CI Investigative Tools Summary Chart

Prepared by DoD Counterintelligence Field Activity (CIFA); POC: [redacted] *9 January 2004 Version*

~~For Official Use Only~~

Authority	Standard/Requirements	What materials does it cover?	How to obtain/Other notes
FISA Pen Register/Trap & Trace Order *50 USC §§ 1841-1846*	[redacted]		
FISA "Business Records" Order *50 USC §§ 1861-1862*			
ECPA National Security Letter (NSL) *Electronic Communications Privacy Act* *18 USC § 2709*			
RFPA NSL *Right to Financial Privacy Act* *12 USC § 3414(a)(5)*			
FCRA NSL *Fair Credit Reporting Act* *15 USC § 1681u*			
FCRA NSL (Terrorism) *Fair Credit Reporting Act* *15 USC § 1681v*			
National Security Act NSL *50 USC § 436*			

General Notes: *All of the information above is intended as a summary of the relevant statutes; many details have been omitted to save space. Consult your legal advisor for applicability in individual cases. All of the NSL provisions above also contain language prohibiting the recipients from disclosing the existence of the NSL to the target. All provisions also carry restrictions on the use and dissemination of the information obtained (although typical use in a CI investigation is generally not a problem).*

Counterintelligence Field Activity

2003 Legal Developments: An Overview for DoD Counterintelligence Operators

As a service to counterintelligence operators, CIFA offers the following summary of significant legal developments relating to counterintelligence. More detailed information on any of the topics addressed here can be obtained from CIFA.[1] *Specific questions about the applicability of these authorities to your operations should be raised with your component's legal counsel.*

Compared to previous two years, 2003 saw relatively few legal developments directly relevant to counterintelligence. The Intelligence Authorization Act for FY2004 made a significant change relating to national security letters for financial information, but otherwise left counterintelligence operational authorities unaltered. Several other provisions of the Act, as well as new guidelines issued by the Justice Department, may indirectly affect DoD CI components.

I. Intelligence Authorization Act for Fiscal Year 2004

The President signed the Intelligence Authorization Act for FY 2004 (Public Law 108-177) on December 13, 2003. Although numerous changes to operational counterintelligence authorities (including changes to the Foreign Intelligence Surveillance Act) had been discussed earlier in the year, the final legislation contains only one – a modification of the national security letter authority for financial records. The Act also included language establishing several "counterintelligence initiatives" and mandated a number of reports.

A. Sections 374: National Security Letters for Financial Information

Section 374 expanded the definition of "financial institution" that applies to "national security letters[2]" issued pursuant to Section 1114[3] of the Right to Financial

---

[redacted] Special Assistant to the Director, CIFA, prepared this summary and is the CIFA point of contact for additional information or feedback. He can be reached at [redacted]

[2] The term "national security letter" does not appear in the statute, but is commonly used to refer to requests

Privacy Act (RFPA). This basically allows RFPA national security letters to be served on a wider variety of institutions, beyond the traditional banks and investment institutions.

By way of background, the RFPA governs the way that financial institutions must safeguard information about their customers, and generally requires that financial institutions inform their customers when a government entity seeks to obtain the financial records of a customer. Section 1114 of the RFPA carves out an exception to this rule, and permits the FBI (and other agencies) to seek "financial records[4]" from "financial institutions" in counterintelligence or counter-terrorism investigations, and prohibits the institution from disclosing this to the customer.

(1) FBI-issued RFPA National Security Letters

Section 1114(a) (5)(A) requires that financial institutions comply with a request for financial records from the FBI, so long as the FBI certifies the records are "sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States." This is the most common form of RFPA national security letters. DoD CI components often make requests for the FBI to issue these letters in joint investigations.

(2) DoD-issued RFPA National Security Letters

Section 1114(a) permits any government agency "authorized to conduct foreign counter- or foreign positive-intelligence activities" or "authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism" to request financial records for the purposes of those investigations/activities. The request must comply with certain forms and be signed by a "supervisory official" designated by the head of the government agency. The financial institution then may release the records without notifying the customer. DoD CI components use this authority directly to issue "national security letters" or "request letters" to financial institutions. The key difference between the FBI's national security letter authority (Section 1114(a)(5)(A)) and that available to DoD directly (Section 1114(a)) is that financial institutions must comply with an FBI letter, and may comply with a DoD (or other agency) request.

---

made by the FBI and other agencies in the context of national security investigations.

[3] Section 1114 of the RFPA is codified at 12 U.S.C. § 3414.

[4] "financial record" means an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution. 12 U.S.C. § 3401(2).

(3) New Definition of "Financial Institution"

Whether issued by the FBI or DoD, RFPA national security letters only apply to "financial institutions," in other words, to institutions regulated by the RFPA. Prior to this year, the relevant definition of "financial institution" was:

> *"any office of a bank, savings bank, card issuer as defined in section 1602(n) of title 15,industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands;"*

This definition, which dates from 1978, is restricted to "traditional" financial institutions like banks, savings and loans, etc. In recent years, a broader range of businesses have been offering services similar to traditional banking (e.g., commercial check cashing establishments, investment houses, on-line brokerage services, insurance companies, car dealerships, etc.). As the government used national security letters to pursue CI subjects making use of less traditional means to handle money, it occasionally encountered businesses that refused to comply with the letter on the grounds that they were not a "financial institution" as defined in the RFPA.

Section 374 of the 2004 Intelligence Authorization Act provides a remedy by applying a different definition of "financial institution" to requests made pursuant to Section 1114. The new definition of "financial institution," which is drawn from Title 31, includes:

> *(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h)));*
>
> *(B) a commercial bank or trust company;*
>
> *(C) a private banker;*
>
> *(D) an agency or branch of a foreign bank in the United States;*
>
> *(E) any credit union;*
>
> *(F) a thrift institution;*
>
> *(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);*
>
> *(H) a broker or dealer in securities or commodities;*
>
> *(I) an investment banker or investment company;*
>
> *(J) a currency exchange;*
>
> *(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;*

(L) an operator of a credit card system;

(M) an insurance company;

(N) a dealer in precious metals, stones, or jewels;

(O) a pawnbroker;

(P) a loan or finance company;

(Q) a travel agency;

(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;

(S) a telegraph company;

(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;

(U) persons involved in real estate closings and settlements;

(V) the United States Postal Service;

(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;

(X) a casino, gambling casino, or gaming establishment with annual gaming revenue of more than $ 1,000,000 which--

(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or

(ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act [25 USCS § 2703(6)]);

(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or

(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

Obviously, the new definition is very broad, and sweeps in every imaginable business that handles significant monetary transactions. According to the conference report accompanying the legislation, it was the intent of Congress to "allow the U.S.

Government to have, through the use of "National Security Letters," greater access to a larger universe of information that goes beyond traditional financial records, but is nonetheless crucial in tracking terrorist finances or espionage activities."

> *CIFA comment: The new definition applies to both FBI and DoD-issued RFPA national security letters, but does not otherwise change the existing Section 1114 authorities. DoD CI components should implement and make use of the expanded definition, as operationally required. As national security letters are served on businesses not already accustomed to receiving them, CI components may encounter the need to educate recipients on the nature and requirements of RFPA national security letters (including the non-disclosure requirement and the cost reimbursement provision).*

B. Section 341: Counterintelligence Initiatives

As means of addressing various concerns about counterintelligence issues, Congress has mandated five counterintelligence "initiatives" in the Act. The Act describes these in very general terms; the actual form of each initiative will depend on how the Executive Branch chooses to implement each initiative. The five initiatives are:

(1) Classified Information Inspection Process

The DCI, acting through the office of the National Counterintelligence Executive (NCIX) will establish an inspection process for all government agencies that handle classified national security information. The goal of the inspection process will be to ensure that classified information is handled properly, and that appropriate operational security measures are in place. The conference report explains that the NCIX will report to Congress on the adequacy of existing investigatory/inspection mechanisms by April 1, 2004, and propose new procedures[5]. The NCIX will then be responsible for implementing the new procedures (or delegating implementation to the various agencies).

(2) Review of Dissemination Lists

The DCI will establish a process annually reviewing the routine dissemination lists of all elements of the Intelligence Community to ensure that all persons on the list continue to have a "particularized need to know" the distributed information.

---

[5] Specifically, the conference language says that NCIX will "include proposed uniform policies and procedures for all Intelligence Community components to conduct annual inspections of each agency's handling of classified information, to include, as appropriate, prohibitions on employee's bringing items such as cameras, document scanners, and personal electronic devices into Intelligence Community facilities." Conference Report (H.R. 108-381), p. 50.

(3) Financial Disclosure Statements

The DCI, acting through the NCIX, will establish a process by which the head of each intelligence community element directs that employees being given access to classified information submit the financial disclosure forms required by Executive Order 12968, § 1.3(b).

(4) Protection of HUMINT

The DCI shall establish "programs and procedures" by which classified information relating to human intelligence is protected from unauthorized disclosure by employees of intelligence community elements.

