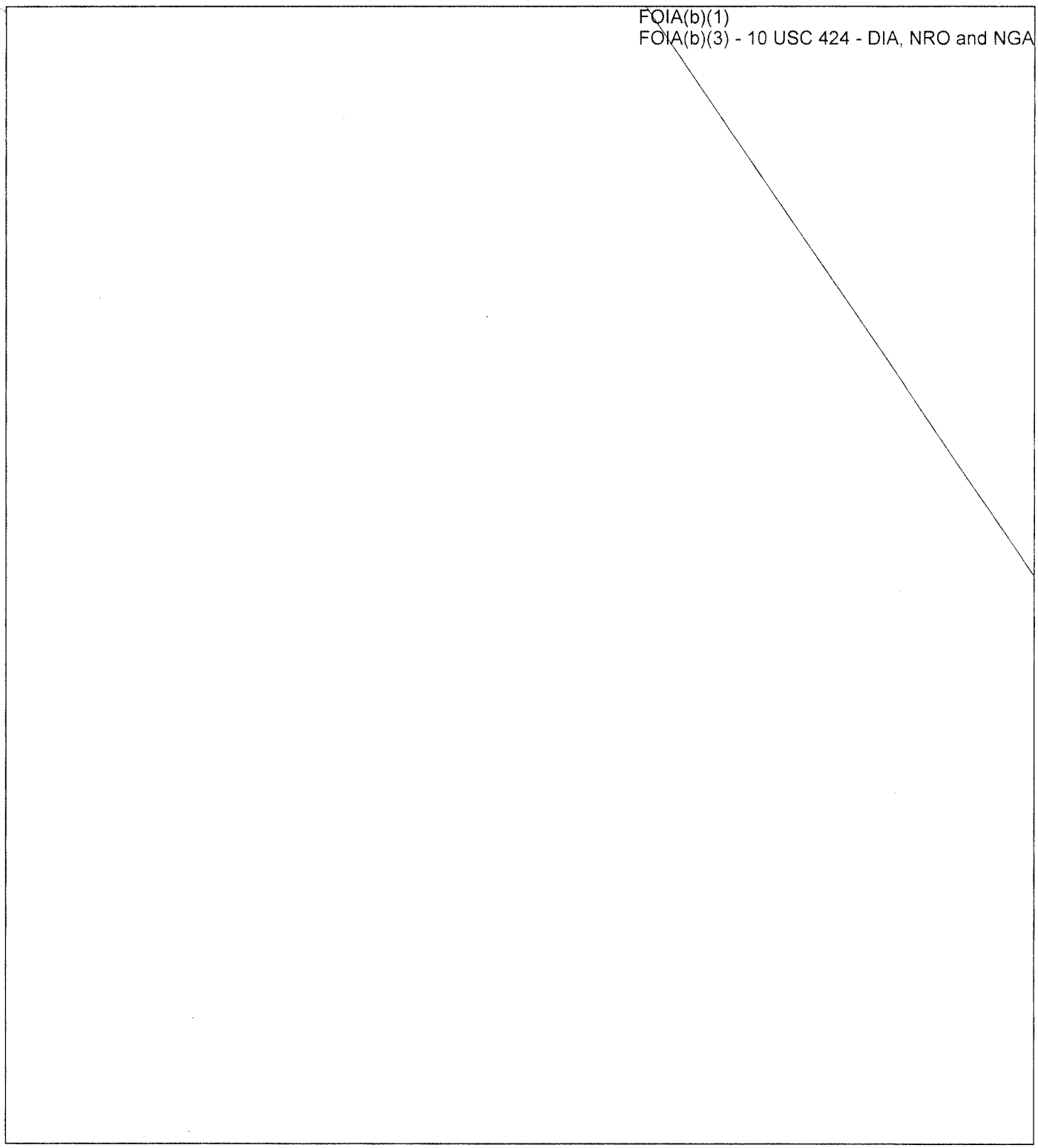
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

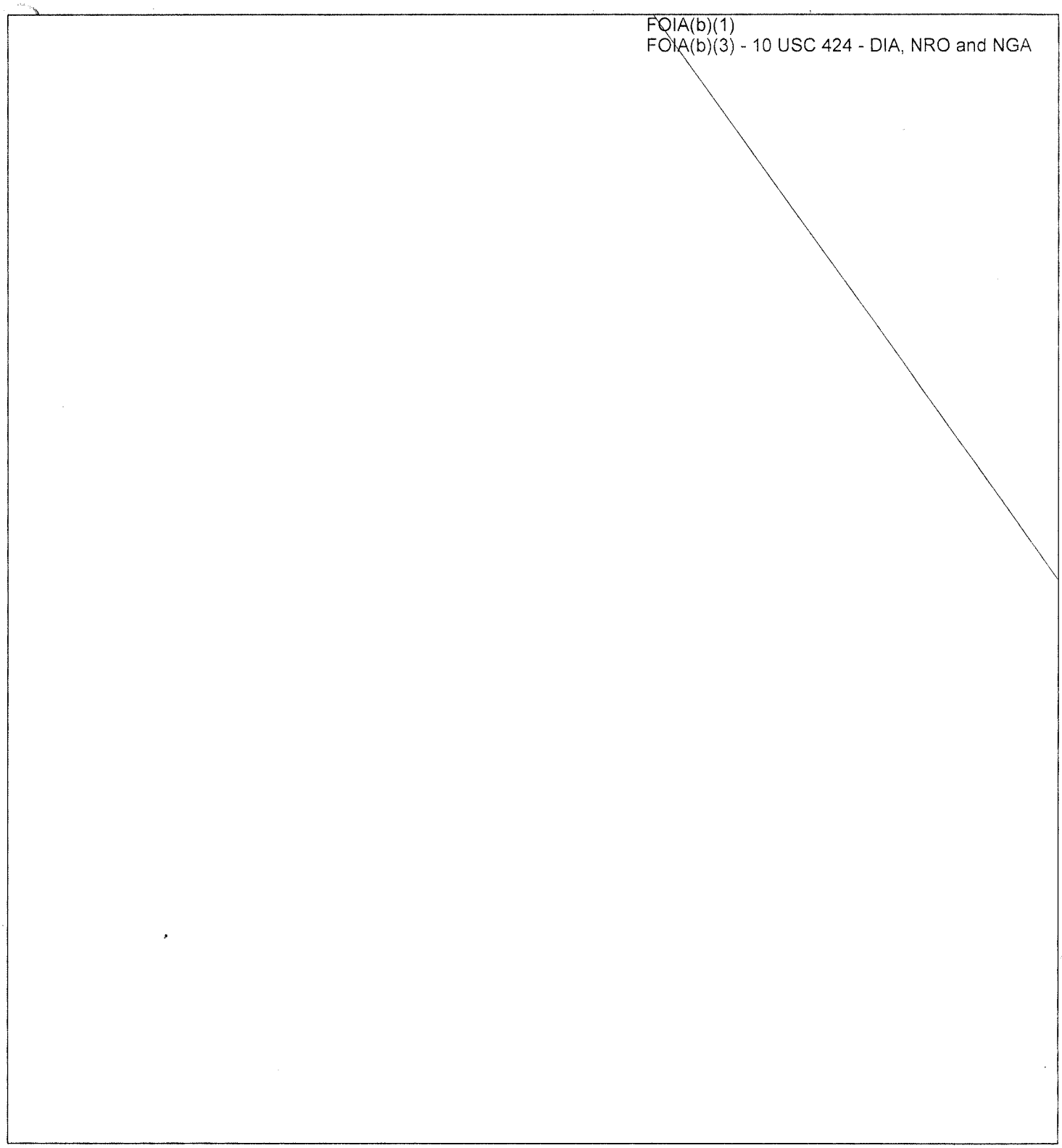


FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

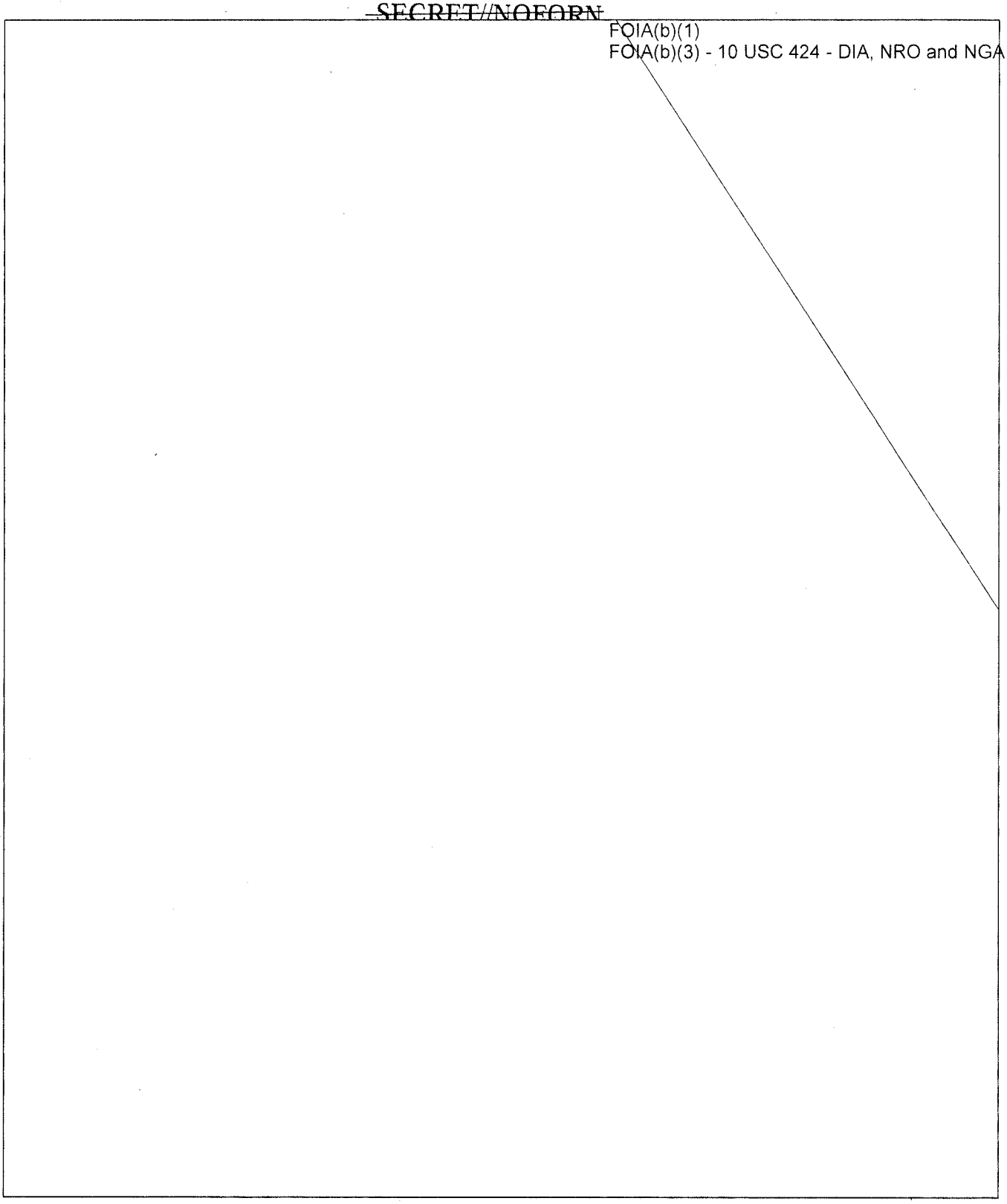


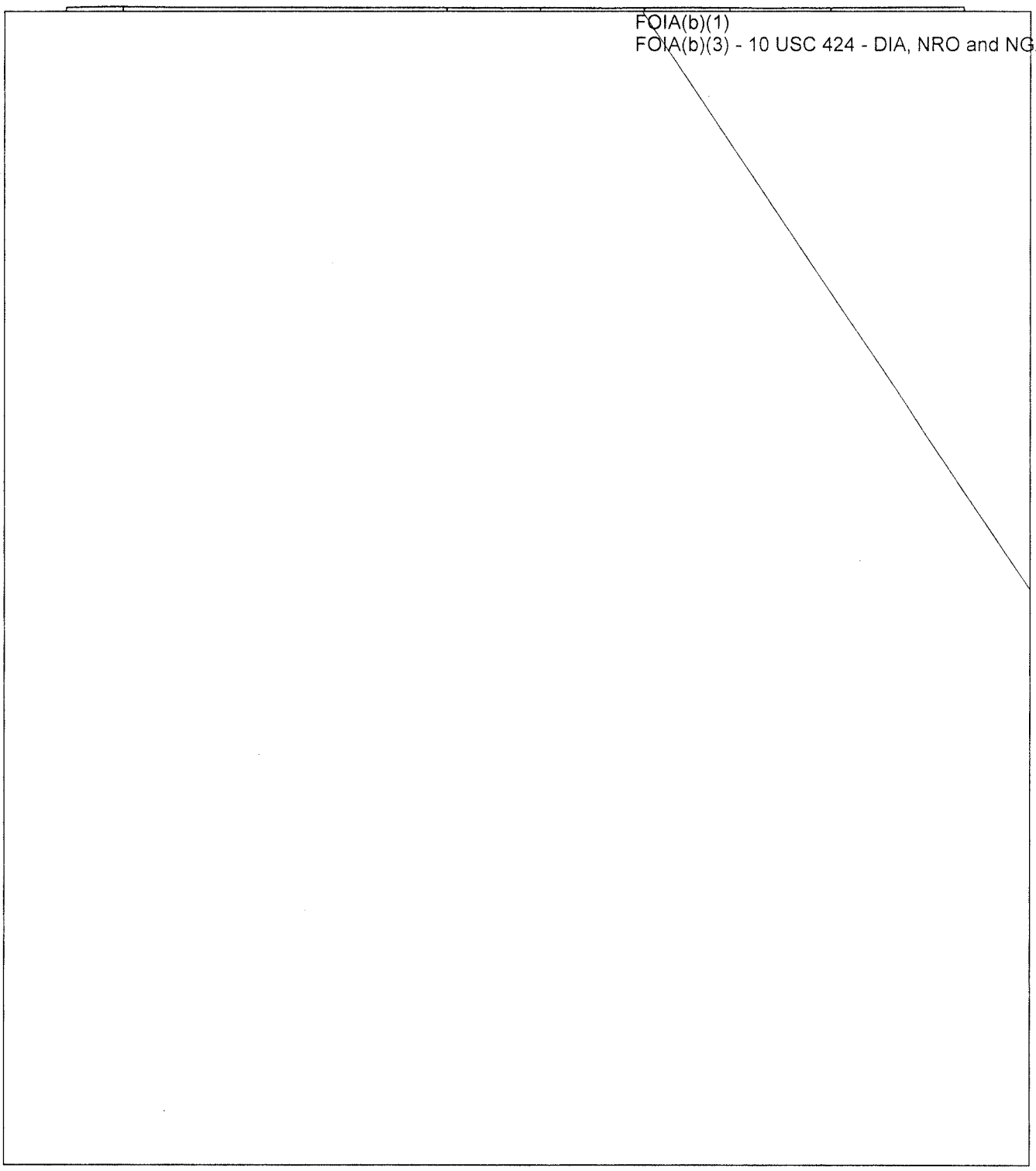
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