(5) Espionage Prosecutions

The Attorney General (through the Office of Intelligence Policy and Review), in consultation with the DCI (through the NCIX), will develop policies and procedures "to assist the Attorney General in the consideration of intelligence and national security-related equities in the development of charging documents and related pleadings in espionage prosecutions." According to the conference report language, this initiative reflects concern that the too much sensitive information was disclosed in the criminal indictments filed in recent espionage cases (the Hanssen case is mentioned by name). The report states that, in balancing the needs of a criminal prosecution with the protection of intelligence sources and methods, the Attorney General "should have the benefit of the perspective of counterintelligence professionals before making his decision on how much previously classified or sensitive information should be included in a charging document or related pleading."

CIFA Comment: These first four initiatives all focus on improving the security of classified information by fully implementing existing safeguards and by enforcing new requirements where necessary. They address specific Congressional concerns arising from recent espionage cases (Hanssen, Montes, Regan), as well as general concerns about lax security for classified information. DoD CI components will doubtless be involved in some or all of these initiatives. In addition, the implementation of these initiatives may bring to light persons or situations of counterintelligence interest.

The fifth initiative should be of interest to DoD CI components that have had, or are now investigating, espionage cases. The initiative addresses a common, and frequently contentious, issue in espionage prosecutions. As a principal holder of intelligence equities, DoD could benefit from procedures that more clearly define the mechanism for timely input into the Attorney General's prosecutorial decisions. Hopefully, DoD CI professionals will be among those called upon to contribute to the development of these procedures.

C. Other Provisions of Interest

The Act also contains sections aimed at improving various aspects of the national security apparatus generally. It establishes a training program to improve information sharing between federal, state, and local officials (Section 316); a pilot program to distribute the analysis of certain SIGINT throughout elements of the intelligence community (Section 317); and a pilot program to recruit and train intelligence analysts (Section 318).

The Act, in Sections 351 through 360, requires various reports to Congress, including reports on the insider threat to computer networks, on security background investigations and clearance procedures, on detailing civilian personnel in the intelligence community and DoD, on information sharing policy changes, on strategic planning, on U.S. dependence on computer hardware or software manufactured overseas, on lessons learned from Iraqi Freedom, and reports on aspects of the Terrorist Threat Integration Center (TTIC) and the Terrorist Screening Center.

II. Defense Authorization Act for Fiscal Year 2004

Two sections of the 2004 Defense Authorization Act (Public Law 108-136) address topics of potential interest to DoD CI operators. Section 841 grants DoD the authority to enter into personal services contracts for (1) services deemed necessary and appropriate to DoD activities outside the U.S.; (2) services that directly support the mission of a defense intelligence component or counterintelligence organization of the Department of Defense; and (3) services that directly support the activities of the special operations command of the Department of Defense. This authority is important because it allows DoD to contract directly with an individual for services, as opposed to going through the established contract and procurement process. The authority is designed to allow people with specific critical skills to be made available quickly when the services to be procured are "urgent and unique" and it would not be practicable for DoD to obtain them by other means. An example of this might be the need to bring in a special translator to facilitate an intercept or interrogation. CI operations have encountered such situations in the past, and this authority may prove useful.

Section 1041 addresses the DoD polygraph program and, among other things, repeals the statutory ceiling on the number of DoD counterintelligence polygraphs.

III. New DOJ Guidelines for FBI Investigations

Although not directly applicable to DoD components, many joint FBI-DoD CI investigations will be affected by the issuance of the new "Attorney General's Guidelines

for FBI National Security Investigations and Foreign Intelligence Collection[6]." These guidelines, which the Attorney General issued on October 31, 2003, replace the old "FCI Guidelines" that governed the FBI's counterintelligence and counter-terrorism investigations. Since the passage of the USA PATRIOT Act, DOJ now has revised all of the FBI's operational guidelines to better meet the current national security threats.

The new "National Security Investigation Guidelines" or "NCIG" aim to fully implement the provisions of the PATRIOT Act and the subsequent decisions of the Foreign Intelligence Court of Review. In so doing, they essentially eliminate the distinction between "counterintelligence" and "criminal" investigations for the FBI, and acknowledge that the threat posed by foreign powers and international terrorists is best met by "national security investigations" that use the full range of available investigative tools. The NCIG summarizes this approach as follows:

> *The investigations authorized by these Guidelines serve to protect the national security by providing the basis for, and informing decisions concerning, a variety of measures to deal with threats to the national security. These measures may include, for example, recruitment of double agents and other assets; excluding or removing persons involved in terrorism or espionage from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warning to other federal agencies and officials, state and local governments, and private entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats. In addition, the matters identified by these Guidelines as threats to the national security, including international terrorism and espionage, almost invariably involve possible violations of criminal statutes. Detecting, solving, and preventing these crimes – and, in many cases, arresting and prosecuting the perpetrators – are crucial objectives of national security investigations under these Guidelines. Thus, these investigations are usually both "counterintelligence" investigations and "criminal" investigations.*

CIFA Comment: This approach represents a substantial departure from the traditional dichotomy between criminal and counterintelligence investigations – a division that is maintained in many DoD authorities. DoD CI elements working jointly with the FBI will likely begin to encounter the effects of the new Guidelines as they are implemented this year. In some cases the integrated approach now mandated for the FBI may not be fully consistent with the structure or authorities of the relevant DoD component. Individual CI components may need to examine or adjust their interaction with the FBI to take this into account.

---

[6] The Guidelines are issued pursuant to Executive Order 12,333 and are the FBI's equivalent of DoD 5240.1-R. A redacted, unclassified version of the new guidelines (along with the other revised FBI guidelines) can be found on the DOJ website at www.usdoj.gov/olp/. The full Guidelines are classified SECRET.

CIFA Suspense/Routing Sheet

*Required Actions 1. Signature 2. Prepare Reply 3. Coordinate 4.File 5. INFO 6. Other

To: Name/Office	*Required Action	Comments (or see below)	Initials/Date
DP Admin	Admin Review		[redacted] 27.2.07
[redacted]	3		[redacted] 27-2-07
[redacted]	3		[redacted] 2/27/07
for [redacted]	3		[redacted] 2/27/07
[redacted]	3		[redacted] 01 MAR 07
[redacted]	1		[redacted] 3/1/07
			[redacted]
Chief of Staff			[redacted] 28 Feb 07
Editor	Edit		[redacted] 27 Feb 07

Subject: NSL Report

Suspense Date

Summary/Comments:

Good package – Approved!
Thorough and well written!
We actually met a suspense!
[redacted]

Security Classification ☑

TOP SECRET☐ SECRET☐ CONFIDENTIAL☐ UNCLASSIFIED☒

Action Office Information

Action Officer: [redacted]
Phone: [redacted]

Office: DP
Phone: [redacted]

Administrative Support: DP admin
Phone: [redacted]

Date Prepared: 26 February 2007

Handling Instructions

Return to: [redacted]

Special Instructions:

[redacted]

LOGGED

FEB 28 2007

revision March 2005

COUNTERINTELLIGENCE FIELD ACTIVITY
251 18th STREET
CRYSTAL SQUARE 5, SUITE 1200
Arlington, VA 22202-3537

ACTION MEMO

FOR: ACTING DEPUTY UNDER SECRETARY OF DEFENSE FOR COUNTERINTELLIGENCE AND SECURITY

THROUGH: ACTING DIRECTOR, COUNTERINTELLIGENCE, ODUSD (CI&S)

FROM: James T. Faust, Director, CIFA 3/1/07

SUBJECT: Program Review on DoD Use of National Security Letters (NSLs)

- This memorandum responds to your January 25 request (TAB A) regarding subject review.

- The review was conducted from January 30 to February 21. The CIFA Program Management Directorate interviewed individuals from appropriate offices in OSD, AFOSI, Army INSCOM, and NCIS. The report (TAB B) highlights:

  - DoD guidance on using NSLs.
  - Service philosophies concerning the use of NSLs.
  - Instructional guidance and processes for issuing NSLs.
  - Process times and approval authorities by Service.
  - DoD training.

- The report recommends the Department of Defense:

  - Provide more specific guidance concerning the definition and use of applicable NSL statutes.
  - Review approval authorities to ascertain it is within the intent of applicable NSL statutes.
  - Establish guidelines concerning the legal review of NSL requests.
  - Initiate legislation to expand 15 USC 1681v to include CI investigations.
  - Collect data concerning NSL use and report annual findings to CIFA.
  - Establish standardized training for all DoD basic CI agents and introduce formalized NSL training in JCITA advanced courses.

COORDINATION: TAB C

Attachments:
As stated

Prepared by: [redacted] Deputy, CI Investigations; [redacted]

A

[redacted]

[redacted]

B

DEPARTMENT OF DEFENSE

NATIONAL SECURITY LETTER

PROGRAM REVIEW

CONTENTS

	Page
CONTENTS	2
EXECUTIVE SUMMARY	3
INTRODUCTION	5
Purpose	
Objectives	
DoD CI Components	
Site-visit Team Composition	
REFERENCES	6
DEFINITIONS AND STATUTES	7
DoD GUIDANCE	8
SERVICE IMPLEMENTATION	
Air Force	10
Army	12
Navy	14
TRAINING	16
RECOMMENDATIONS	
Should DoD issue policy concerning the use of NSLs?	17
Should DoD periodically collect data concerning the use of NSLs?	19
Should DoD establish standardized training?	19
Should DoD standardize documents?	20
ENCLOSURES	
1. Memorandum for Director, Counterintelligence Field Activity, Dated 25 Jan 07	21
2. DoDI 5400.15, Enclosure 15	23
3. National Security Letter Statute Extracts	24

EXECUTIVE SUMMARY

On 25 January 2007, the Deputy Undersecretary of Defense, Counterintelligence and Security (DUSD (CI&S)) directed the Counterintelligence Field Activity (CIFA) to conduct a program review (PR) concerning DoD policy and procedures on the use of National Security Letters (NSL) and NSL-Type Letters. [1] From 30 January through 21 February 2007, personnel from CIFA's Program Management Directorate conducted site visits and interviews with key personnel from the Office of the Secretary of Defense (OSD), Washington, DC; Headquarters (HQ), Air Force Office of Special Investigations (AFOSI), Andrews Air Force Base, MD; HQ Army Intelligence and Security Command (INSCOM), Fort Belvoir, VA; and HQ Naval Criminal Investigative Service (NCIS), Washington Navy Yard, DC. The results of the review are documented in this report.

This PR focuses on several factors which include: (1) Definitions and Statutes; (2) A review of DoD Guidance; (3) Service Implementation of the Statutes; (4) Training; and (5) Recommendations. This PR concludes that DoD effectively obtains and uses financial data to further the process of counterintelligence (CI) and counterterrorism (CT) investigations. Even though each service has a differing philosophy on the employment of NSLs, all have established regulatory or instructional guidance governing their respective process. Each process includes a legal review within the investigation approval process and two services conduct another legal review prior to the authorizing official signing the final letter. A detailed outline of each service's process is included in the body of this report.

[redacted]

[1] The definition of National Security Letters was recently modified by the PATRIOT Improvement and Reauthorization act of 2005 – 2006. The authority under which DoD components request financial information no longer falls within the definition of NSL. Nevertheless, the term "NSL" will be utilized throughout this report to avoid confusion. The change in definition does not alter the findings, conclusions, or recommendations contained in this report.

INTRODUCTION

Purpose

This PR was conducted in response to a tasking from DUSD (CI&S) (Enclosure 1). The request directed CIFA to examine how DoD components employ the use of NSLs as an investigative tool, to review their request and approval processes, to cite best practices, and make recommendations pertaining to policy and training.

Objectives

This review focused on the following factors:

1. Definitions and Statutes
2. A review of current DoD Guidance
3. Service Implementation of the Statutes
4. Current Training
5. Recommendations

DoD CI Components

The following are personnel, by office, that were interviewed:

Office of the Secretary of Defense

[redacted]

Naval Criminal Investigative Service

[redacted]

Army Military Intelligence

[redacted]

Air Force Office of Special Investigations

[redacted]

Joint Counterintelligence Training Academy

[redacted]

Site Visit Team Composition

[redacted]

REFERENCES

DoD Directive 5400.12, Obtaining Information from Financial Institutions, Dated 2 Dec 2004
DoD Instruction 5400.15, Guidance on Obtaining Information from Financial Institutions, Dated 2 Dec 04
12 United States Code § 3414 Right to Financial Privacy Act
15 United States Code § 1681v Fair Credit Reporting Act
50 United States Code § 436 National Security Act
Army Regulation 381-20, The Army Counterintelligence Program, 15 Nov 93
Army Regulation 190-6, Obtaining Information from Financial Institutions, 9 Feb 06
AFOSI Manuel 71-119, Counterintelligence Investigations, Approved Draft 11 Feb 02
NCIS General Administration Document OOJ-0002, USA Patriot Act, 26 Feb 03

DEFINITIONS AND STATUTES

Definition: A National Security Letter is a written request by an authorized government agency in authorized national security investigations for limited types of information, such as customer and consumer transaction information, from specified entities, such as U.S. financial institutions, U.S. telecommunications companies, and credit agencies.[2]

Statutes: There are five statutory provisions which authorize specified government officials, primarily from the FBI, to request certain categories of information held by third parties as part of authorized national security investigations. These provisions are:

- Section 1114(a) of the Right to Financial Privacy Act, 12 U.S.C. § 3414
- Section 626 of the Fair Credit Reporting Act, 15 U.S.C. § 1681u
- Section 627 of the Fair Credit Reporting Act, 15 U.S.C. § 1681v
- Section 2709 of Title 18, U.S. Code, 18 U.S.C. § 2709
- Section 802 of the National Security Act, 50 U.S.C. § 436

These statutes have been referred to collectively as the "NSL statutes." Three of the statutes listed above permit specified government officials other than the FBI to request customer and consumer transaction information in authorized investigations. These statues are: the Right to Financial Privacy Act; the Fair Credit Reporting Act (15 U.S.C. § 1681v); and the National Security Act. The remaining two statutes provide exclusive authority to the FBI.

DoD components are authorized to submit their requests for financial information through their respective FBI field office. When the FBI accepts the request, they process the NSL under one of their respective statutes. Compliance with an NSL issued by the FBI is mandatory. In most cases when the FBI issues an NSL at the behest of a DoD component, the request is part of a joint FBI/DoD investigation. However, a DoD component can submit a Request for Assistance (RFA) where the FBI issues an NSL on a DoD investigation (not joint with the FBI).

DoD may also request information under authorities of the "NSL statutes": Right to Financial Privacy Act; the Fair Credit Reporting Act, and the National Security Act. DoD does not use the specific term National Security Letter in written requests. DoD components send written requests for information to institutions and entities under the NSL statutes as permitted law. Because these are requests for information rather than court orders, a DoD request under the NSL statutes cannot be compelled absent court involvement.

The following DoD components are authorized to make requests for information under the NSL statutes in support of CI and CT investigations:

---

[2] As noted on Footnote 1 on Page 3, the definition of an NSL no longer includes financial record checks routinely requested by DoD components. This change was documented in the PATRIOT Improvement and Reauthorization act of 2005 – 2006.

The following DoD components are authorized to make requests for information under the NSL statutes in support of CI and CT investigations:

- U.S. Army Criminal Investigation Command
- U.S. Army Counterintelligence
- Naval Criminal Investigative Service
- U.S. Air Force Office of Special Investigations

DoD GUIDANCE

DoD Directive 5400.12, Obtaining Information from Financial Institutions, provides all DoD components with initial guidance. This directive highlights several important factors:

1. Reference to DoD Instruction 5400.15, Guidance on Obtaining Information from Financial Institutions.
2. Applicability and Scope which defines DoD Components.
3. Section 4, Policy, states: "Authorization of the customer to whom the financial records pertain shall be sought unless doing so compromises or harmfully delays either a legitimate law enforcement inquiry or a lawful intelligence activity."
4. Section 5, Responsibilities, states: "5.2. The Secretaries of the Military Departments and the Heads of the affected DoD Components shall: (5.2.1) Implement policies and procedures to ensure implementation of this Directive and reference (b) when seeking access to financial records."

DoD Instruction 5400.15:

Within this instruction, Enclosure 7, Requests for Financial Records in Connection with Foreign Intelligence and Foreign Counterintelligence Activities, states the following:

Paragraph E7.1.1 "Financial records may be obtained from a financial institution (as identified at paragraph E2.1.3.) by an intelligence organization, as identified in DoD 5240.1 (reference (i)), authorized to conduct intelligence activities, to include investigation or analyses related to international terrorism, pursuant to references (i) and Executive Order 12333 (reference (j))."

1. Paragraph E2.1.3 defines Financial Institutions (for intelligence purposes only).
2. DoD Directive 5240.1, defines the respective intelligence components within DoD that are authorized to conduct intelligence activities.

Paragraph E7.1.3 "When a request for financial records is made under paragraph E7.1.1., above, a Component official designated by the Secretary of Defense, the Secretary of a Military Department, or the Head of the DoD Component authorized to conduct foreign intelligence or foreign counterintelligence activities shall certify to the financial institution that the requesting component has complied with the provisions of reference (b). Such certification in a format similar to enclosure 15 shall be made before obtaining any records."

1. Enclosure 15 of DoDI 5400.15 provides a sample which is attached as Enclosure 2.
2. Reference (b) in this paragraph refers to Chapter 35 of 12 U.S.C. Right to Financial Privacy Act of 1978.

E7.1.4. "An intelligence organization requesting financial records under paragraph E7.1.1., above, may notify the financial institution from which records are sought that section 3414(3) of reference (b) prohibits disclosure to any person by the institution, its agents, or employees that financial records have been sought or obtained."