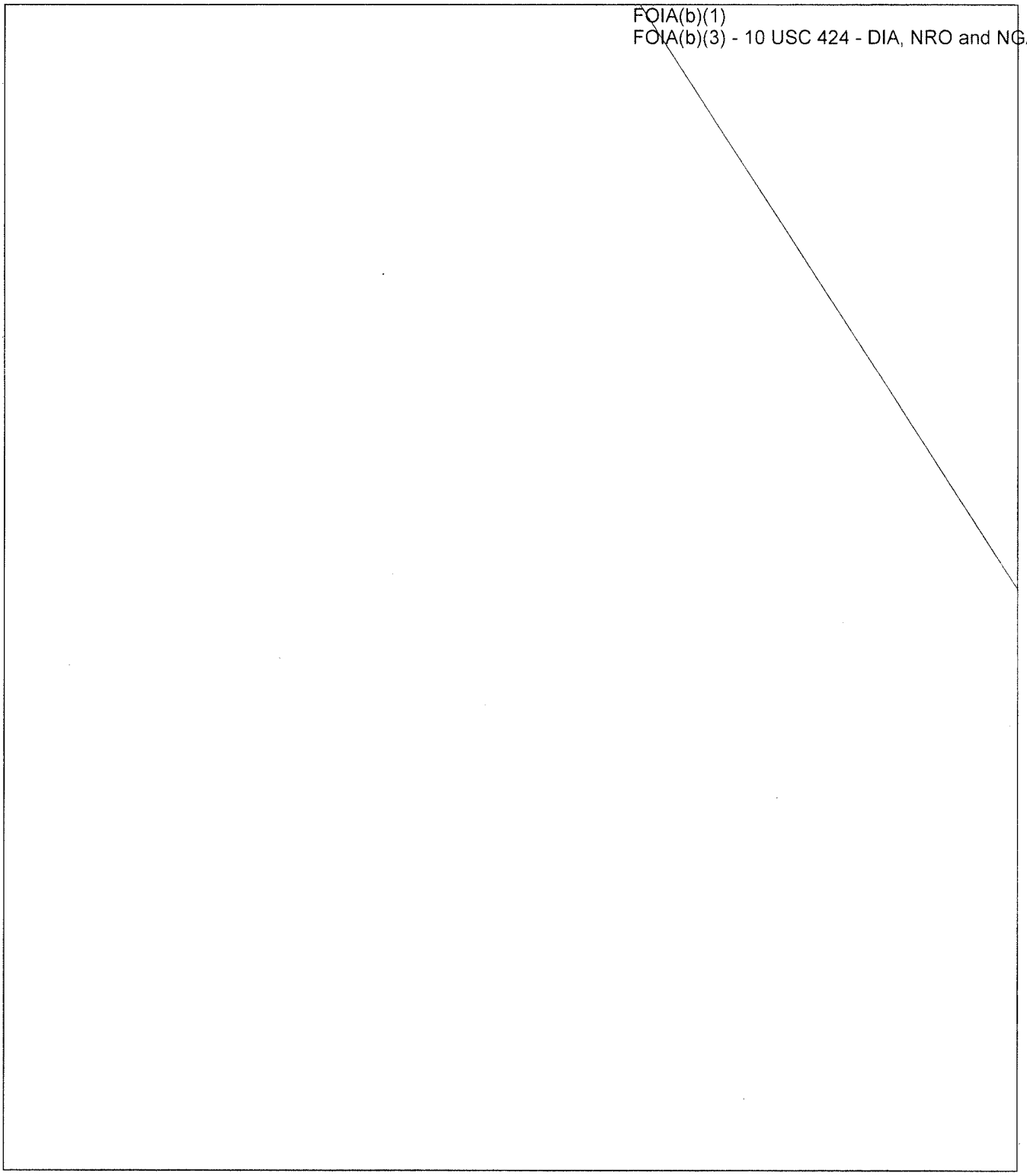

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

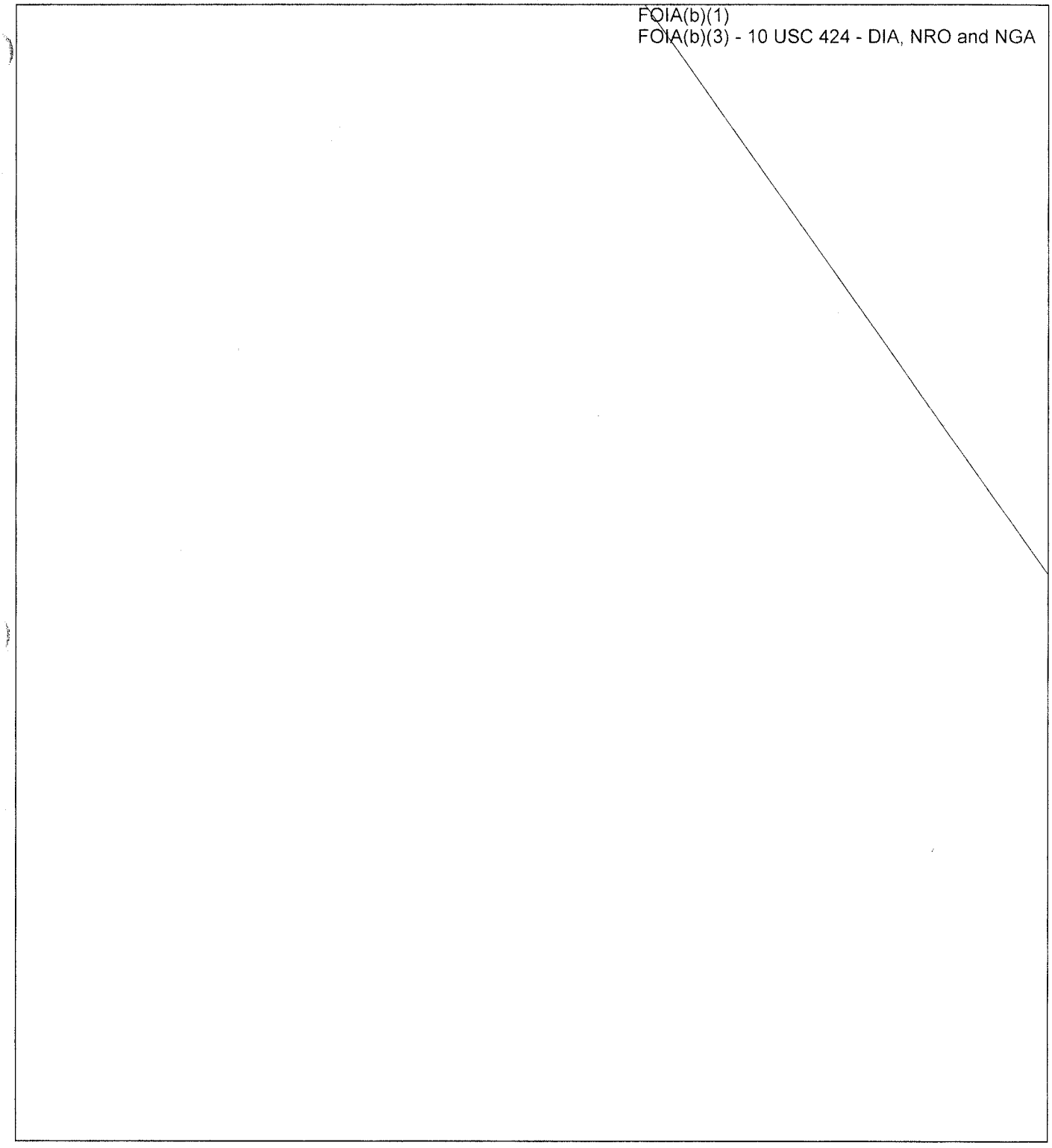

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

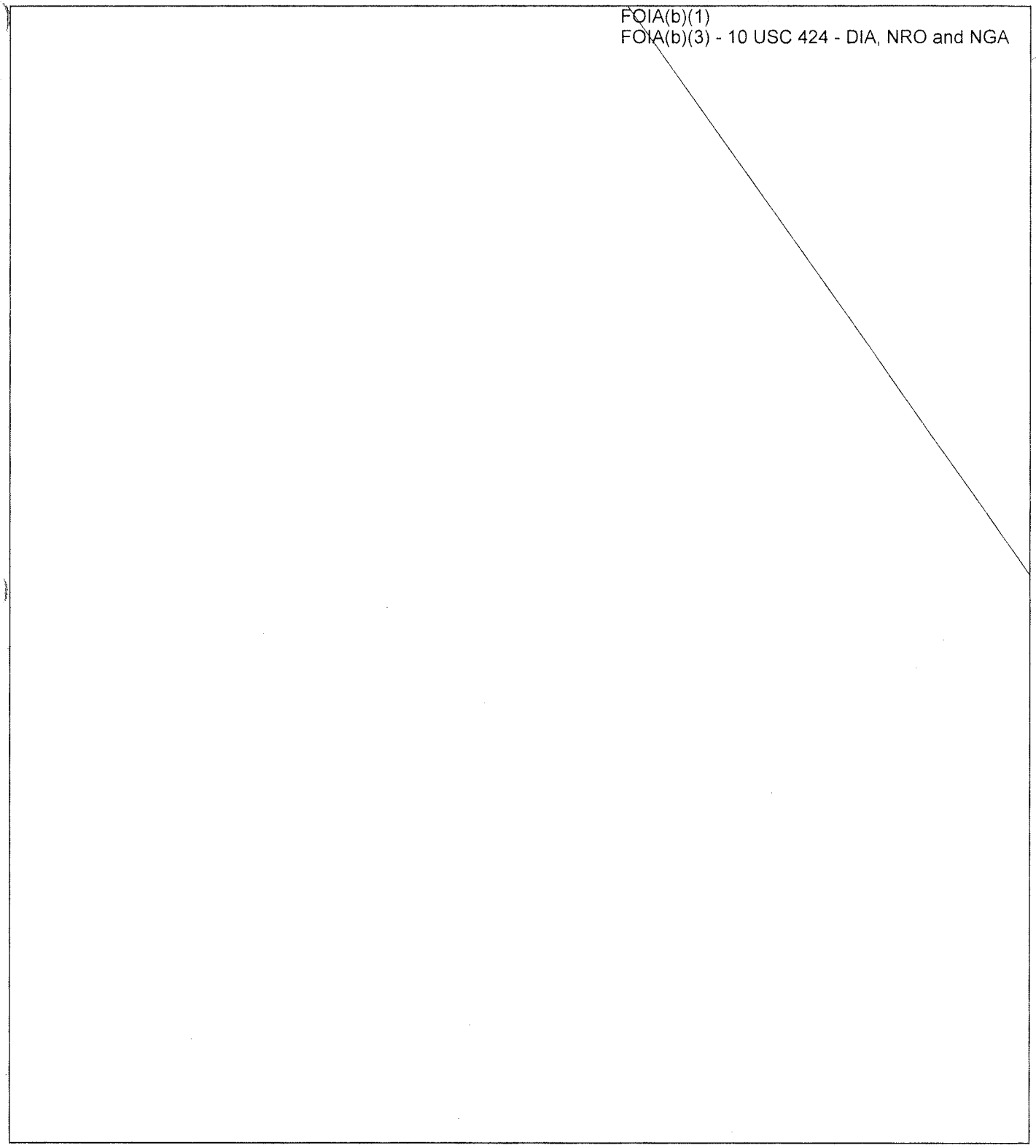
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