E7.1.5. "An intelligence organization requesting financial records under paragraph E7.1.1., above, shall maintain an annual tabulation of the occasions in which this access procedure was used."

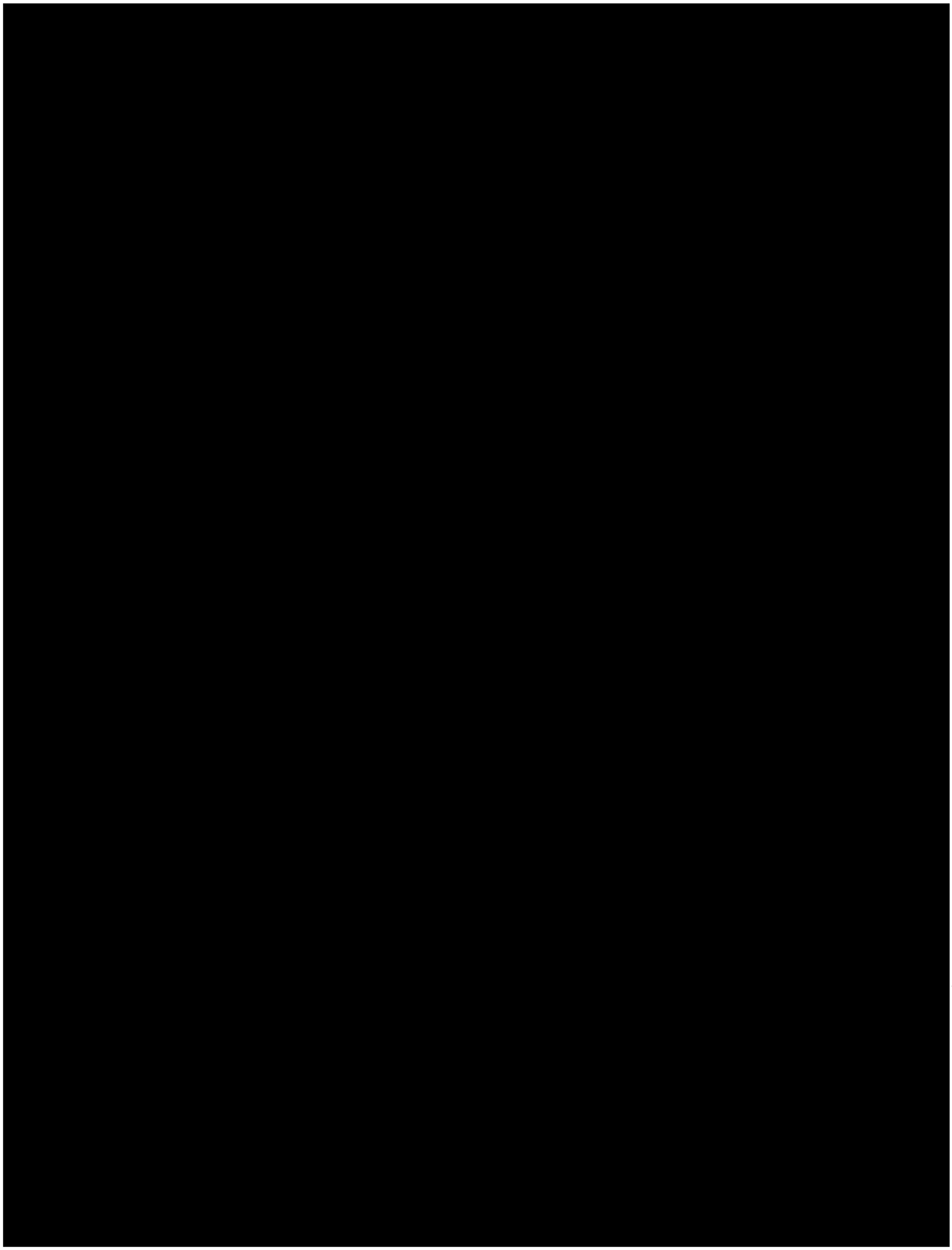
SERVICE IMPLEMENTATION

AFOSI

Philosophy: AFOSI has traditionally exercised its authority to issue NSLs primarily under the Right to Financial Privacy Act, 12 U.S.C. § 3414. Most stateside AFOSI CI and CT investigations are conducted jointly with the FBI. Since an AFOSI NSL is viewed as a request for information which the financial institution could refuse to comply with, and a request from the FBI pursuant to any of the three statutes is compulsory, [redacted] To, date, AFOSI cannot cite any CI or CT investigation where the FBI has refused to issue an NSL. Another benefit to processing the letter through the FBI is the available analytic support provided by the FBI that assists in filtering through the vast amount of data that result from NSL requests. AFOSI views this as a force multiplier, which allows their agents to pursue other aspects of the investigation.

Note: While this approach to the use of NSLs differs from the other two services, it fully supports those investigations that require access to financial data and conforms to all legal guidelines governing the use of NSLs.

Instruction/Regulations: [redacted]



ARMY Military Intelligence (MI)

Philosophy: Army MI exercises its authority to issue NSLs primarily under the Right to Financial Privacy Act, 12 U.S.C. § 3414. Army MI views NSLs as a valuable investigative tool and uses them when they meet the criteria of a logical investigative step. MI understands the authorities they have under all three statutes, but they also recognize the manpower trail associated with this tool. Any records received as a result of the request must be sorted through and analyzed to extract information they seek, or before additional leads are developed. If Army MI is conducting a joint case with the FBI, the responsibility for issuing NSLs is determined through mutual agreement (division of labor) at the field unit level. Army MI plans to continue using NSLs when pertinent.

Instruction/Regulations: Army Regulation 381-20 and Army Regulation 190-6 provide guidance on the use of NSLs.

[redacted]

Naval Criminal Investigative Service (NCIS)

Philosophy: NCIS exercises its authority to issue NSLs under all three statutes that pertain to DoD. They view NSLs as an invaluable investigative tool which they use not only to verify existing information, but to serve as a lead generation tool. According to DoD statistics, NCIS issues more letters than the other DoD agencies. They effectively and efficiently employ NSLs through detailed program management, investigative oversight, and training. The attorneys in the National Security Law Unit (NSLU) are responsible for providing the legal review on NSLs. One of the attorneys is embedded within the Counterintelligence Directorate, enabling her to be involved in all steps of the investigative process and remain intimately familiar of the status of an investigation as it progresses. NCIS plans to increase the utilization of this investigative and lead generation process through program direction, timely investigative review, and increased awareness training.

Instruction/Regulations: General Administrative Order OOJ-0002.

Process: The NCIS process for issuing an NSL follows:

1. The case agent submits a draft NSL along with the supporting documentation to the appropriate NCIS desk officer (CI or CT). In many cases, these investigations have already been identified as Special Interest or Director Special Interest cases. Because of this status, HQ NCIS desk officers and the legal unit are intimately familiar with the case.
2. If the desk officer finds the documentation meets all requirements, it is forwarded to an attorney in the NCIS NSLU for a legal review.
3. The NSLU attorney reviews the documentation to ensure all criteria of the relevant statute are met and that the draft NSL contains all required information.
4. If the NSLU legal review supports the request for an NSL, the documentation is forwarded to senior officials at NCIS headquarters for final review and signature. The total number of headquarters officials authorized to sign an NSL within NCIS varies depending upon which statute is invoked.
5. Assuming an authorized senior NCIS official signs the NSL, the case agent or desk officer must contact the intended recipient of the NSL before it can be transmitted (usually electronically), to assure the recipient is appropriately sensitized to both investigative and privacy considerations.

Process Time: The turn-around time from the initial request to the time HQ NCIS transmits the letter is usually within twenty-four hours.

Approval Authorities: The NCIS Director, NCIS Deputy Directors, and Executive Assistant Directors for CI and CT have approval authority for all three statutes that pertain to DoD. The

Approval Authorities: The NCIS Director, NCIS Deputy Directors, and Executive Assistant Directors for CI and CT have approval authority for all three statutes that pertain to DoD. The Deputy Assistant Directors for CI and CT may sign letters pursuant to 12 USC § 3414 and 15 USC § 1681v.

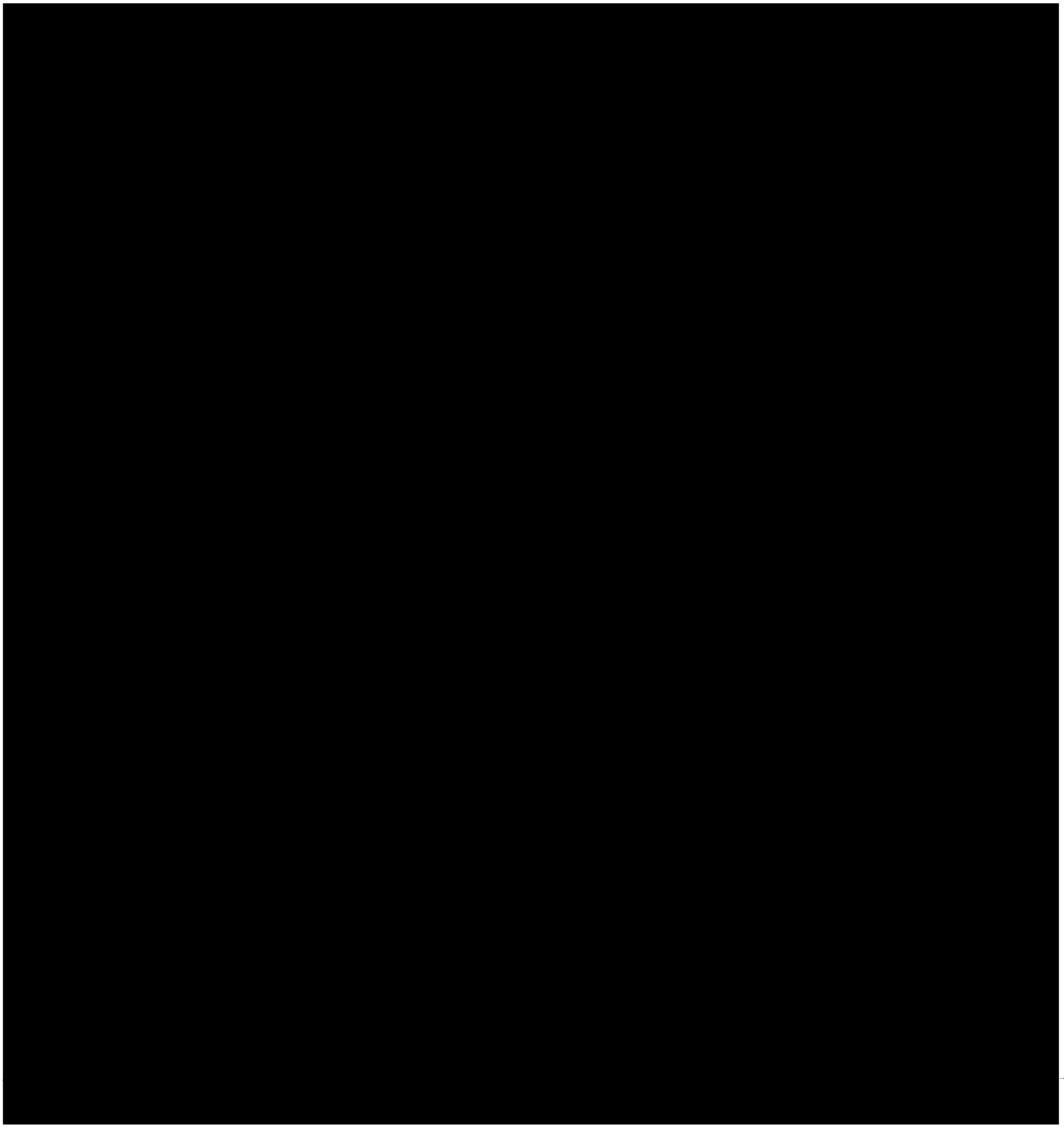
Statistics

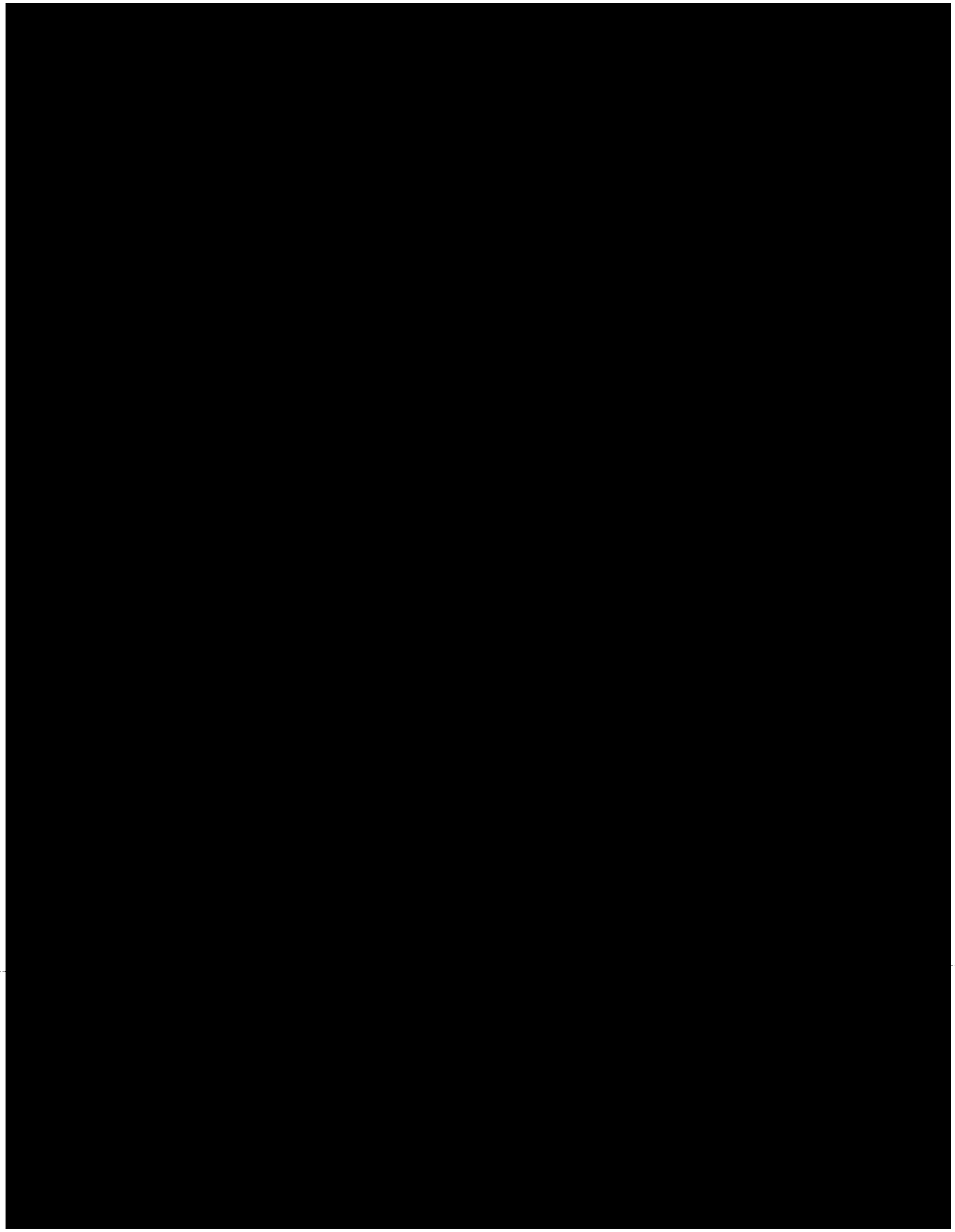
[redacted]