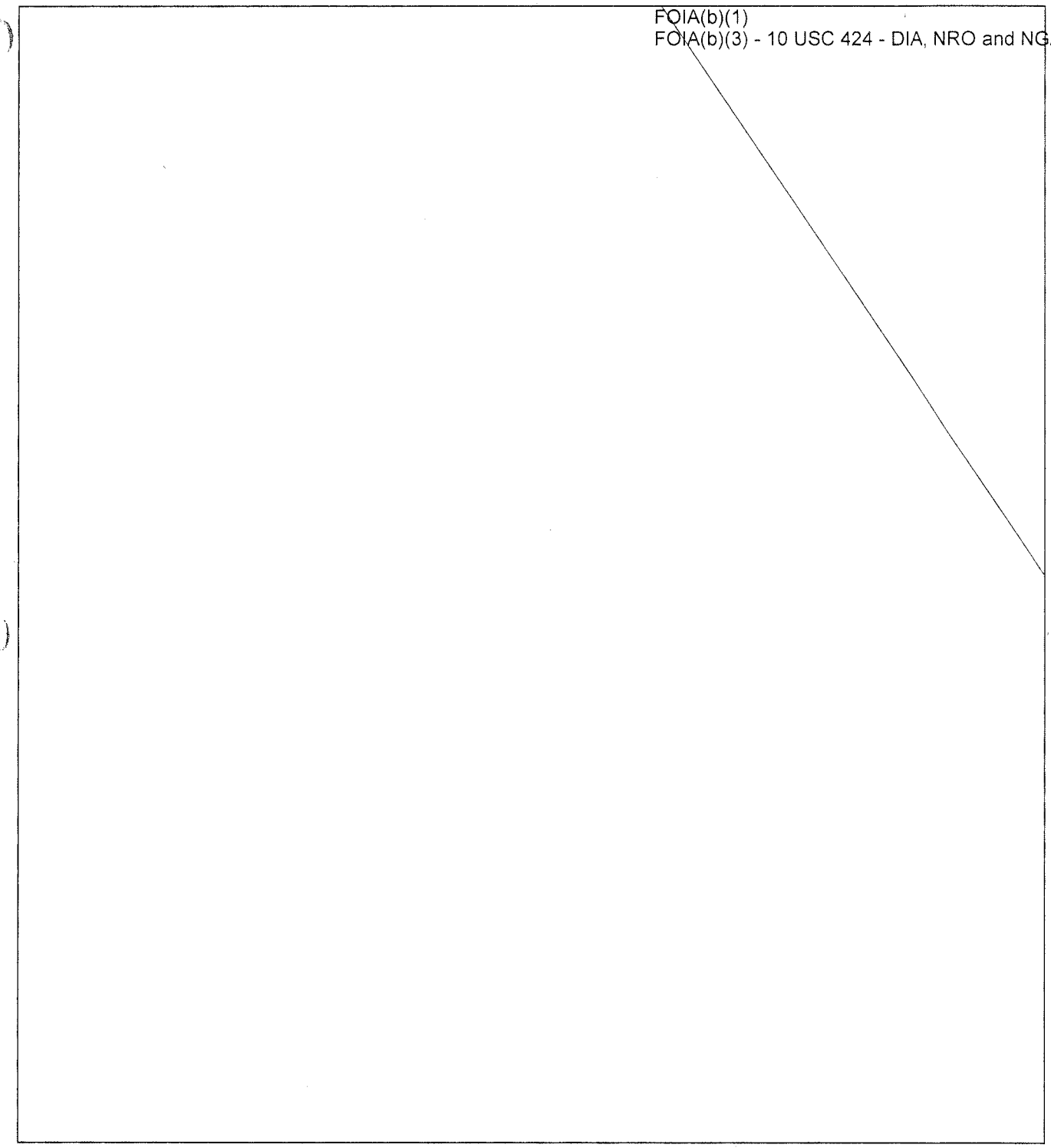


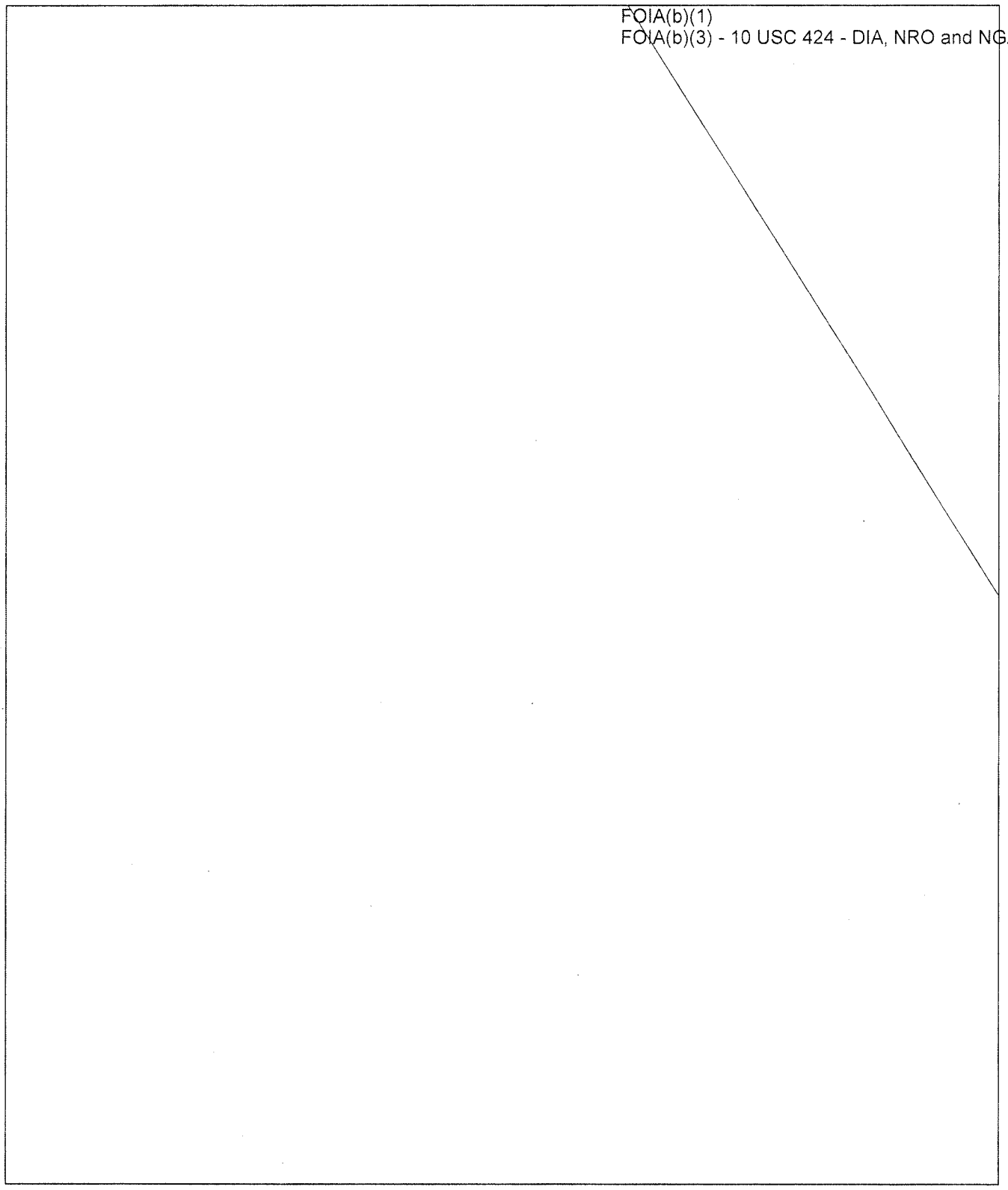


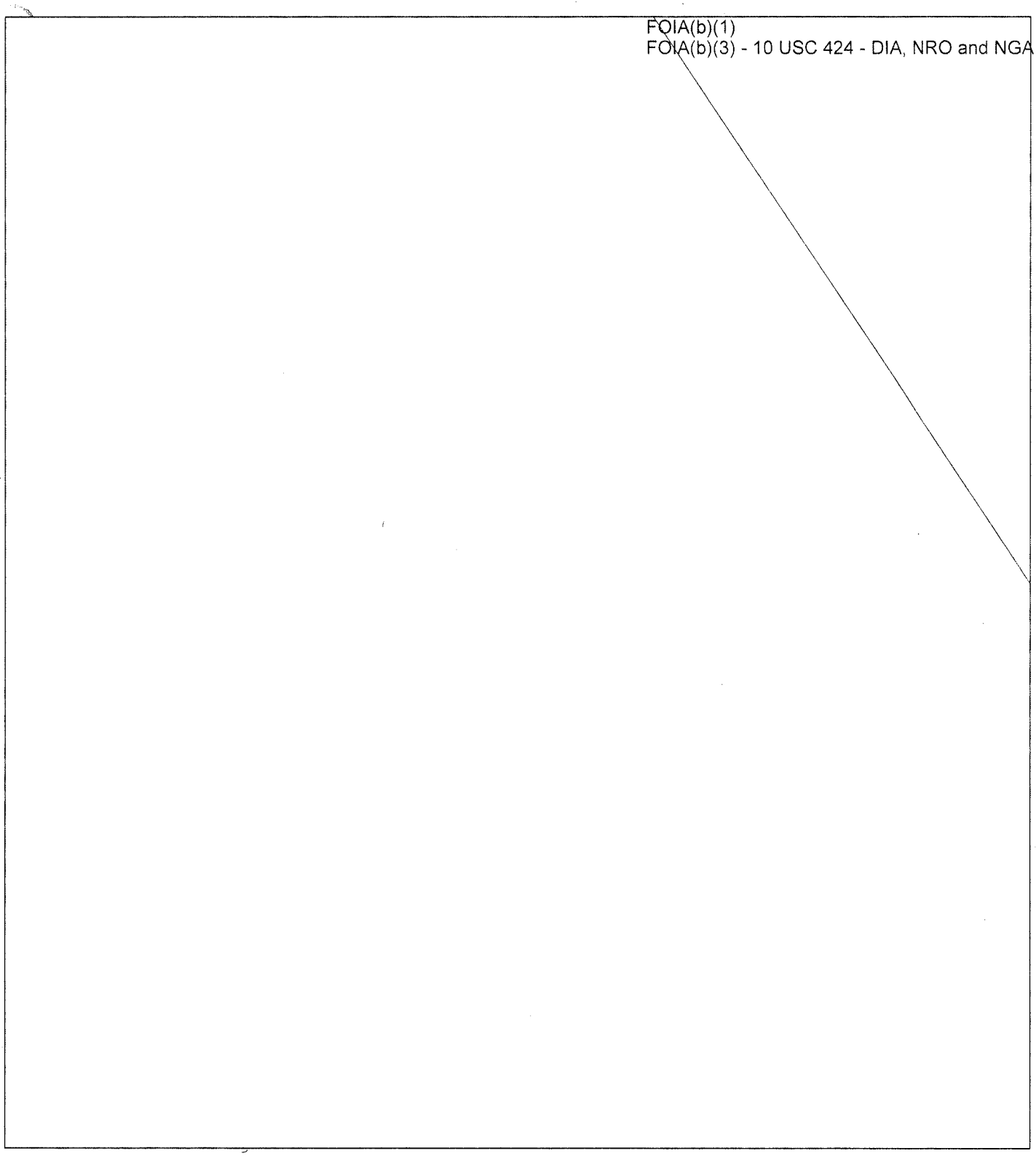

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

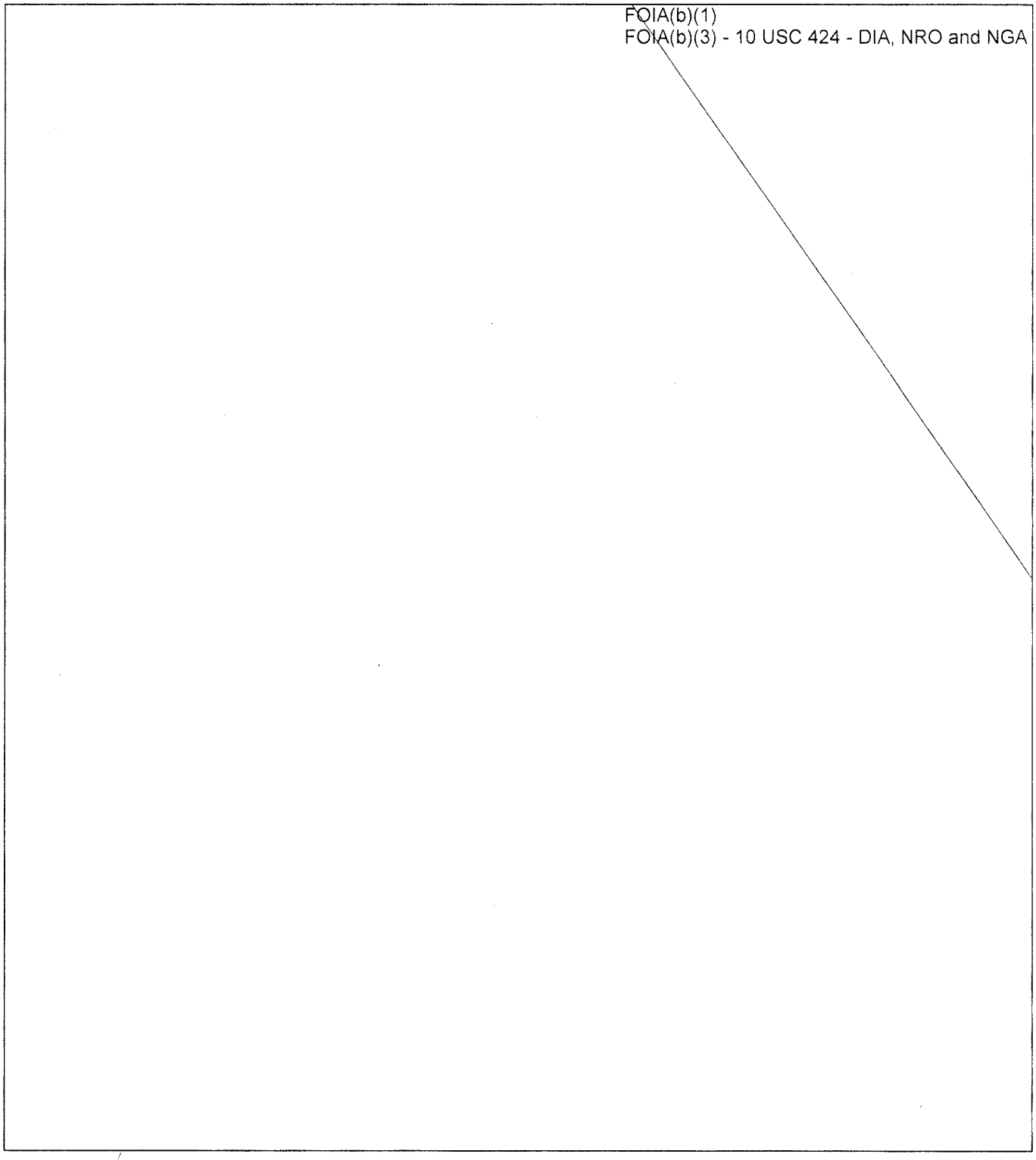


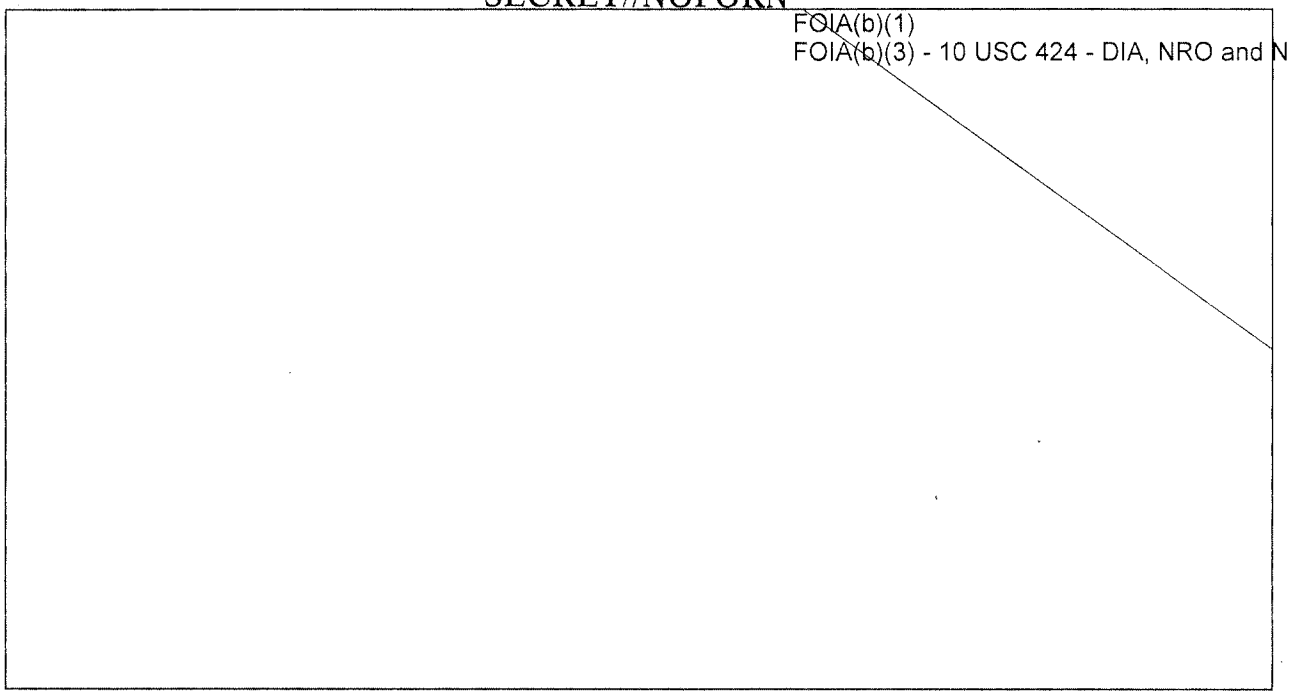

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA


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

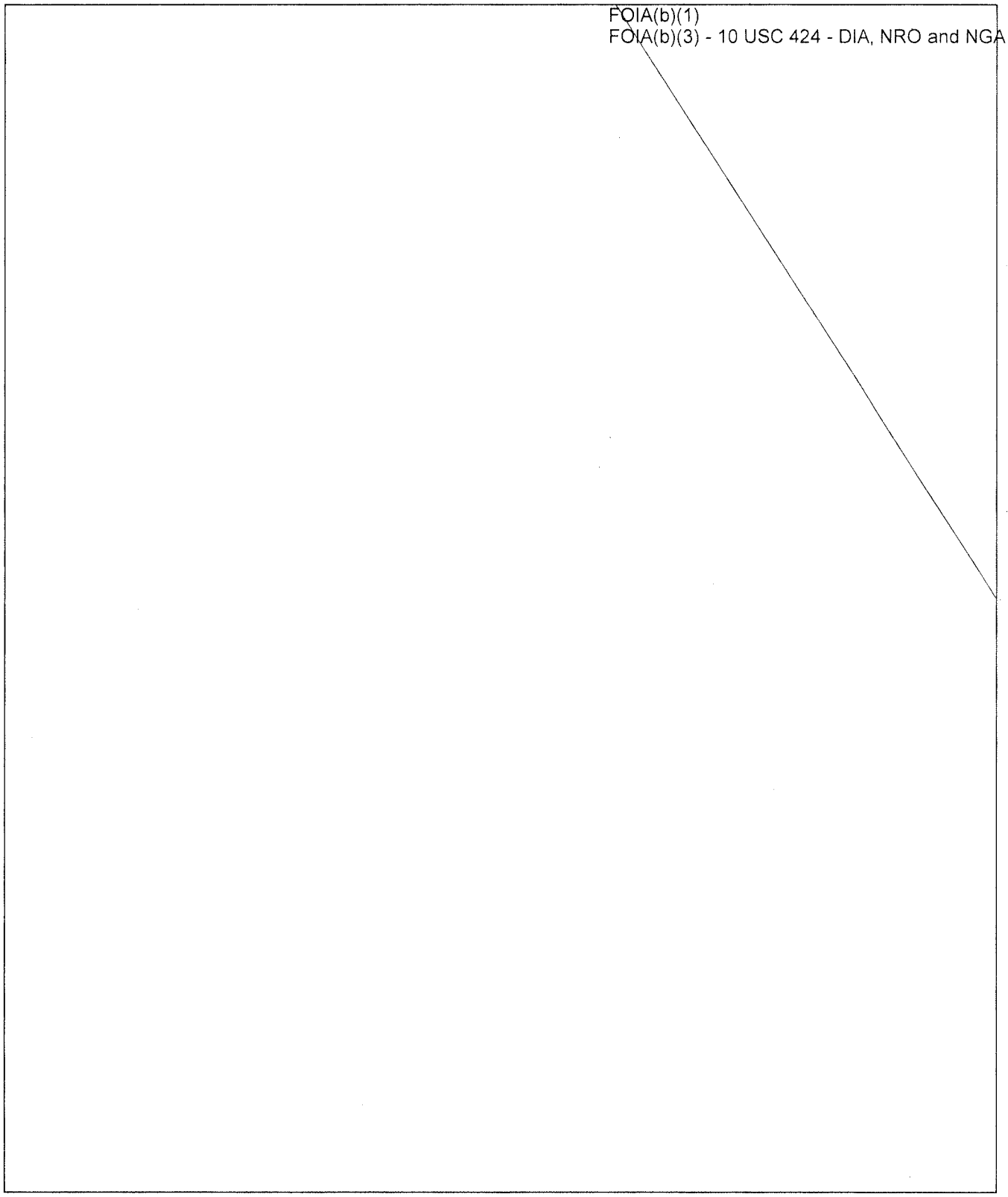