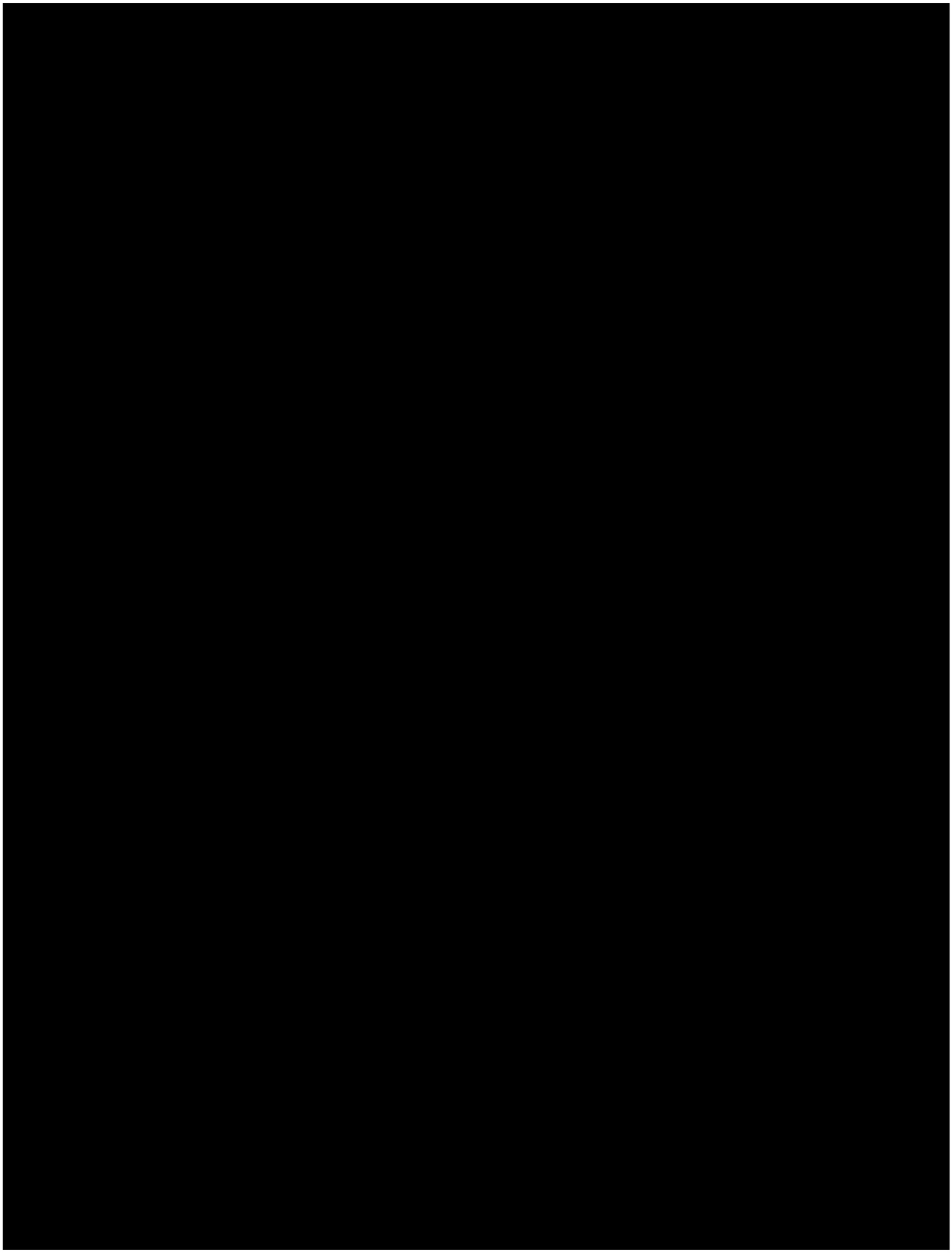
TRAINING

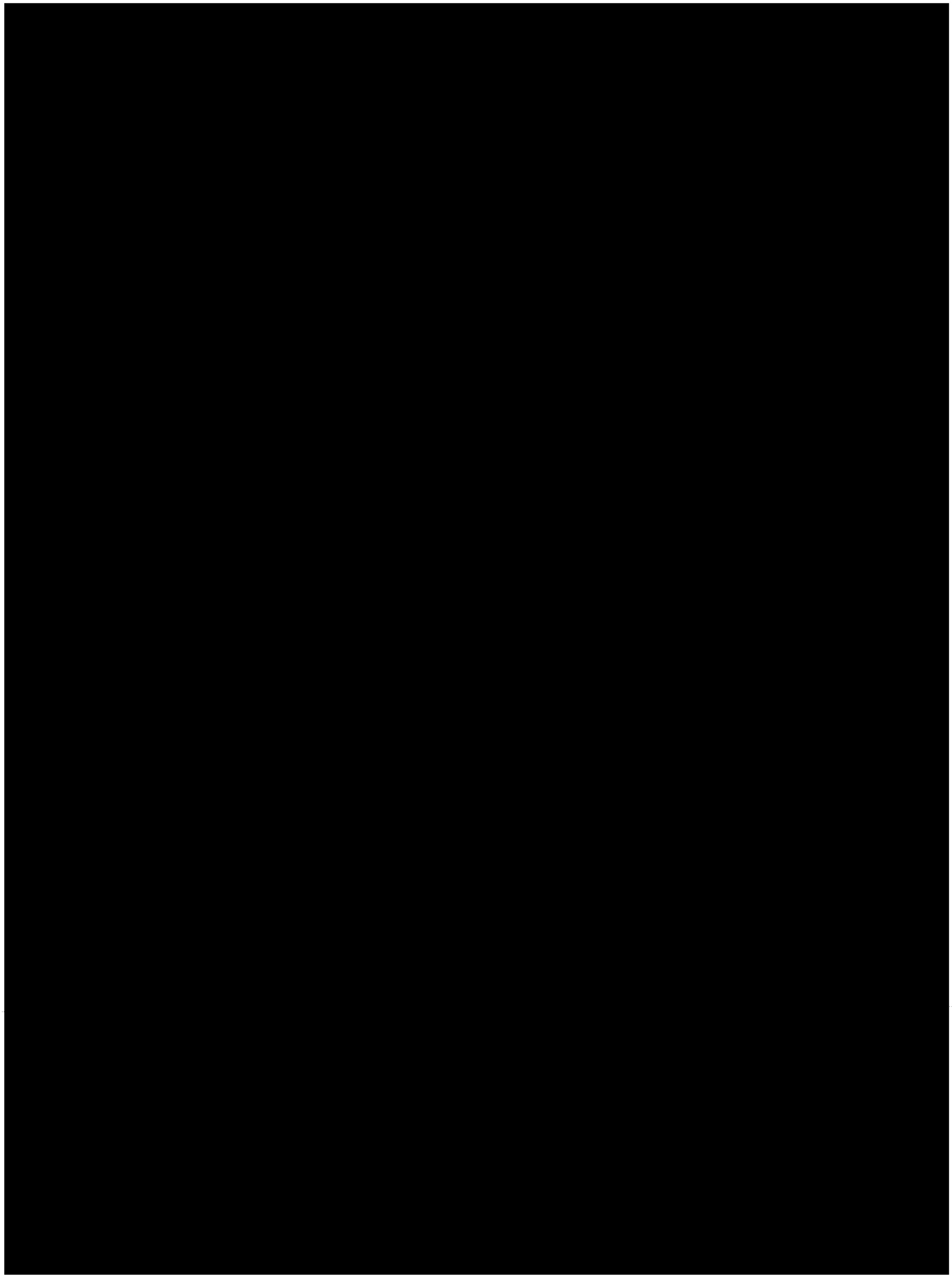
Within DoD, each of the services have several opportunities where training on the use of NSLs could be addressed. New agents to AFOSI and NCIS receive basic law enforcement training at the Federal Law Enforcement Training Center in Georgia. After the basic course each service has a supplemental counterintelligence course that all agents are required to attend. Army MI agents attend their basic CI training at the United States Army Intelligence Center and School, Fort Huachuca, AZ. Each service reviewed their respective programs of instruction for basic courses and verified new agents do not receive NSL specific training.

CI and CT agents are also able to attend advanced courses and seminars at the Joint Counterintelligence Training Academy in Elkridge, MD. There are two main courses where NSL specific training would prove advantageous for service investigators. They are the Joint Terrorism Task Force Seminar and the National Securities Investigation Course. Another course that would benefit Defense Agency personnel is the DoD CI Agent Certification Course. Officials at JCITA reviewed the programs of instruction for each of the listed courses and verified NSL specific training is not provided as part of the current curriculum. However, JCITA did advise NSLs are addressed in the law blocks of instruction which are presented at the National Securities Investigation Course and DoD CI Agent Certification Course. The statutes are usually addressed by the lawyers teaching the respective blocks of instruction which in turn generates additional dialog.









E15. ENCLOSURE 15

FORMAT FOR CERTIFICATE OF COMPLIANCE WITH
THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

[Official Letterhead]

[Date]

Mr./Mrs. XXXXXXXXXX
Manager
Army Federal Credit Union
Fort Anywhere, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXX

I certify, pursuant to section 3403(b) of the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et. seq., that the applicable provisions of that statute have been complied with as to the [Customer's authorization, administrative subpoena or summons, search warrant, judicial subpoena, formal written request, emergency access, as applicable] presented on [date], for the following financial records of [customer's name]:

[Describe the specific records]

Pursuant to section 3417(c) of the Right to Financial Privacy Act of 1978, good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records.

[Official Signature Block]

ENCLOSURE 3

12 U.S.C. 3414

(a)(1) Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 of this title) shall apply to the production and disclosure of financial records pursuant to requests from:

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities;

(B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 3 U.S.C. 202, Public Law 90-331, as amended); or

(C) a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

15 U.S.C. 1681v.

(a) Disclosure

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.

(b) Form of certification

The certification described in subsection (a) shall be signed by a supervisory official designated by the head of a Federal agency or an officer of a Federal agency whose appointment to office is required to be made by the President, by and with the advice and consent of the Senate.