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

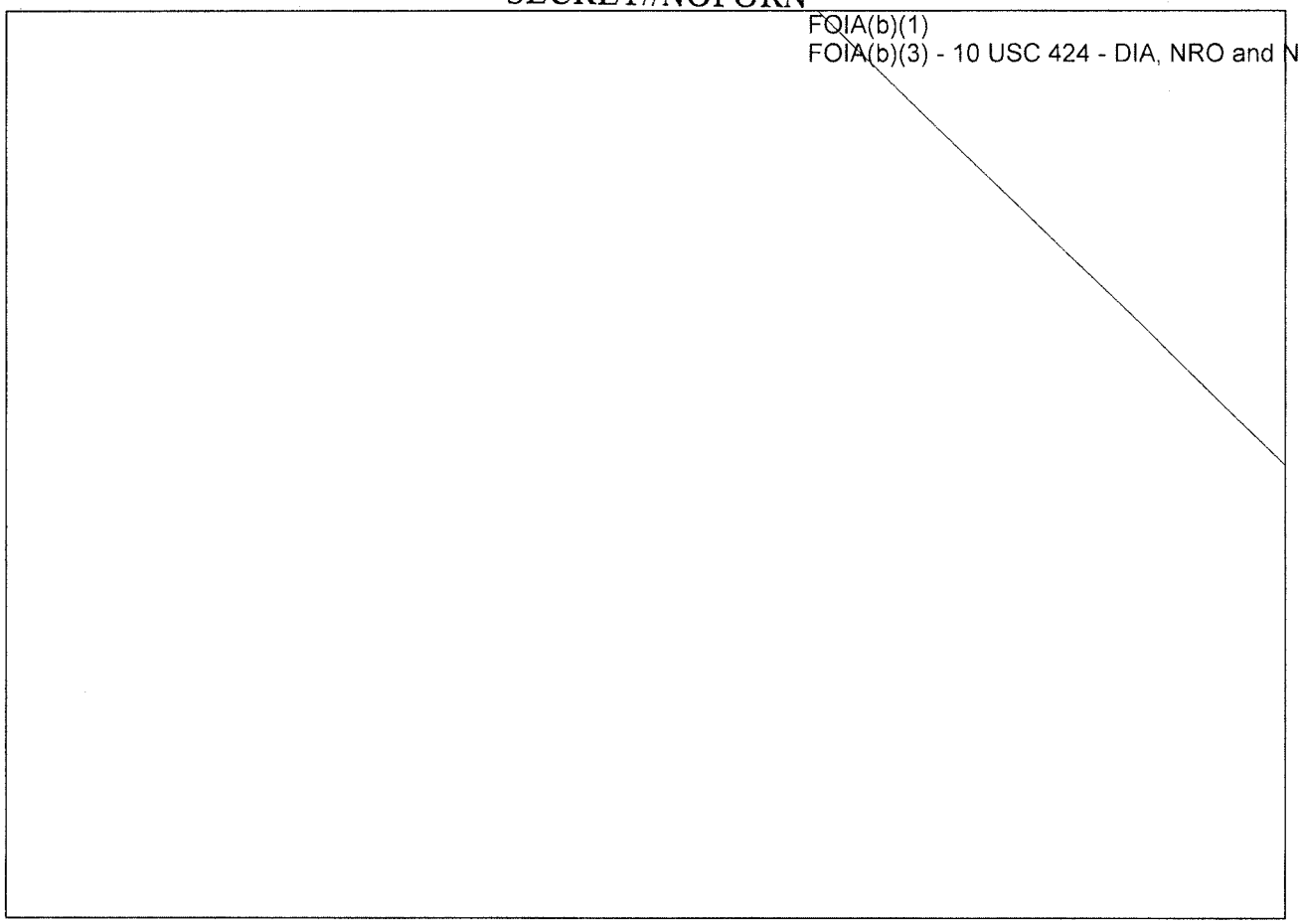

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA


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

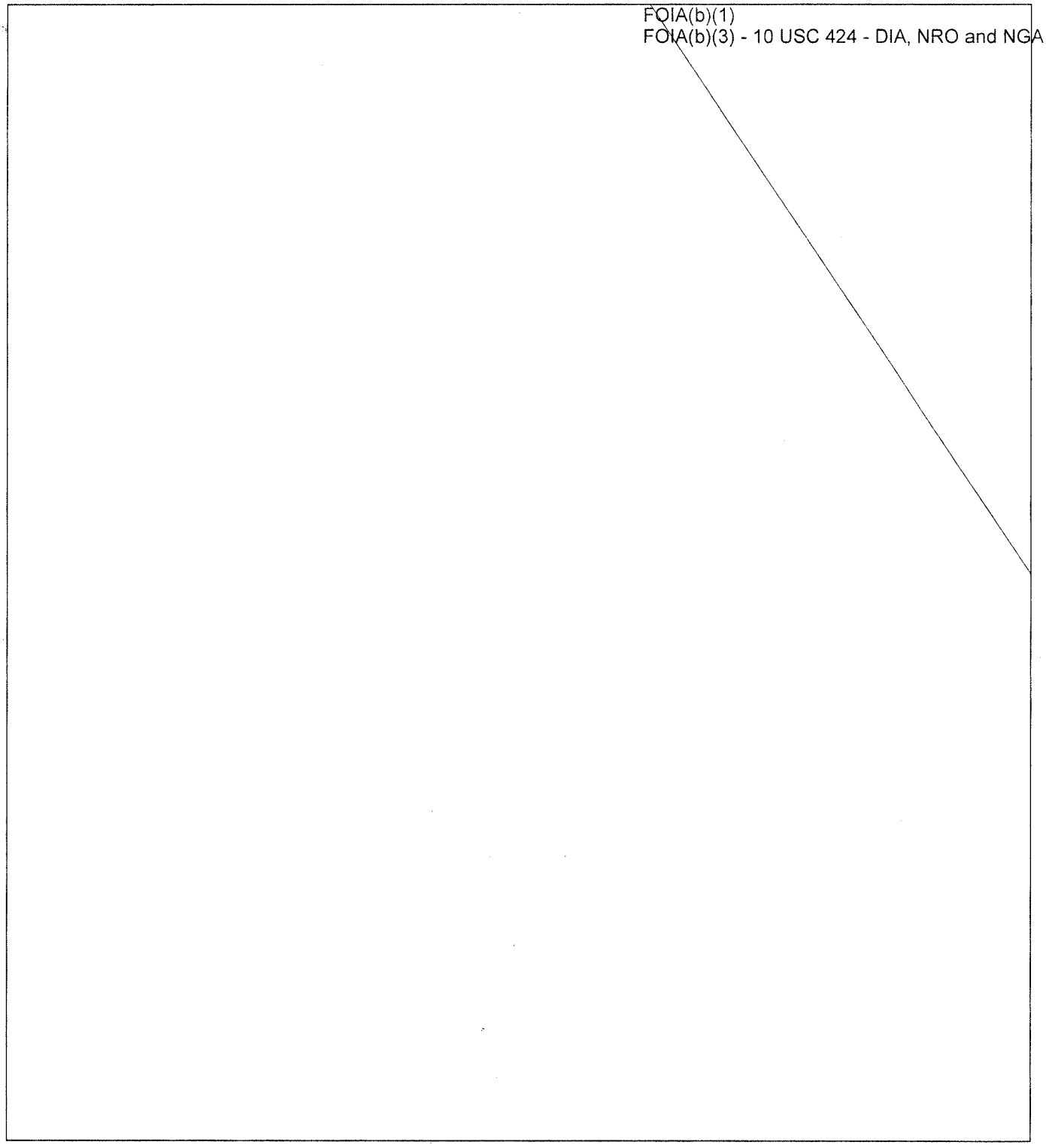

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

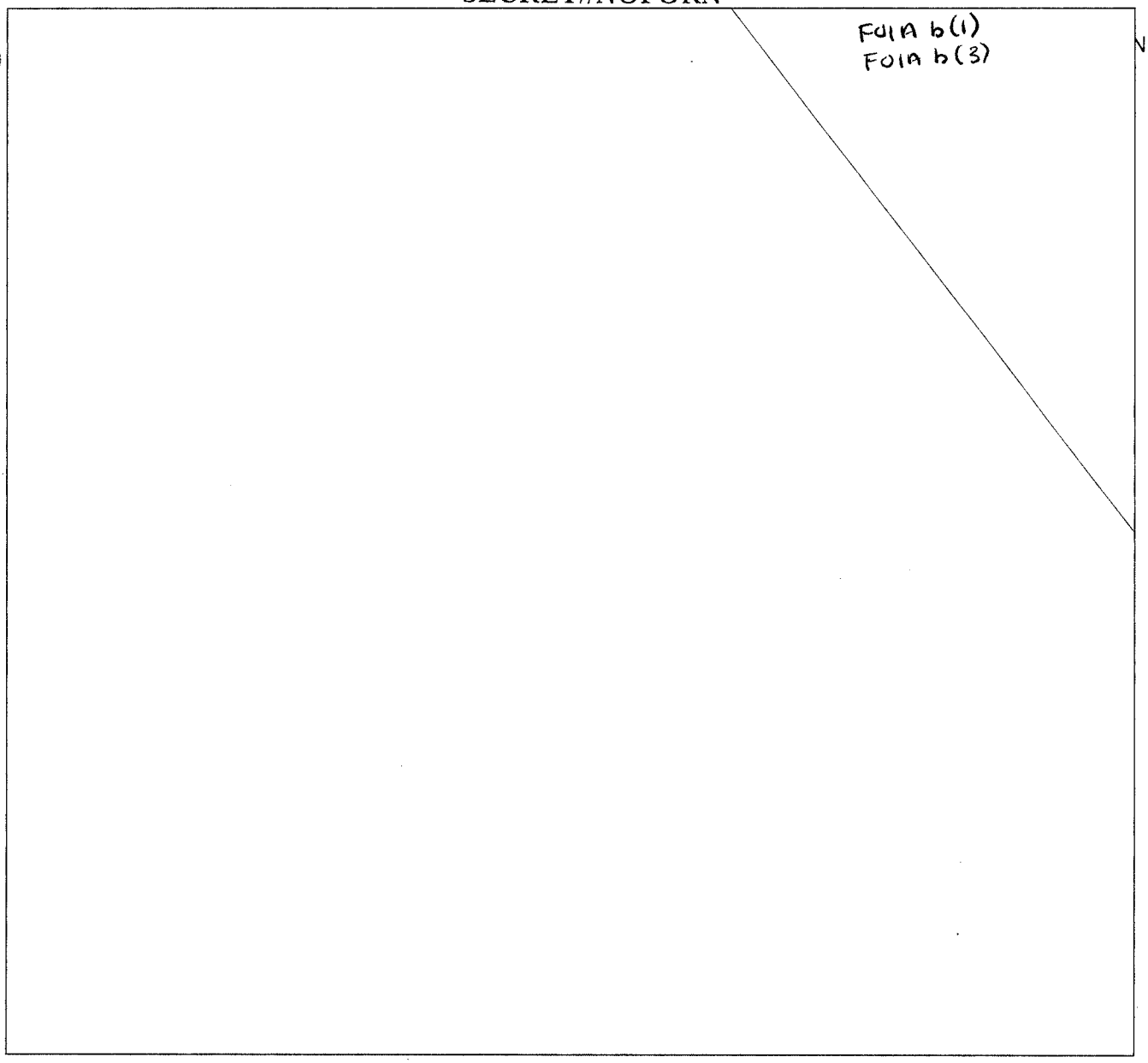
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

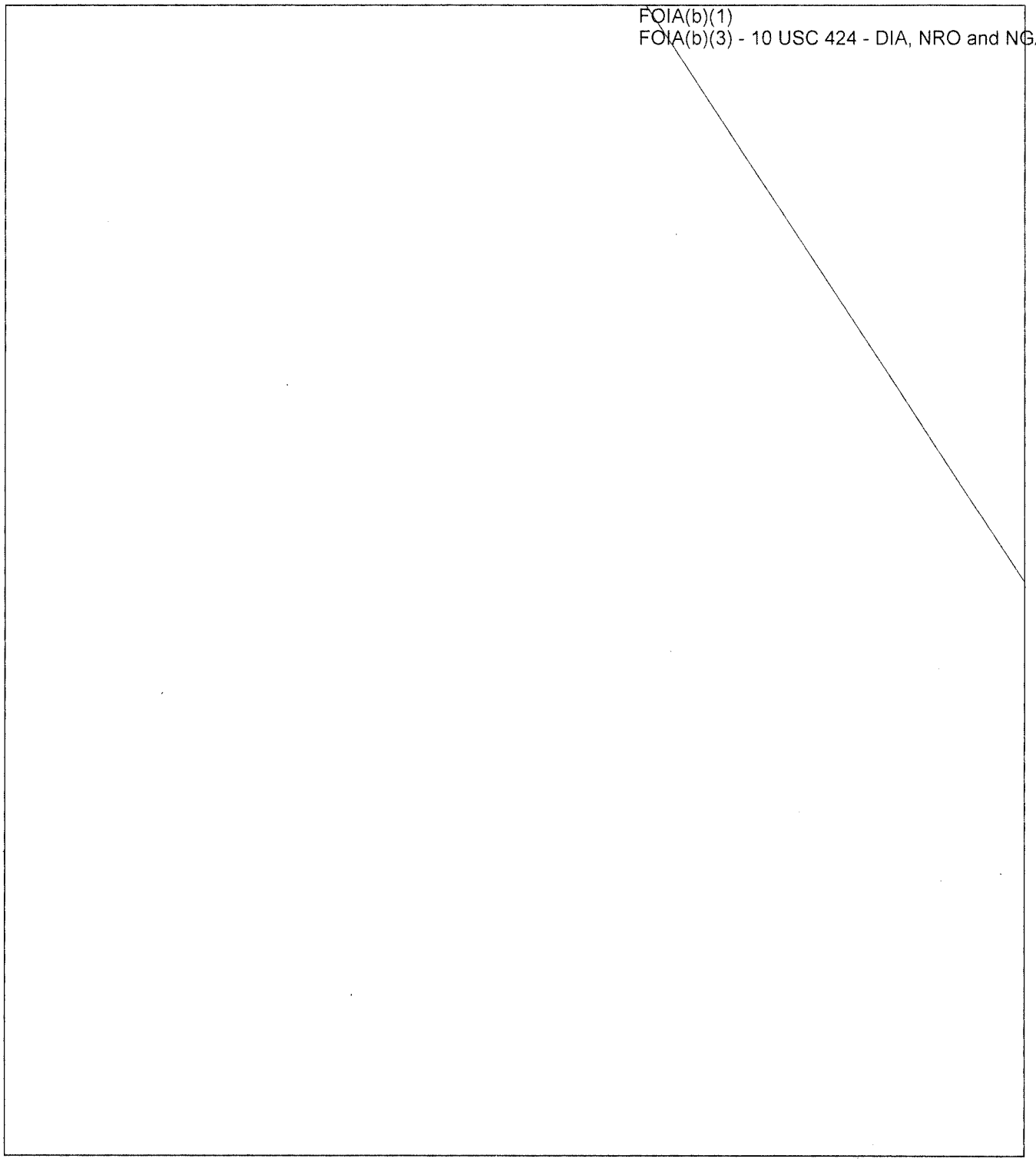


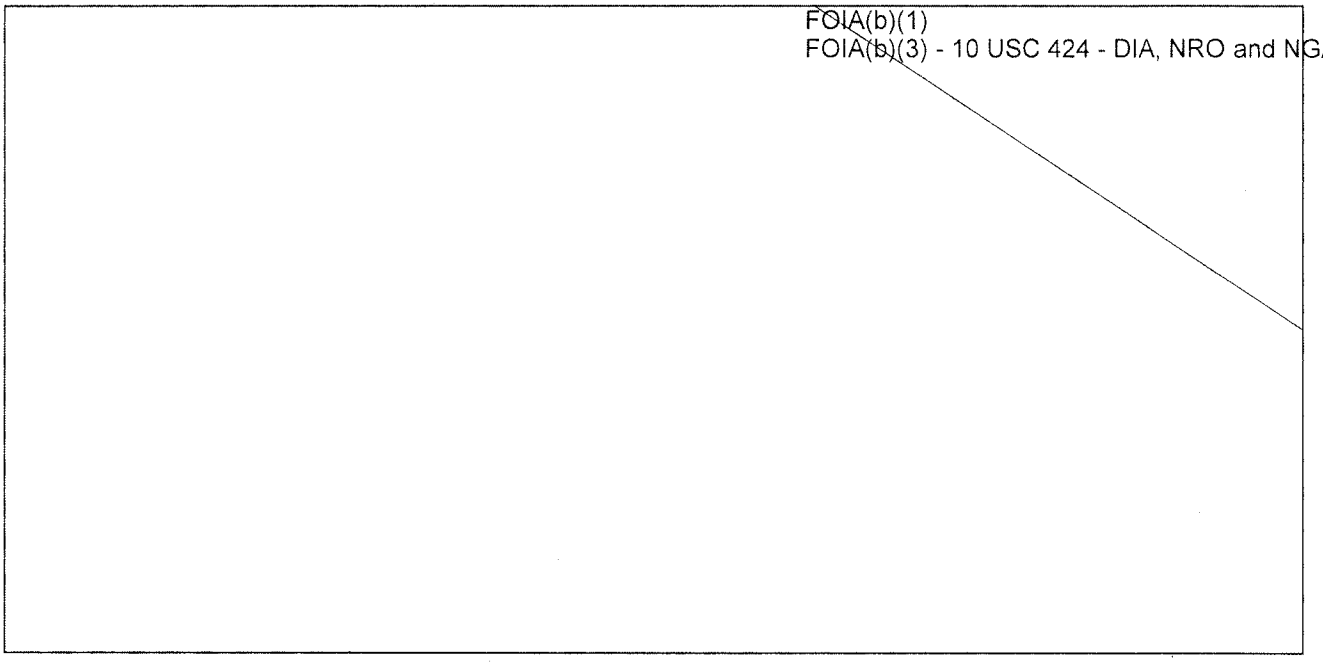

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

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

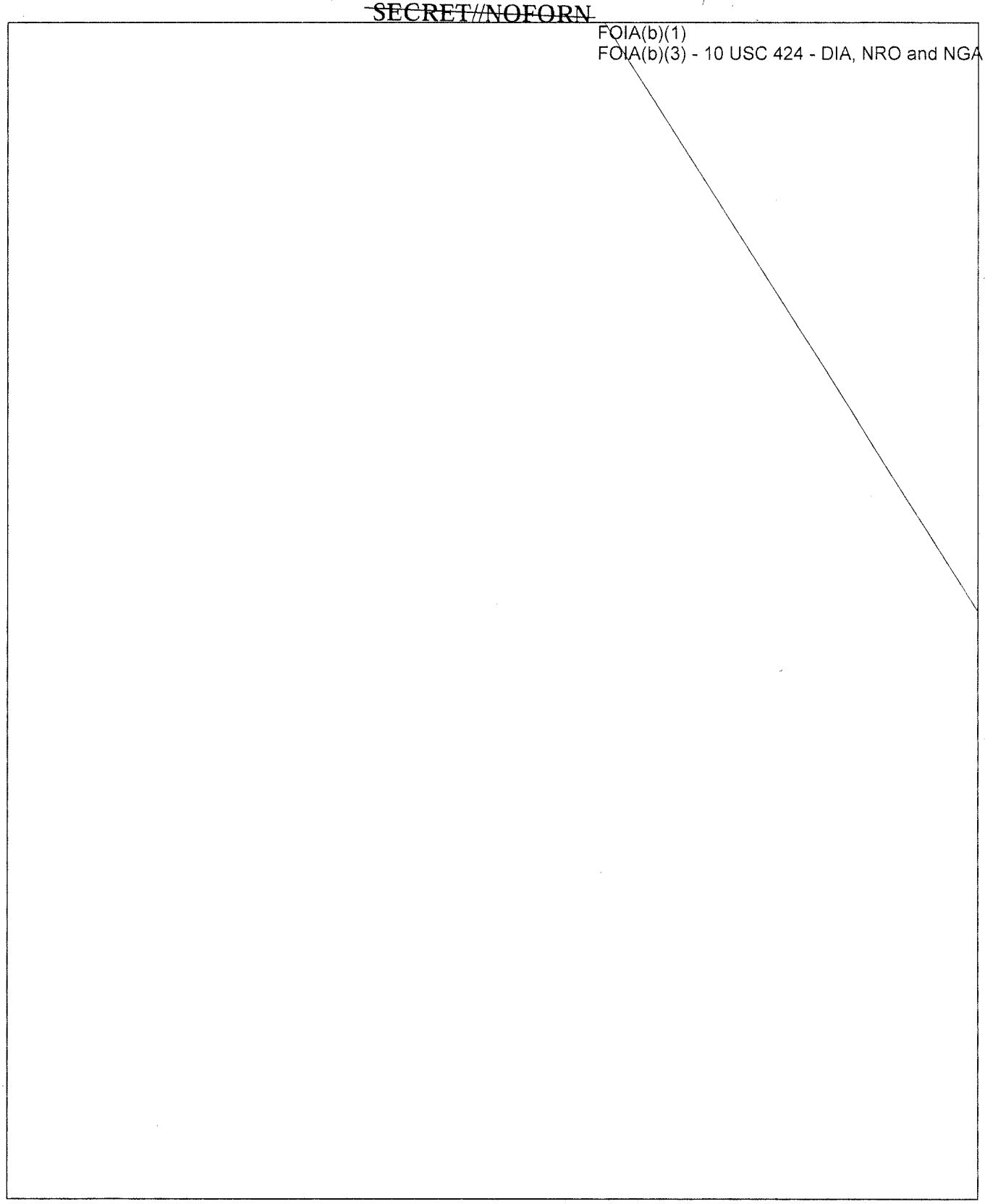


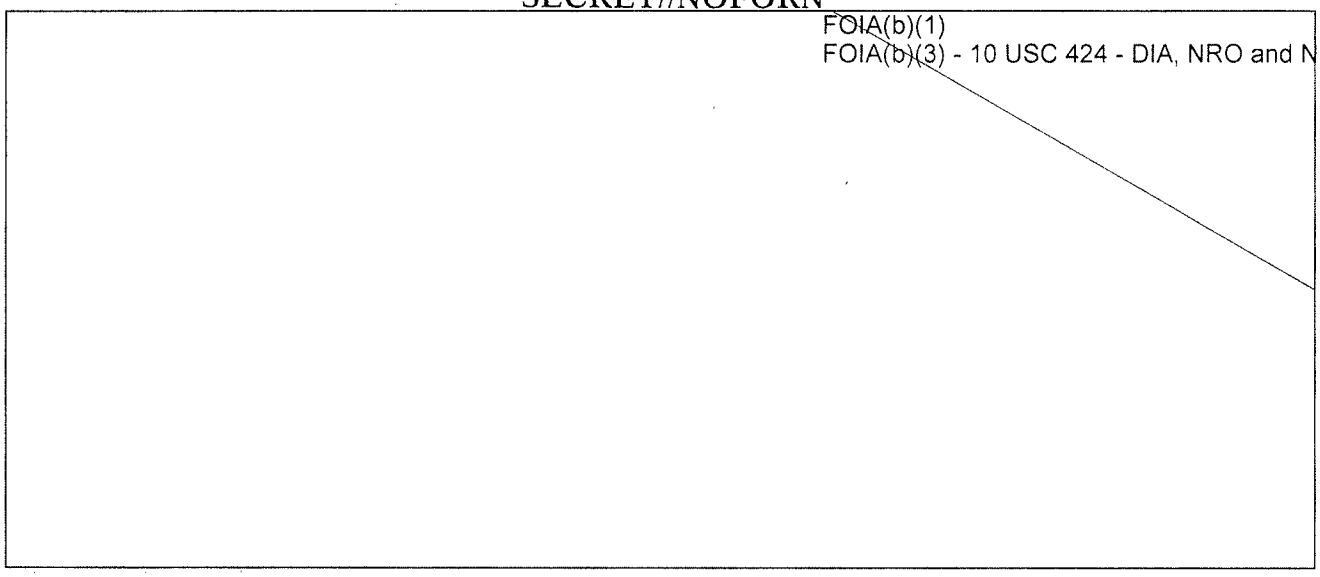


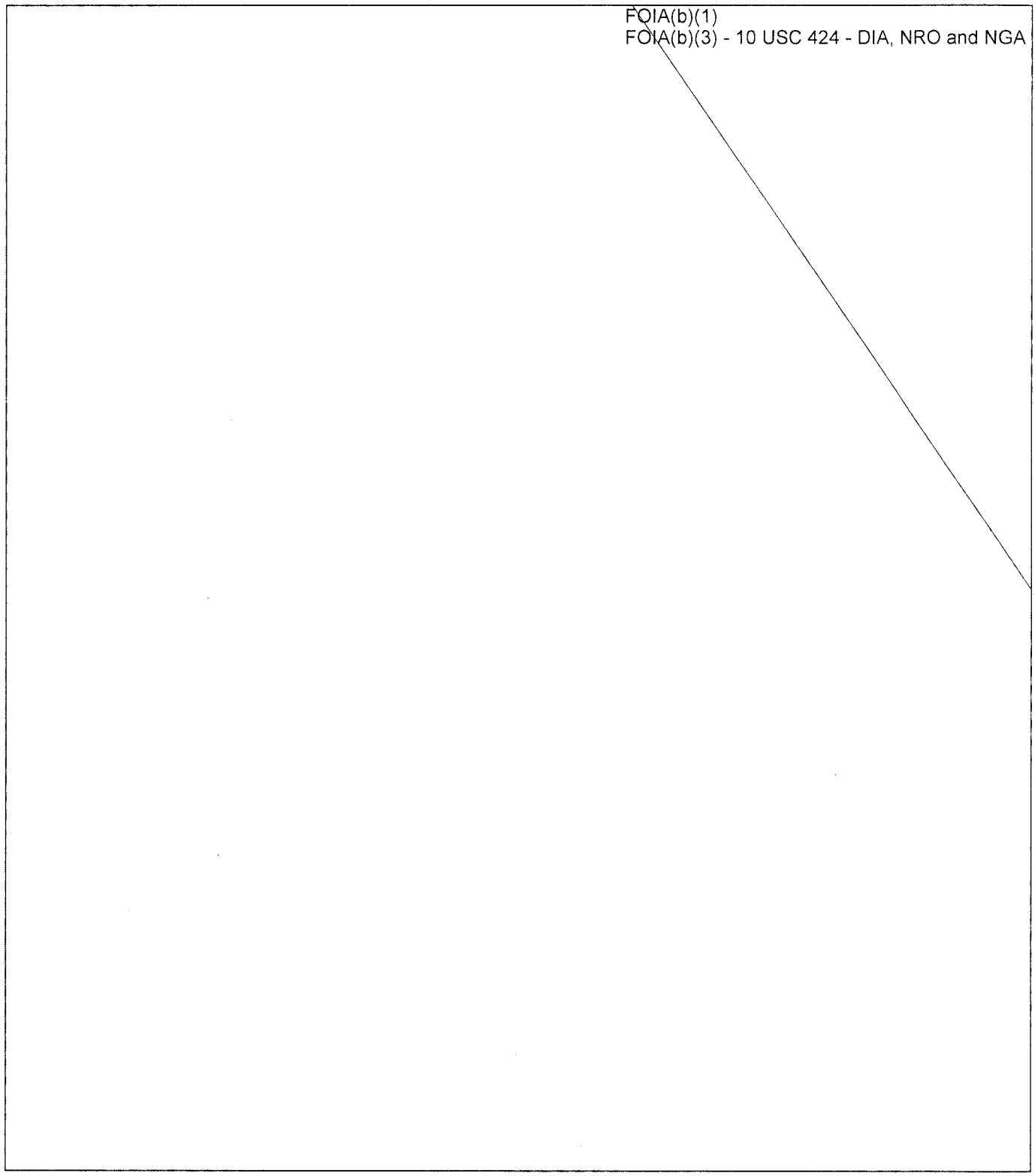

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA


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

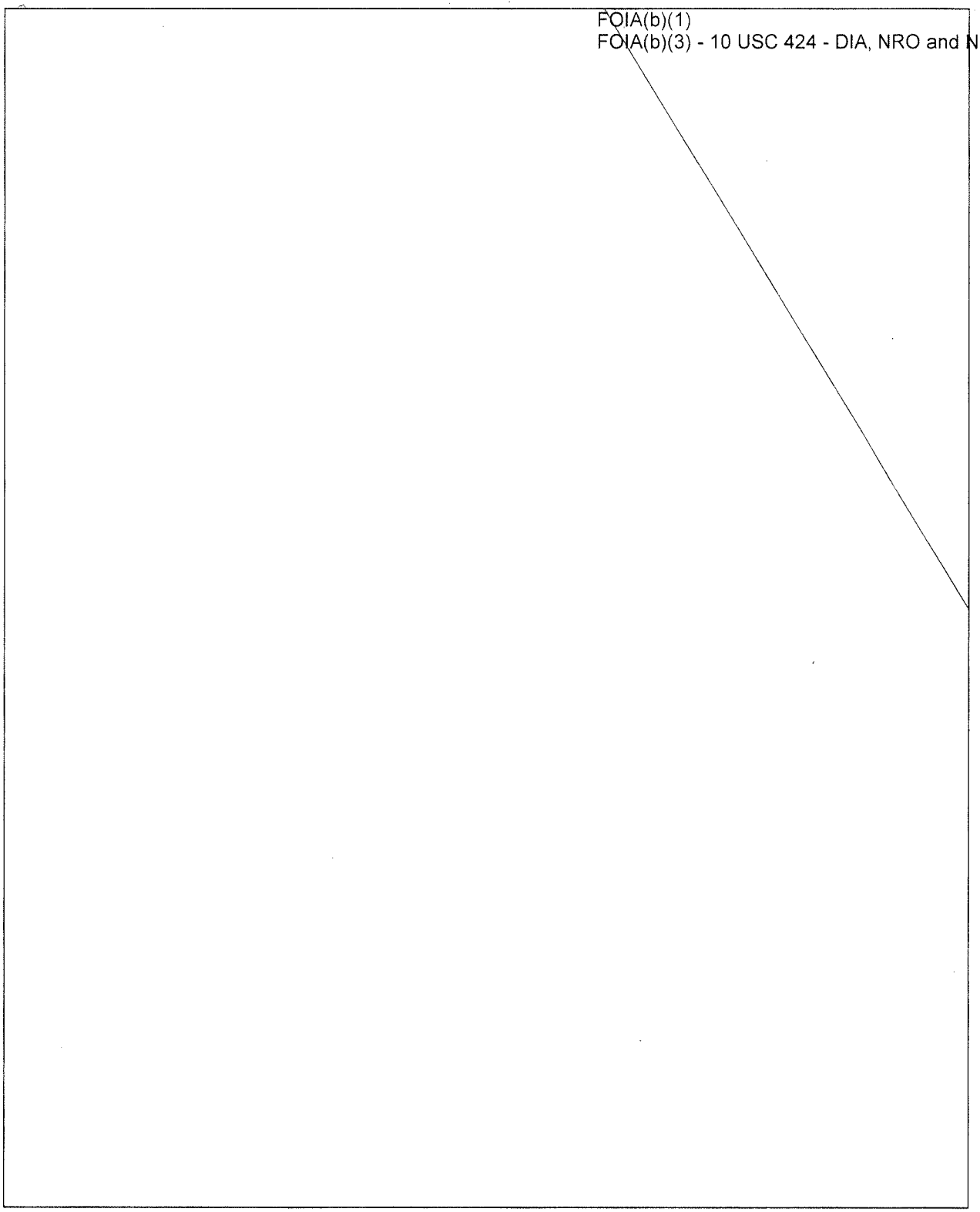
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