(c) Confidentiality

50 U.S.C. 436.

(a) Generally

(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where —

(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Each such request —

(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that —

(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

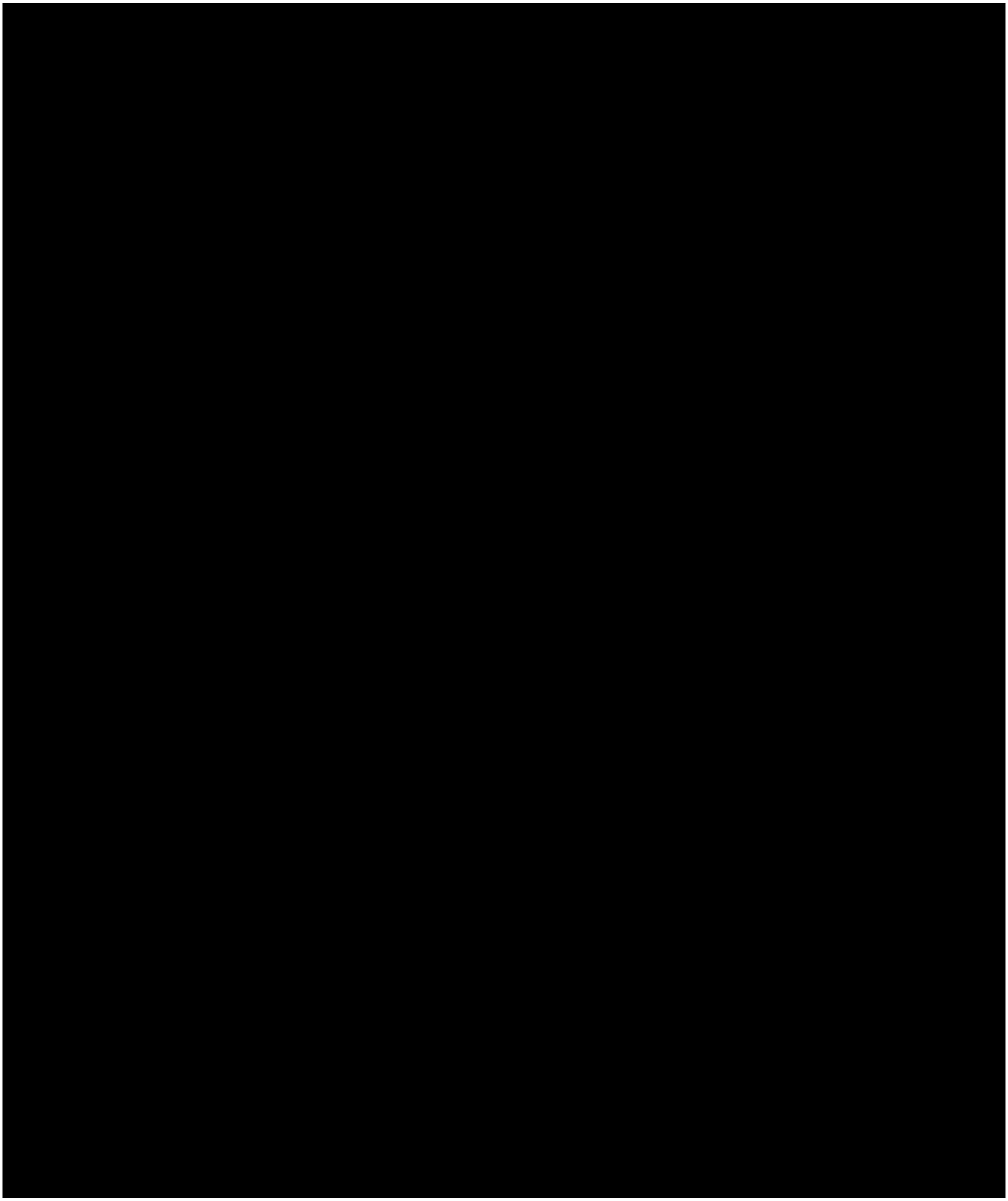
(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

C

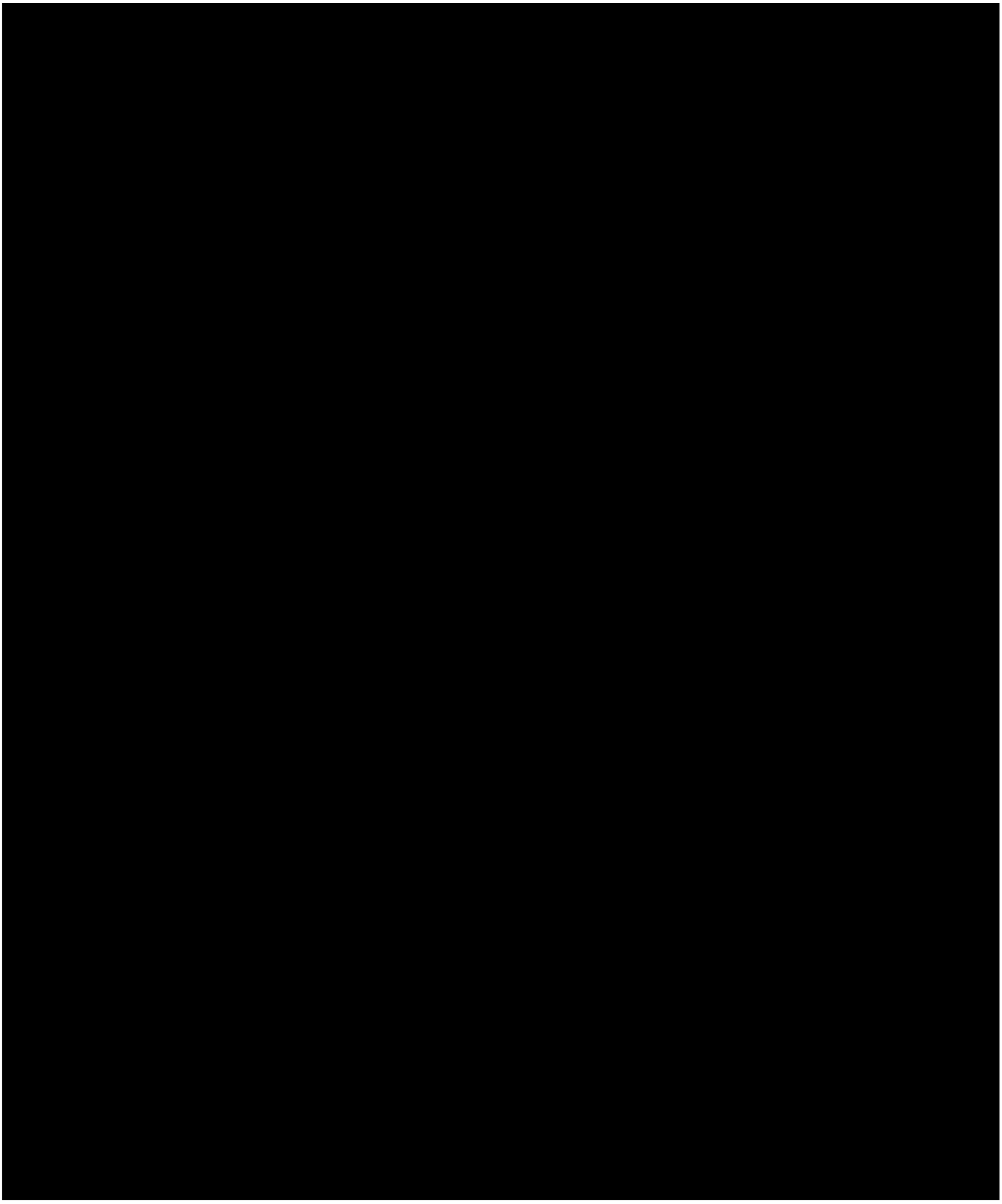
COORDINATION

DUSD (CI&S)	[redacted]	January 30, 2007
OSD (OGC)		February 1, 2007
OUDA(I) Congressional Affairs		February 1, 2007
NCIS-NSLU		February 5, 2007
Army G2-A2X		February 6, 2007
HQ AFOSI/XOQ		February 6, 2007
HQ AFOSI-Legal		February 6, 2007
JCITA		February 7, 2007



[redacted]

[redacted]



[redacted]

US Bank
Custodian of Records
800 Main Street
Minneapolis, MN 55402
Fax (xxx) xxx-xxxx

Dear Custodian of Records:

Pursuant to Executive Order 12333 and the Right to Financial Privacy Act (Act), 12 United States Code §§3401, et seq., you are requested to provide the Naval Criminal Investigative Service with the name, address and financial records pertaining to the customer or accounts listed below:

Customer Name: if available

Address: if available

Date of birth: if available

Social Security: if available

Account numbers: if available

Requested period: if applicable (you may be required to pay for the records/search)

Pursuant to Section 3403(b) of the Act, I certify that NCIS has complied with the Special Procedures Provision contained in Section 3414. In accordance with Section 3417(c), your good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these records.

Please note that disclosing this request to the customer or others without a need to know in order to process this request may result in danger to the national security of the United States and interference with a counterterrorism or counterintelligence investigation. Accordingly, your company or its officers, employees, or agents are prohibited from disclosing to the customer that these records have been sought or obtained.

As a result of the sensitive nature of this request, please contact NCIS Special Agent _____ at (xxx) xxx-xxxx to make arrangements to provide the records. Thank you for your cooperation in this matter.