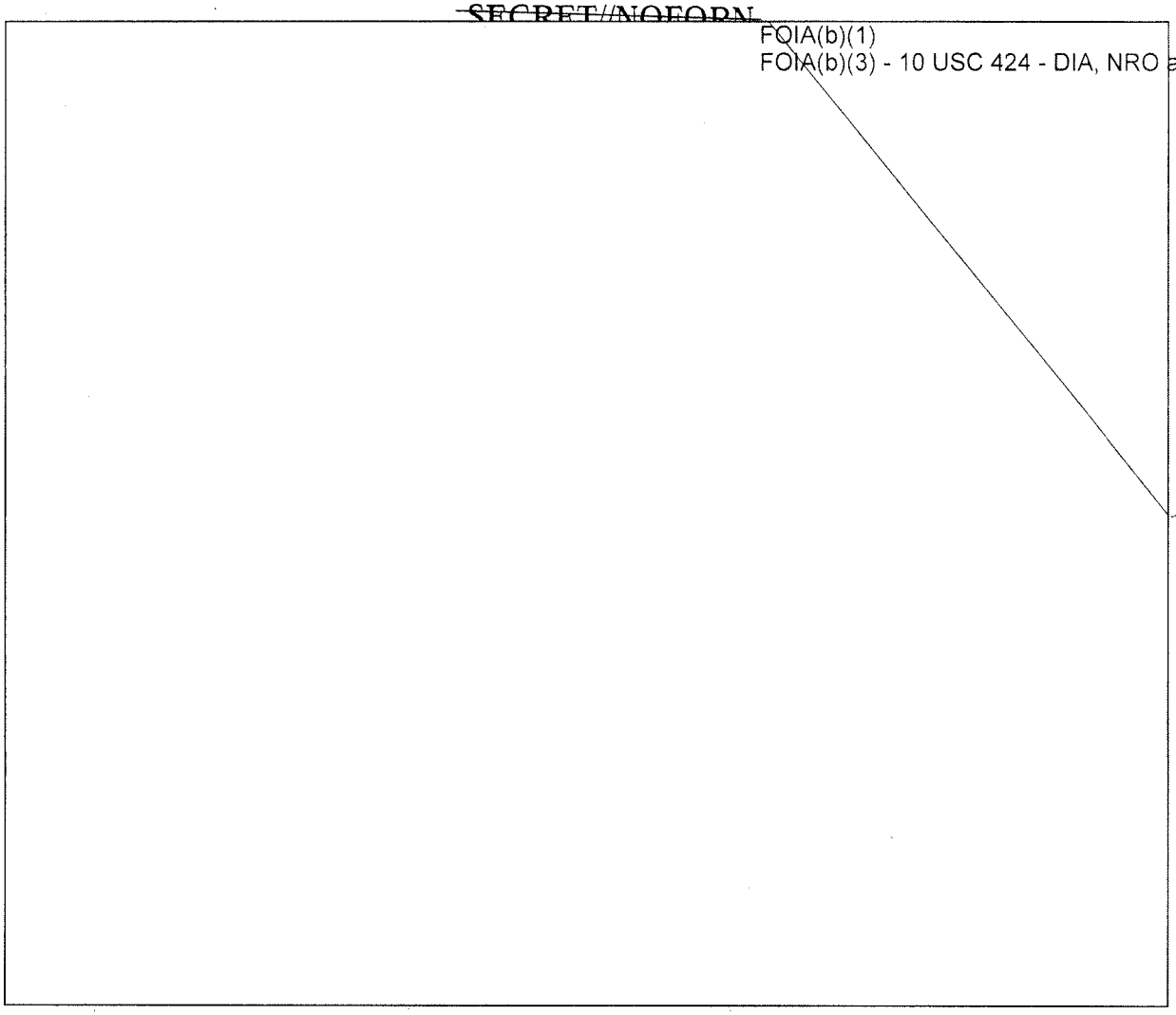




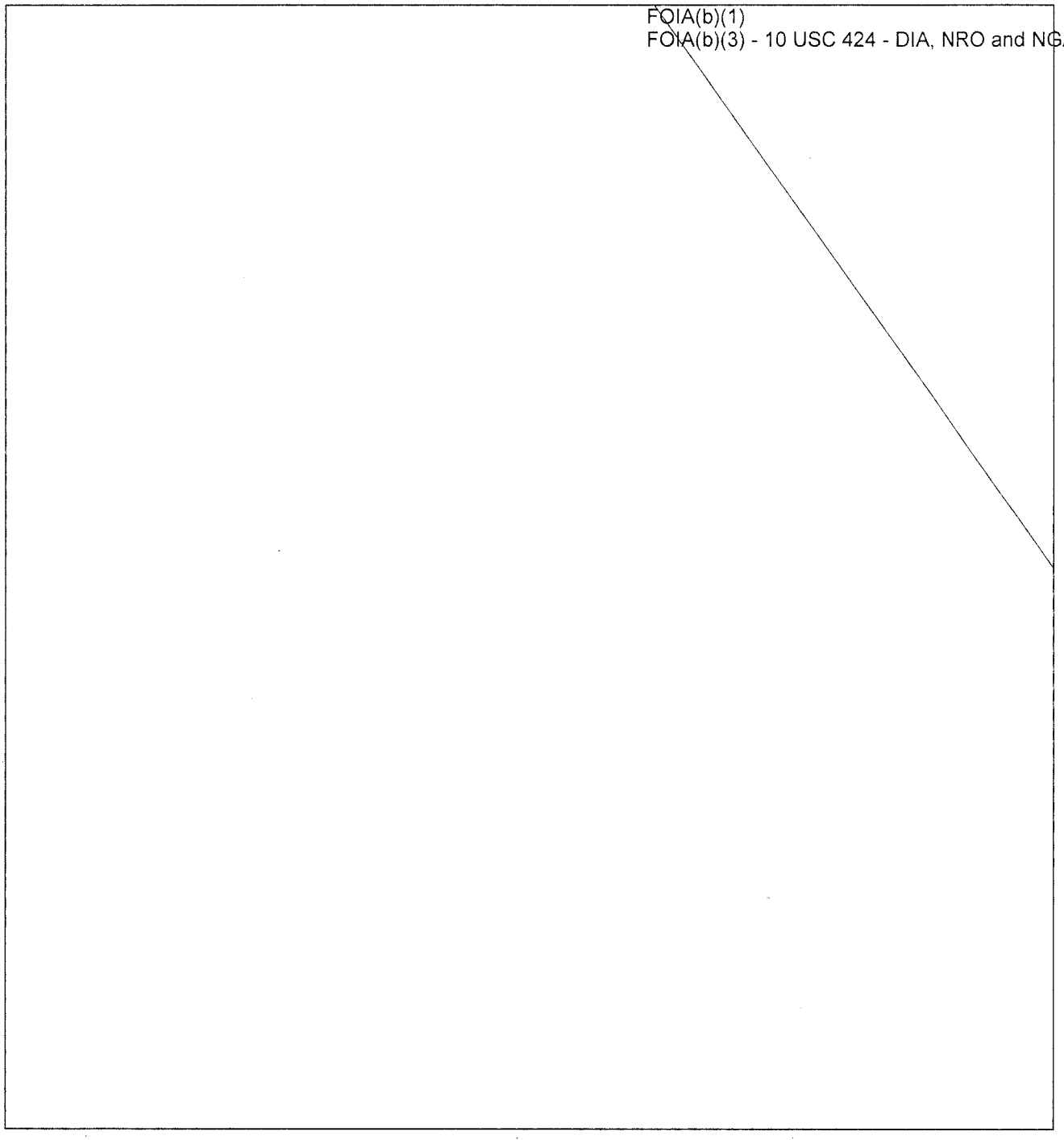

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

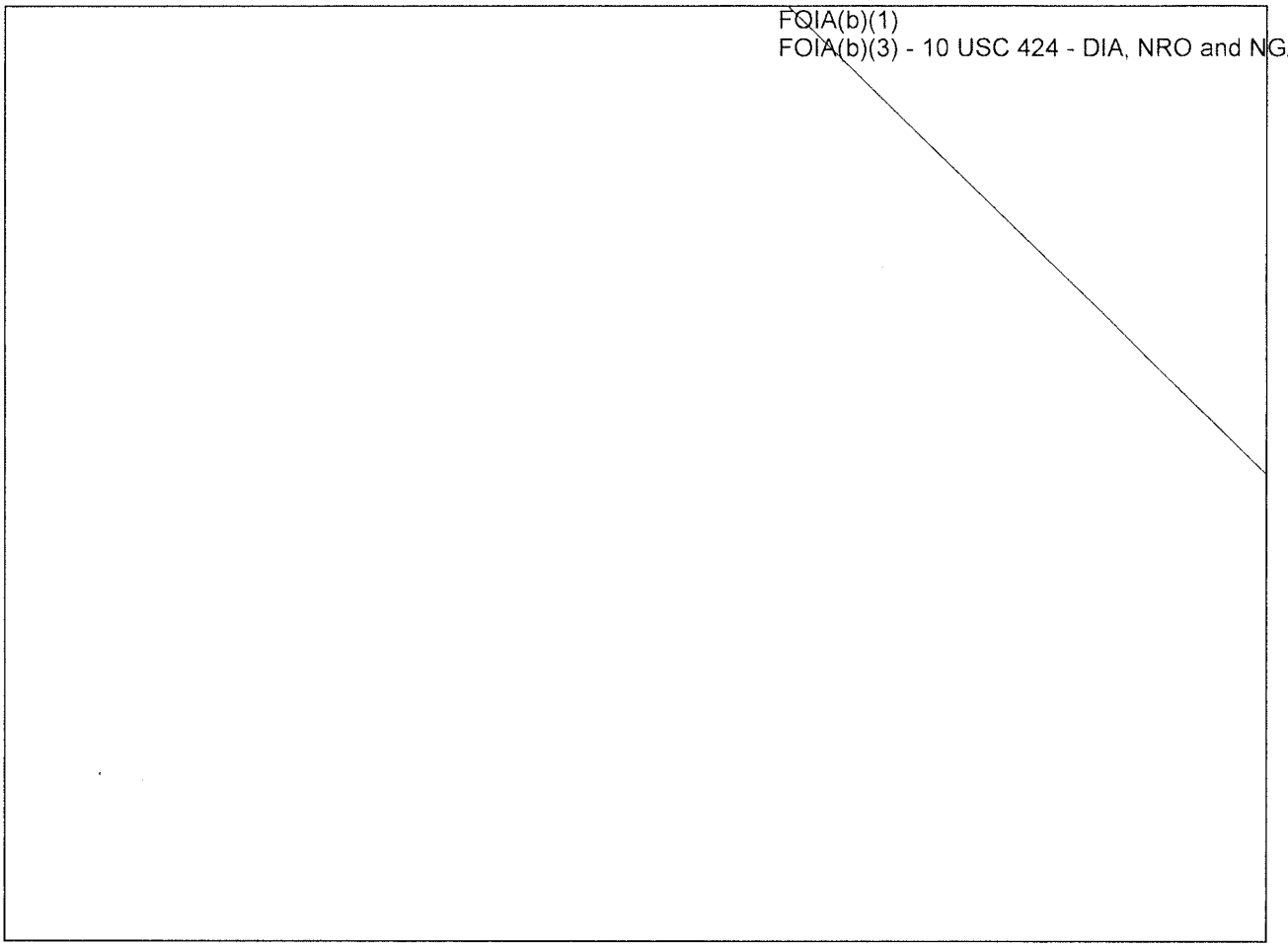
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

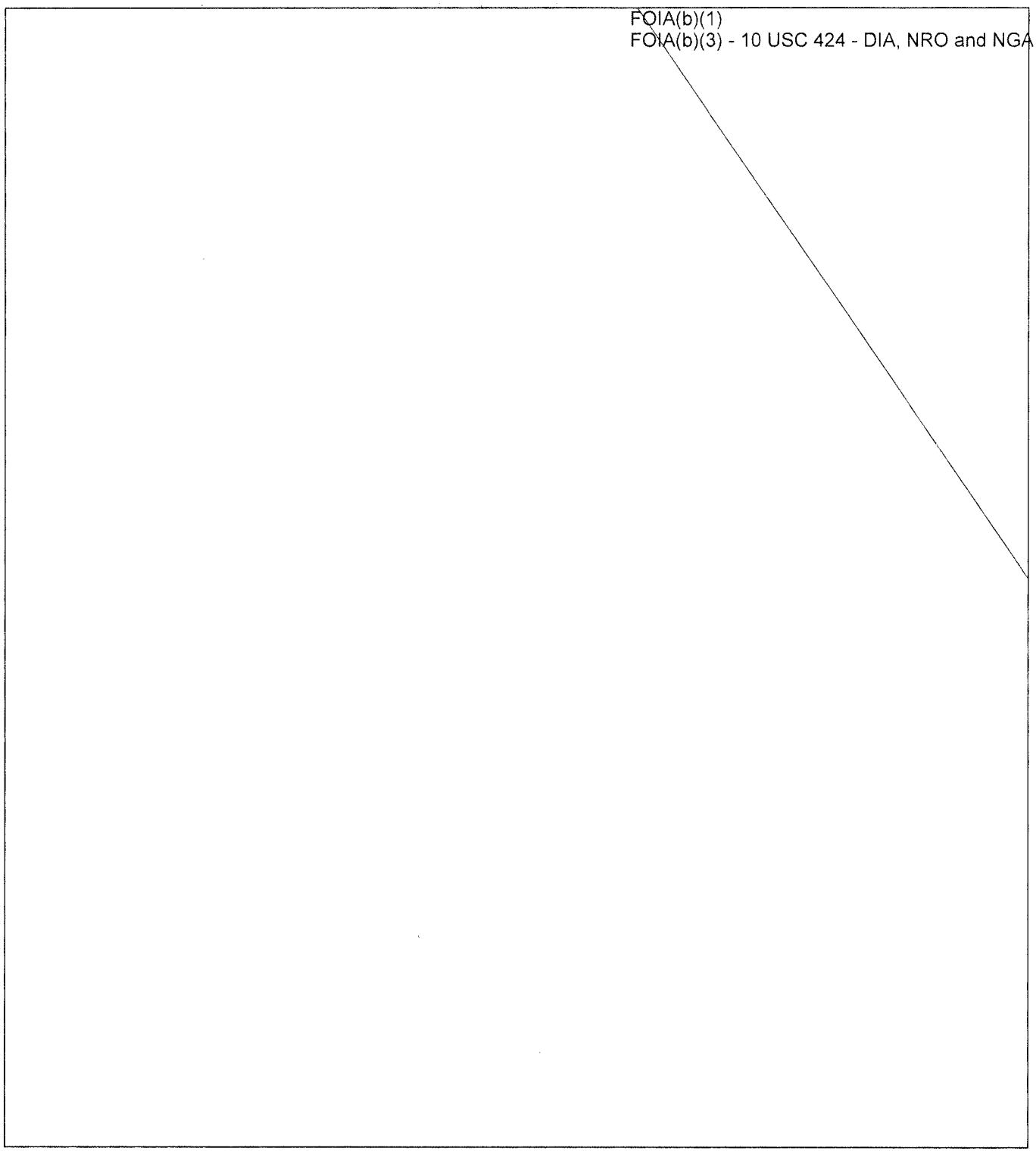

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

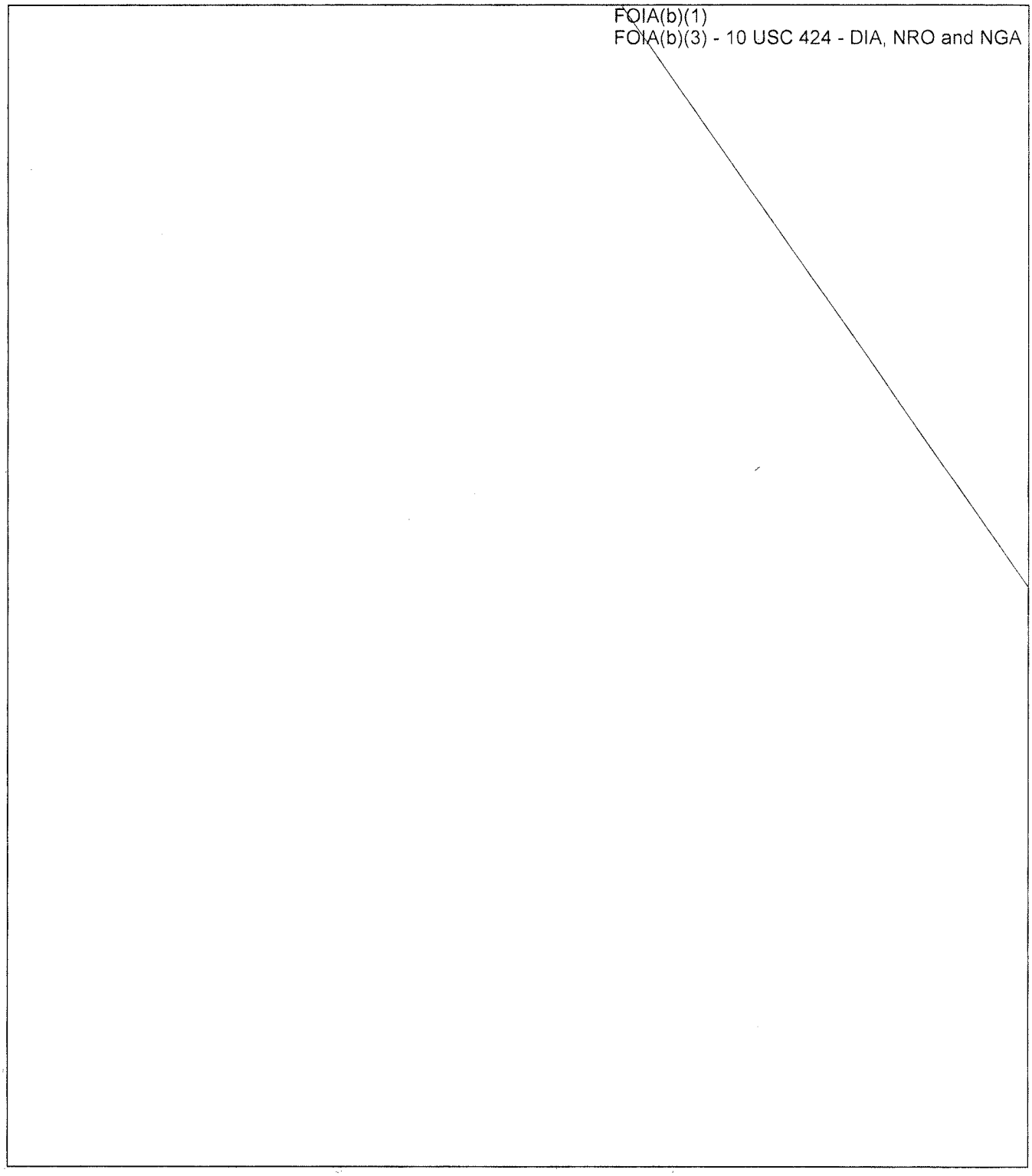


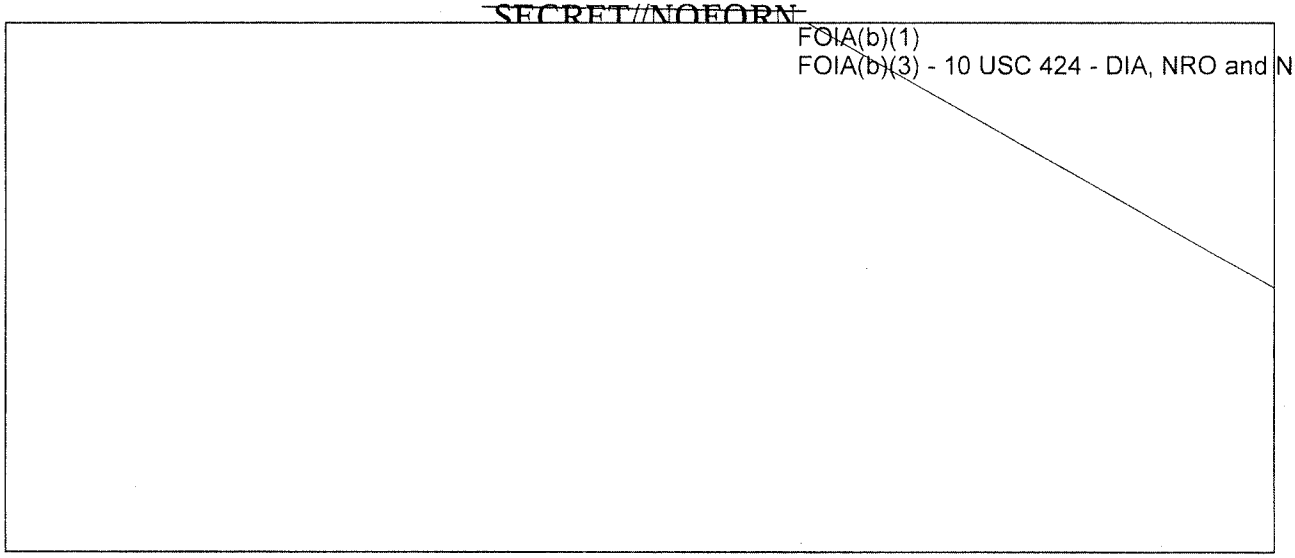
FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA


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

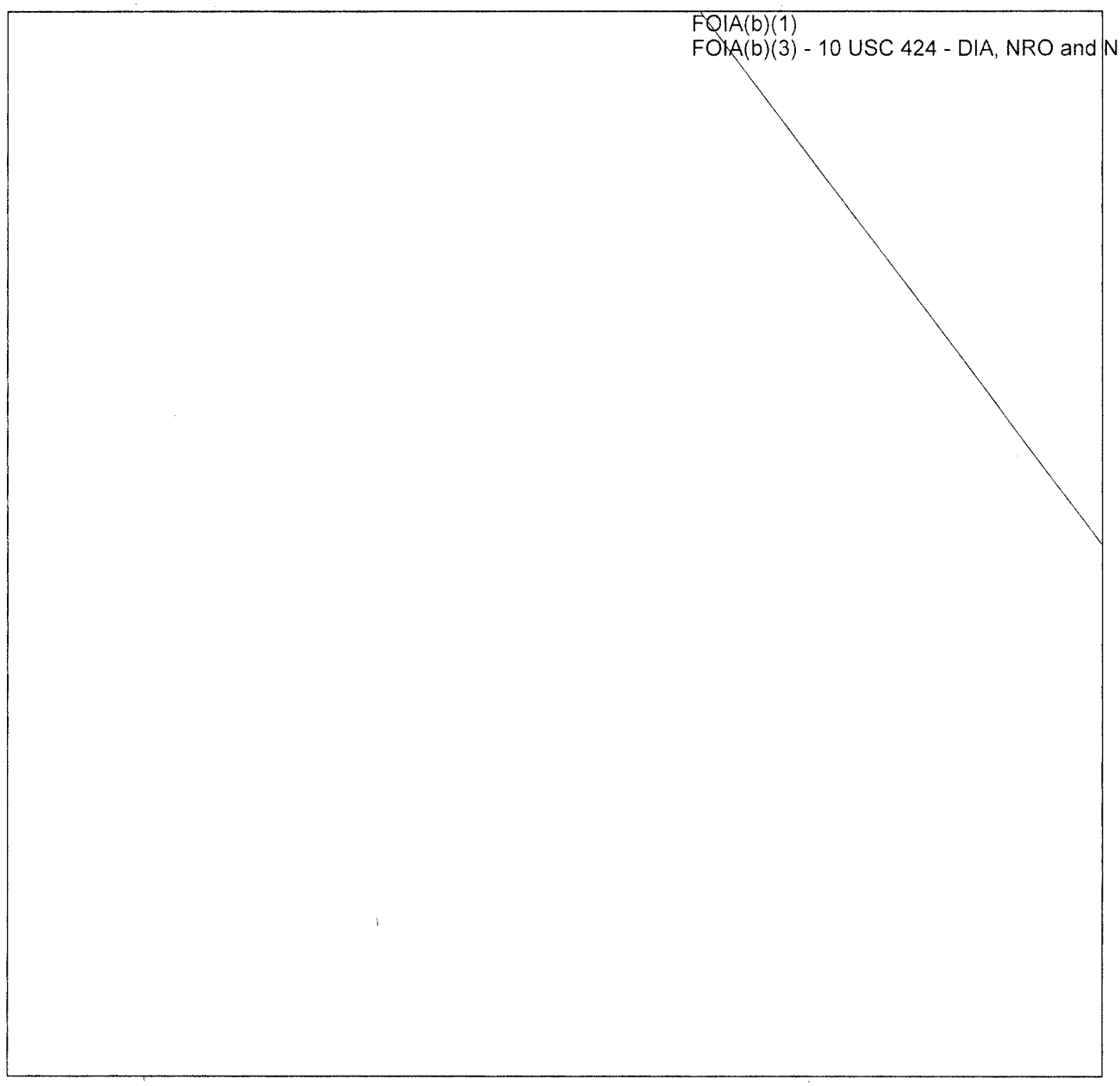

FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA

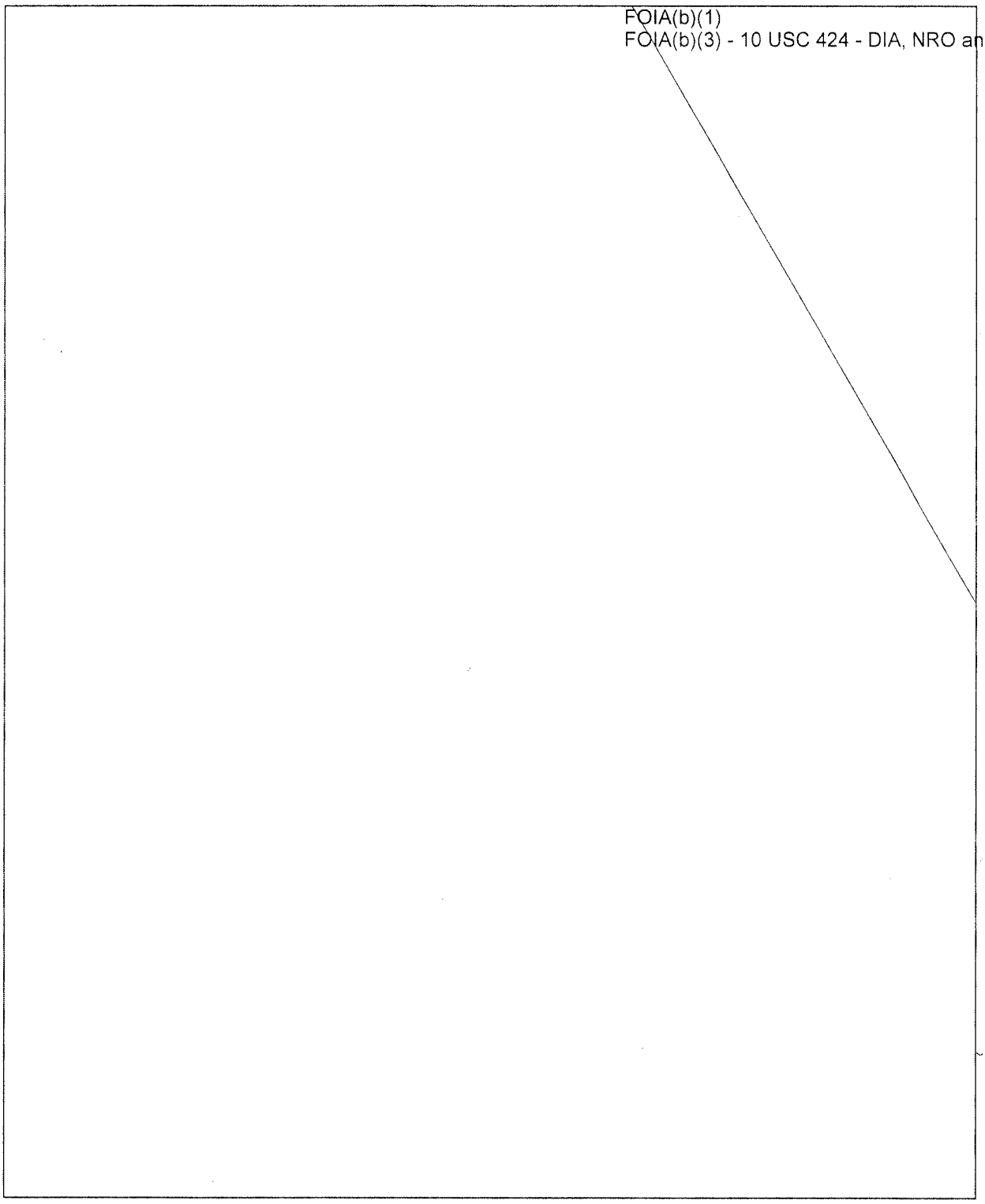



FOIA(b)(1)
FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA



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


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


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

FOIA(b)(6)

From: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)
Sent: Wednesday, February 29, 2012 4:38 PM
To: [redacted]
Subject: clean up instructions

Classification: ~~SECRET//NOFORN~~

Classified By: ESOG
Reason: 1.4(g)
Declassify On: 20370228
Derived From: NGA SCG SEC-08.1.1

==========

[redacted]

I spoke to [redacted] and his security folks asked from us something in writing detailing our cleanup instructions. I gather it is to show DSS their next audit.

Would you mind checking my comprehension below (or will all of these instructions be included in the letter your group will be giving the CORs)?

1. NGA desires that the reason to be given for this effort is "These presentations were not cleared for release". More elaborate procedures are not desired since NGA does not wish to draw attention to the aggregate.

2. Presentations #6 "IT/IS Migration" and #10 "Ops Support" of the Jan. 2012 ARL PMTR are to be removed:

a. All softcopies are to be deleted from any server the presentations are stored on. No effort is required to sanitze any transmitting server or router.

6. All hardcopies are to be destroyed.

c. An email stating a&b above is to be sent to all invitees.

d. The Table of Contents of any and all backup tapes containing the presentations will be deleted. It is then sufficeint to place the tapes back into circulation such that they will be over written in the noraml course of operations.

Did I catch all the instructions correctly?

thanks,

[redacted]
National Geospatial-Intelligence Agency
ESOG StL L-22
MSNCC System Engineer
[redacted]
unclassified email: [redacted]

ecret email: [redacted]

==========

Classification: ~~SECRET//NOFORN~~

From: FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)
Sent: Friday, March 02, 2012 12:52 PM
To:
Subject: RE: CIAD abd ARL contact info

classification:~~SECRET//NOFORN//~~

The presentations in question were reviewed by NGA Classification Management and determined to be classified SECRET//NOFORN IAW the NGA Security Classification Guide. As such, the documents cannot reside or be stored on any unclassified computer system.

-----Original Message-----
From: [mailto:]
Sent: Thursday, March 01, 2012 11:20 AM
To:
Subject: RE: CIAD abd ARL contact info

Classification: UNCLASSIFIED//~~FOUO~~

I would like to understand the specific reasons the two presentation needed to be deleted. We want to prevent an issue like this in the future and also make sure it is not elsewhere in our documentation. At this point I do not have enough information to do either.

Thanks,

From:
Sent: Wednesday, February 29, 2012 12:00 PM
To
Subject: CIAD abd ARL contact info

s the Project Lead for my system and is one of their ISSOs. He is leading the clean up effort on the Austin side.

s the person we are working with in security. He has offered to help out with specific questions that are beyond my job jacket.

I of course will still remain plugged in with both sides throughout the process.

National Geospatial-Intelligence Agency

From: FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)
Sent: Tuesday, March 06, 2012 8:23 AM
To:
Subject: RE: CIAD abd ARL contact info

classification:~~SECRET//NOFORN//~~

in addition, please ensure the cleanup and sanitization of all affected AIS is done in accordance with your local policy and procedures for this level of information.

-----Original Message-----
From:
Sent: Friday, March 02, 2012 1:52 PM
To:
Subject: RE: CIAD abd ARL contact info

classification:~~SECRET//NOFORN//~~

The presentations in question were reviewed by NGA Classification Management and determined to be classified SECRET//NOFORN IAW the NGA Security Classification Guide. As such, the documents cannot reside or be stored on any unclassified computer system.

-----Original Message-----
From: [mailto
Sent: Thursday, March 01, 2012 11:20 AM
To:
Subject: RE: CIAD abd ARL contact info

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

I would like to understand the specific reasons the two presentation needed to be deleted. We want to prevent an issue like this in the future and also make sure it is not elsewhere in our documentation. At this point I do not have enough information to do either.

Thanks,

From:
Sent: Wednesday, February 29, 2012 12:00 PM
To:
Subject: CIAD abd ARL contact info

[redacted] ~~is the Project Lead for my system and is one of their ISSOs. He is leading the clean up effort on the Austin~~ FOIA(b)(6) side.

[redacted] ~~is~~ the person we are working with in security. He has offered to help out with specific questions that are beyond my job jacket.

I of course will still remain plugged in with both sides throughout the process.

[redacted]
[redacted]
National Geospatial-Intelligence Agency
ESOG StL
MSNCC System Engineer/Service MAnager
[redacted]
unclassified email: [redacted]
secret email: [redacted]

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

==========

Classification: UNCLASSIFIED//~~FOUO~~

Warning: This document may not be used as a source of derivative classification.
CL By: Unknown
CL Reason: Sec.1.4(g)
DECL ON:
Derived From:
~~SECRET//NOFORN//~~
~~SECRET//NOFORN//~~

From:
Sent: Friday, March 16, 2012 7:44 AM
To:
Subject: FW: CIAD abd ARL contact info FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)

classification:~~SECRET//NOFORN//~~

-----Original Message-----
From:
Sent: Wednesday, March 14, 2012 7:12 AM
To:
Subject: RE: CIAD abd ARL contact info

classification:~~SECRET//NOFORN//~~

Good morning. I just wanted to check in with you to request a status update on the effort below.

r/

-----Original Message-----
From: [mailto
Sent: Thursday, March 01, 2012 11:20 AM
To:
Subject: RE: CIAD abd ARL contact info

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

I would like to understand the specific reasons the two presentation needed to be deleted. We want to prevent an issue like this in the future and also make sure it is not elsewhere in our documentation. At this point I do not have enough information to do either.

Thanks,

From:
Sent: Wednesday, February 29, 2012 12:00 PM

To:
Subject: CIAD abd ARL contact info

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

is the Project Lead for my system and is one of their ISSOs. He is leading the clean up effort on the Austin side.

is the person we are working with in security. He has offered to help out with specific questions that are beyond my job jacket.

I of course will still remain plugged in with both sides throughout the process.

-

National Geospatial-Intelligence Agency
ESOG StL
MSNCC System Engineer/Service MAnager
unclassified email:
secret email:

==========

Classification: UNCLASSIFIED//~~FOUO~~

Warning: This document may not be used as a source of derivative classification.
CL By: Unknown
CL Reason: Sec.1.4(g)
DECL ON:
Derived From:
~~SECRET//NOFORN//~~
~~SECRET//NOFORN//~~

From:
Sent: Monday, March 19, 2012 2:20 PM
To:
Subject: RE: clean up instructions

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

The action outlined in this email below were completed by the end of February

-----Original Message-----
From:
Sent: Wednesday, February 29, 2012 4:38 PM
To
Subject: clean up instructions

Classification: ~~SECRET//NOFORN~~

Classified By: ESOG
Reason: 1.4(g)
Declassify On: 20370228
Derived From: NGA SCG SEC-08.1.1
==========

I spoke to and his security folks asked from us something in writing detailing our cleanup instructions. I gather it is to show DSS their next audit.

Would you mind checking my comprehension below (or will all of these instructions be included in the letter your group will be giving the CORs)?

1. NGA desires that the reason to be given for this effort is "These presentations were not cleared for release". More elaborate procedures are not desired since NGA does not wish to draw attention to the aggregate.

2. Presentations #6 "IT/IS Migration" and #10 "Ops Support" of the Jan. 2012 ARL PMTR are to be removed:
a. All softcopies are to be deleted from any server the presentations are stored on. No effort is required to sanitze any transmitting server or router.
6. All hardcopies are to be destroyed.
c. An email stating a&b above is to be sent to all invitees.
d. The Table of Contents of any and all backup tapes containing the presentations will be deleted. It is then sufficeint to place the tapes back into circulation such that they will be over written in the noraml course of operations.

Did I catch all the instructions correctly?

thanks,

National Geospatial-Intelligence Agency
ESOG StL L-22
MSNCC System Engineer
[redacted]
unclassified email: [redacted]

secret email [redacted]

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

Classification: ~~SECRET//NOFORN~~

From:
Sent: Monday, March 26, 2012 8:23 AM
To: FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
Subject: RE: clean up instructions FOIA(b)(6)

classification:~~SECRET//NOFORN//~~
Thank you I would also like to request a copy of the final report as well. I need a copy for my records.
r/

-----Original Message-----
From: [mailto:
Sent: Monday, March 19, 2012 3:20 PM
To:
Subject: RE: clean up instructions

The action outlined in this email below were completed by the end of February.

-----Original Message-----
From:
Sent: Wednesday, February 29, 2012 4:38 PM
To:
Subject: clean up instructions

Classification: ~~SECRET//NOFORN~~

Classified By: ESOG
Reason: 1.4(g)
Declassify On: 20370228
Derived From: NGA SCG SEC-08.1.1
==========

I spoke to and his security folks asked from us something in writing detailing our cleanup instructions. I gather it is to show DSS their next audit.

Would you mind checking my comprehension below (or will all of these instructions be included in the letter your group will be giving the CORs)?

1. NGA desires that the reason to be given for this effort is "These presentations were not cleared for release". More elaborate procedures are not desired since NGA does not wish to draw attention to the aggregate.

2. Presentations #6 "IT/IS Migration" and #10 "Ops Support" of the Jan. 2012 ARL PMTR are to be removed:
a. All softcopies are to be deleted from any server the presentations are stored on. No effort is required to sanitze any transmitting server or router.

6. All hardcopies are to be destroyed.

c. An email stating a&b above is to be sent to all invitees.

d. The Table of Contents of any and all backup tapes containing the presentations will be deleted. It is then sufficeint to place the tapes back into circulation such that they will be over written in the noraml course of operations.

Did I catch all the instructions correctly?

thanks,

[redacted]

[redacted]

National Geospatial-Intelligence Agency
ESOG StL L-22
MSNCC System Engineer
[redacted]
unclassified email: [redacted]

secret email: [redacted]
Classification: ~~SECRET//NOFORN~~

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

Warning: This document may not be used as a source of derivative classification.
CL By: Unknown
CL Reason: Sec.1.4(g)
DECL ON:
Derived From:
~~SECRET//NOFORN//~~

From:
Sent: Friday, June 08, 2012 1:58 PM
To:
Cc:
Subject: RE: ARL possible Security Spill

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

We understand that this final ruling has been determined to be classified, however, we still don't know what specific information in these presentations are classified. The ruling initially made by cites information from the SCG that are not present in the presentations which is why we challenged the ruling. Please provide us specific information about what exactly is classified so we will know what information we need to protect and avoid any future incidents. If you have any questions I would be happy to discuss the details over a STE phone. I appreciate your help in this matter. Thanks.

Applied Research Labs, University of Texas at Austin Information System Security Manager
Phone:

-----Original Message-----
From
Sent: Wednesday, May 30, 2012 2:33 PM
To:
Cc:
Subject: RE: ARL possible Security Spill

Classification: ~~SECRET//NOFORN~~

Classified By: 1030432-1
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370530
==========

(S//NF) I concur with the classification determination rendered on the ARL security spill. ARL should employ the mitigation plan provided for such instances. NGA Classification Management

-----Original Message-----
From:
Sent: Wednesday, May 30, 2012 8:18 AM
To:

Cc:

Subject: RE: ARL possible Security Spill

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

Classification: SECRET//NOFORN

C-lassified By:
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370530
==========

The position of NGA CIAD is this incident is considered a security violation due to the fact that classified information was stored and processed on a system not authorized to do so. The classification determination was provided by NGA Classification Management and forwarded on to ARL-UT. In a phone conversation I had with both and FOIA(b)(6) mid-April, I requested a copy of the report outlining the steps taken to clean and sanitize the affected computer systems. When asked if the steps already taken would be sufficient to say the spill had been mitigated, I replied that the processes needed to sanitize the computer systems should be in accordance with ARL-UT policies and procedures concerning data spills. If ARL-UT did not have these mitigation plans (and they should) then I would be happy to provide guidance. I was told by that ARL-UT did have the policies and procedures in place but there was still a question of how/why the information was classified. All this being said, this issue was first reported to to be opened especially when the circumstances appear to be pretty straight forward. I understand that and ARL-UT want to be certain the information is classified before initiating cleanup procedures due to the manpower and resources needed to accomplish this. But NGA Classification Management has provided their classification determination the information is classified SECRET//NOFORN. At this point, I don't know what else there is to do other than perform the cleanup and provide a copy of the report.

FOIA(b)(1) NGA

r/

-----Original Message-----
From:
Sent: Tuesday, May 29, 2012 4:13 PM
To:
Subject: FW: ARL possible Security Spill

Classification: SECRET//NOFORN

Classified By
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370529
==========

Per our discussion, do you care to chime in on this?

-----Original Message-----
From:
Sent: Tuesday, May 29, 2012 1:14 PM
To:
Cc:
Subject: RE: ARL possible Security Spill

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370529
==========

My O&M contractor have been enquiring if what they have performed in the past as "cleanup" is sufficient and if they can close this out.

Thanks,

TOSG - Geodesy & Geophysics Branch, IT Services Division, Operations Control Office, Service Operations Group mailstop L-022 Application Support Staff/Program and Technical Engineer MSNCC System Engineer/Service Manager G&G support

-----Original Message-----
From
Sent: Wednesday, May 23, 2012 9:49 AM
To
Cc
Subject: RE: ARL possible Security Spill

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370523
==========

I have been on TDY and have lost the bubble. Talking to this morning, it sounds like we are all looking for closure. ...So, has a decision been made that a spill occurred or was that decision rescinded? If the decision stands, then has ARL been asked to send in their write up documenting what they have done to delete the files? Assuming they have not sent in a write up; is there something I can do to facilitate this process?

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

-----Original Message-----
From:
Sent: Sunday, May 13, 2012 6:52 AM
To:
Cc:
Subject: RE: ARL possible Security Spill

Classification: ~~SECRET//NOFORN~~

Classified By:
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
Reason: 1.4(c),(g)
Declassify On: 20370513
==========

Good Morning.

I have included as the NGA CIAD individual responsible for this investigation. Because I don't know their internal process, I will allow him to lead us through this. I stand by for any additional security review that is required from our office.

v/r,

-----Original Message-----
From:
Sent: Thursday, May 10, 2012 7:29 PM

~~SECRET/NOFORN~~

To
Cc
Subject: RE: ARL possible Security Spill

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

Classification: ~~SECRET//NOFORN~~

Classified By: NSA
Reason: 1.4(c), (g)
Declassify On: 20370510
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1
==========

Looking at the slides.... and thinking hard about the connections necessary to reach the Secret level (in aggregation). I think we can agree, that by shredding all hard copies, deleting all fines, and cleaning the various delete files, this possible spill should be closed, based on actions taken so far.

Additionally, I know my opinion means noting. But if anyone wants my opinion. I do not think these slides (even if they were presented in the same brief would aggregate to the level of a Secret (and therefore constitute a spill).

Recommend, that the issue should be closed, with words to the effect; "Upon further review, this incident does not rise to the level of aggregation necessary to be categorized as a spill. Recommend this case be closed."

-----Original Message-----
From
Sent: Thursday, May 10, 2012 9:06 AM
To:
Subject: RE: ARL possible Security Spill

(S/NF I am unsure what parts decided "aggregated". My original email pointed out that all of page number

FOIA(b)(1) NGA

(S/NF can you wade in with more specific details that answer questions? My original thoughts were that a spill had not occurred, but that we had gotten close. Obviously you saw something that I missed.

Thanks,
-

~~SECRET/NOFORN~~

SOG - Geodesy & Geophysics Branch, Production Services, IT Operations, Enterprise Service Operations mailstop L-022
Application Support Staff/Program and Technical Engineer MSNCC System Engineer/Service Manager G&G support

-----Original Message-----
From:
Sent: Thursday, May 10, 2012 7:44 AM
To:
Subject: ARL possible Security Spill

Classification: ~~SECRET//NOFORN~~

Classified By: NSA
Reason: 1.4(c), (g)
Declassify On: 20370510
Derived From: NGA SCG AIS-08.1.1, NGA SCG MET-08.1.1

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

==========

Please resend a copy of the offending slides. I will actually need just the two slides that have to things that aggregated to cause the violation: with Circles and Arrows and "a paragraph on the back."

==========

Classification: ~~SECRET//NOFORN~~

==========

Classification: ~~SECRET//NOFORN~~

==========

Classification: ~~SECRET//NOFORN~~

==========

Classification: ~~SECRET//NOFORN~~

==========

Classification: ~~SECRET//NOFORN~~

==========

Classification: ~~SECRET//NOFORN~~

==========

lassification: ~~SECRET//NOFORN~~

==========

Classification: ~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

APR 19 2013

INTELLIGENCE

MEMORANDUM FOR DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

SUBJECT: (U) Rationale for Denial of Classification Challenge Appeal by the Advanced Research Lab – University of Texas to the Interagency Security Classification Appeals Panel

(U) The Office of the Under Secretary of Defense for Intelligence Security Directorate hereby endorses and submits the attached information paper from the National Geospatial-Intelligence Agency (NGA), providing background information and facts regarding to the Advanced Research Lab – University of Texas classification challenge and appeal to the Interagency Security Classification Appeals Panel. Questions should be directed to

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

Timothy A. Davis
Director of Security

Attachment:
As stated

cc:
NGA Classification Management Branch

CLASSIFIED BY: G.R. Sturgis, Information Security Policy Support
DERVIED FROM: NGA Information Paper (Same Subject)
DECLASSIFY ON: 20371219

THIS COVER PAGE IS UNCLASSIFED UPON REMOVAL OF ATTACHMENT

~~SECRET//NOFORN~~

INFORMATION PAPER

SUBJECT: (U) Rationale for Denial of Classification Challenge Appeal by Advanced Research Lab – University of Texas (ARL-UT) to the Interagency Security Classification Appeals Panel (ISCAP)

1. **(U//~~FOUO~~) Purpose**. To provide essential background information and the facts surrounding the ARL-UT Classification Challenge and Appeal to ISCAP, submitted in accordance with Executive Order (E.O.) 13526, "Classified National Security Information," Section 5.3. *Interagency Security Classification Appeals Panel,* and provide justification for Denial

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

CL BY: 1303432
CL REASON: NGA SCG
DECL ON: 20371219

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

UT contractor was directed to initiate spill remediation procedures for both these deliverables.

3. **(S//NF) Background on NGA's final ruling on ARL-UT materials:**

FOIA (b)(1) NGA

Item # 1. Description: (U) An aggregate account of individual items, otherwise unclassified, items that reveal a system, objective, requirement, plan or other aspect of NGA or its mission the disclosure of which would jeopardize NGA organization, functions and organization, functions and capabilities, or U.S. intelligence sources or methods. See remarks. Classification: SECRET, Release: NOFORN, Declass: 25 yrs, Reason: 1.4 (C), Remarks: This is known as classification by compilation.

Item #14. Description: (C)

Item #16. Description: (U//~~FOUO~~)

Item #17. Description: (U//~~FOUO~~)

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

b) Additionally, NGA's Classification Management Branch relied upon subject NGA Security Classification Guide (SCG) (TAB E), Version 1.1, Table 1.10 (U)

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

Remarks:

4. (U) Summary

(U) The information security classification decision-making process in this matter is sound and resulted in the accurate identification of Secret//NOFORN information (both in the case of normal, day-to-day derivative classification operations, and upon close analysis by the NGA OCA's duly authorize representatives); utilized up-to-date SCGs approved by an NGA OCA; and relied upon long experience in protection of information systems architectures in a major intelligence community element supporting both DoD and national intelligence missions.

(U) The contractor in question was provided with accurate, up-to-date classification guidance and regular direction regarding NGA's information security and protection expectations and requirements and caused a security violation due to their flawed implementation of that contractually binding direction.

(S//NF) A reversal by ISCAP of NGA's classification management decision in this matter would result

FOIA(b)(1) NGA

[1] Subsequent to the events involved in this classification challenge, on February 13, 2013 the President signed an Executive Order "Improving Critical Infrastructure Cyber Security," which emphasizes that:

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

(U) Information systems security, network outage management, and vulnerability information has long been protected by NGA as properly classifiable national security information. NGA's approach in this matter is consistent with that of the rest of the Intelligence Community, the Department of Defense, United States Cyber Command, and the spirit and intent of the new Cyber Security Executive Order.

5. (U) Point of contact. The NGA point of contact for this matter is [redacted] who may be reached at [redacted] or [redacted]

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

ATTACHMENTS:

TAB A – (2) DD 254 Tasking Order for delivery of classified materials

20110225 – TOP SECRET Tasking Order, Contract Number N00024-07-D-6200

(U) Section 15K of this Tasking Order provides a complete list of DoD and NGA mandatory compliance documents, to include security classification guides/guidance.

TAB B – Statement of Work (SOW) Memorandum of Understanding

TAB C – ARL-UT Presentation: "MSN OPS Support"

(~~S//~~NF) This Exhibit addresses:

- [redacted]

FOIA(b)(1)

"Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cyber security. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.

"Critical Infrastructure – The term Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacitation 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"

SUBJECT: (U) Advanced Research Lab – University of Texas (ARL-UT) Classification Challenge Appeal to the Interagency Security Classification Appeals Panel (ISCAP)

interruptions. An additional consideration would be Internet connectivity at MSNCC to provide an alternate VPN path.

(S//NF)

FOIA(b)(1) NGA

TAB D – ARL-UT Presentation: "IT/IS Migration dated 25 January 2012

FOIA(b)(6)

(U) Refer to pages 3 and 6. This Exhibit lists:

- Migration schedule (p 6)
- Network IP space to NGA managed addresses (p 3)

TAB E – NGA Security Classification Guide (SCG), Version 1.1, (25 March, 2008; verified current during FCGR, June, 2012)

~~SECRET//NOFORN~~

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

7500 GEOINT Drive
Springfield, Virginia 22150

S-2013-0261-SI

MAR 1 1 2013

MEMORANDUM FOR EXECUTIVE SECRETARY, INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

SUBJECT: (U) Interagency Security Classification Appeals Panel Classification Challenge by Applied Research Laboratories, University of Texas at Austin

REFERENCE: (U) ISCAP letter, Reference: ISCAP No. 2013-030, 7 February 2013 (U)

1. (U) As requested in the referenced letter, the National Geospatial-Intelligence Agency (NGA) submits the following documents as pertinent material and related correspondence regarding the Applied Research Laboratories, University of Texas (ARL-UT) classification challenge appeal to ISCAP:

a. (U) NGA Security Classification Guide (SCG), Version 1.1, 25 March 2008 (S//NF) (enclosure 1).

b. (U) DD Form 254 Tasking Order, Prime Contract Number N00024-07-D-6200 (U) (enclosure 2).

c. (U) Draft Memorandum of Understanding between NGA and Defense Security Service (DSS) (enclosure 3).

d. (U) Executive Order, "Improving Critical Infrastructure Cybersecurity," 12 February 2013 (U) (enclosure 4).

2. (U) The NGA classification determination of SECRET//NOFORN, made on ARL-UT's information, adhered to the strict guidance contained in the NGA Security Classification Guide (SCG), the Geospatial Intelligence SGC Annex: Commercial Electro-Optical Imagery, and DoD 5200.1-H, DoD Handbook for Writing Security Classification Guidance.

CL BY: [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA
Derived from: Multiple Sources
DECL ON: 20380228

UPON REMOVAL OF ENCLOSURE 1, THIS DOCUMENT BECOMES UNCLASSIFIED

~~SECRET//NOFORN~~

S-2013-0261-SI

SUBJECT: (U) Interagency Security Classification Appeals Panel Classification Challenge by Applied Research Laboratories, University of Texas at Austin

3. (U) The NGA point of contact for this matter is [redacted] who may be reached at [redacted] FOIA(b)(3) - 10 USC 424 - DIA, NRO and NGA FOIA(b)(6)

J. Composto
Brigadier General, USMC (Ret.)
Director, Security and Installations Directorate

Enclosures
As stated