Sincerely,

Director, DD, AD for CI, AD for CT, or DAD for CI, or DAD for CT

NCIS PROCESS FOR USE OF NSLs

NCIS exercises its authority to issue National Security Letters (NSLs) under three statutes: The Right to Financial Privacy Act, or RFPA (12 USC 3414, authority dating to 1978), which may be exercised in counterintelligence (including counterterrorism) investigations; the Fair Credit Reporting Act, or FCRA (15 USC 1681v, authority dating to 2001), which may be exercised in support of counterterrorism investigations, activities, or analysis; and the National Security Act (50 USC 436, authority dating to 1994) that authorizes government investigative agencies to request - as part of an authorized law enforcement investigation, counterintelligence inquiry, or security determination - certain financial, consumer reporting, and commercial information pertaining to government personnel for which they have investigative responsibility and who meet certain criteria, including recent access to classified information. NCIS exercises these authorities only in certain circumstances: (1) In those cases in which the agency has primary jurisdiction; (2) In those cases in which the FBI has deferred primary jurisdiction to NCIS; or (3) In those cases in which the FBI asks NCIS to issue such an NSL in furtherance of a joint NCIS-FBI investigation.

The NCIS process for issuing an NSL under each of the applicable statutes is as follows:

1. The case agent submits a draft NSL, along with the supporting documentation, to the appropriate NCIS desk officer (CI or CT).

2. If the desk officer finds the documentation meets all requirements, it is forwarded to an attorney in the NCIS National Security Law Unit (NSLU) for a legal review.

3. The NSLU attorney reviews the documentation to ensure that all the criteria of the relevant statute are met and that the draft NSL contains all required information.

4. If the NSLU legal review supports the request for an NSL, the documentation is forwarded to one of a small number of senior officials at NCIS headquarters for final review and signature. The total number of headquarters officials authorized to sign an NSL within NCIS varies depending upon which statute is invoked, but in no case exceeds seven.

5. Assuming an authorized senior NCIS official signs the NSL, the case agent or desk officer must contact the intended recipient of the NSL before it can be transmitted, in order to assure that the recipient is appropriately sensitized to both investigative and privacy considerations.

NCIS Process for Use of National Security Letters

The NCIS process for issuing an NSL under each of the applicable statutes is as follows:

1. The case agent submits a draft NSL along with the supporting documentation to the appropriate NCIS desk officer (CI or CT). In most cases, these investigations have already been identified as Special Interest or Director Special Interest cases. Because of this status the HQ NCIS desk officers and the legal unit are intimately familiar with the case.

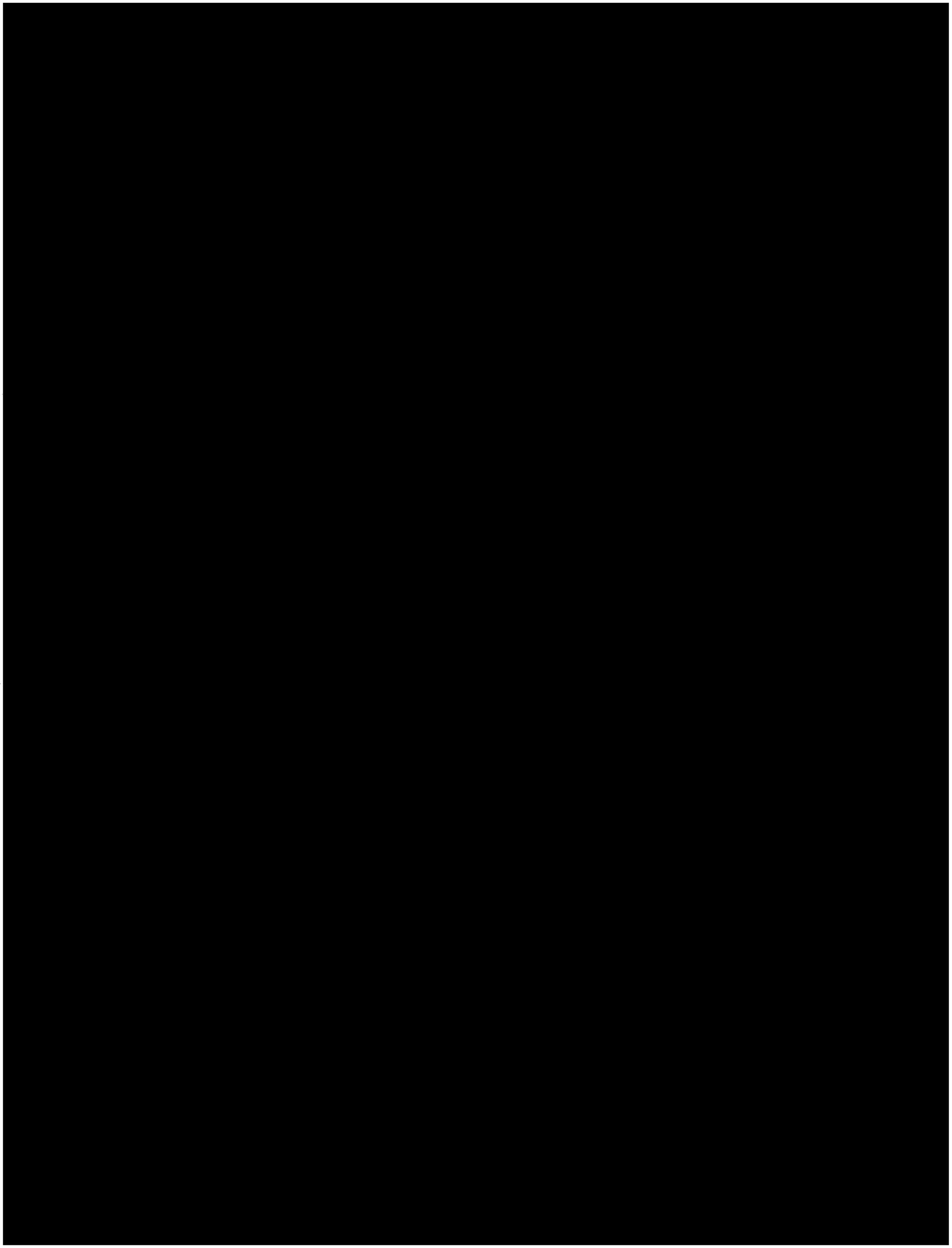
2. If the desk officer finds the documentation meets all requirements, it is forwarded to an attorney in the NCIS National Security Law Unit (NSLU) for a legal review.

3. The NSLU attorney reviews the documentation to ensure all criteria of the relevant statute are met and that the draft NSL contains all required information.

4. If the NSLU legal review supports the request for an NSL, the documentation is forwarded to senior officials at NCIS headquarters for final review and signature. The total number of headquarters officials authorized to sign an NSL within NCIS varies depending upon which statute is invoked.

5. Assuming an authorized senior NCIS official signs the NSL, the case agent or desk officer must contact the intended recipient of the NSL before it can be transmitted (usually electronically), to assure the recipient is appropriately sensitized to both investigative and privacy considerations.

The turn-around time from the initial request to the time HQ NCIS transmits the letter is usually within twenty-four hours.



[redacted]

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

15-10 Financial Checks

a. Legal and Regulatory Framework. The right to privacy extends to the financial aspects of a person's life. Because the U.S. financial system is complex and consists of several different types of institutions each covered by different laws and regulations; it will come as no surprise that there are also several portions of the USC that government's ability to access those records. In the following paragraphs the major relevant portions of the USC are identified and discussed with an emphasis on the authorities, exceptions and procedures that allow CI agents to access them.

(1) Fair Credit Reporting Act (15 USC 1681). The Fair Credit Reporting Act was passed to ensure the privacy, as well as the fair and accurate reporting of consumer credit information for a multitude of purposes including employment and credit worthiness. The act significantly restricts the ability of the government to perform un-consented checks of consumer reporting agency records (AKA credit reporting services). Generally, these records can be obtained only with consent or by a warrant, judicial or administrative subpoena or other court order.

(a) Exception for Identifying Data. A general exemption (15 USC 1681f) allows all governmental agencies (including Army CI) access to limited identification information. Upon the presentation of a formal written request, consumer reporting agencies will provide, name and address, former addresses, places of employment and former places of employment for named consumers. This limited authority can be used for all authorized investigative and operational purposes. (LINK to template of Request)

(b) FBI CI Exception. The original act provided the FBI a specific exception for disclosures for CI purposes (15 USC 1681u). A similar general exception for military CI services does not exist. However, the FBI exception specifically authorized the FBI to disseminate results of their checks to appropriate investigative authorities within the military as may be necessary for the conduct of a joint foreign CI investigation. Additionally, it authorizes the FBI to provide information to the military for SUBJECTs who fall under the UCMJ.

(c) Exception for International Terrorism. The PATRIOT Act added a broader exception for international terrorism (15 USC 1681v), which allows **any government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism** to conduct un-consented checks of these records. Army CI may utilize this exception. A formal written request certifying compliance with the code is required. (LINK to Consumer Reporting Services Template)

(2) Right to Financial Privacy Act of 1978 (12 USC 3401-3422). The Right to Financial Privacy Act is the primary source of financial privacy rights and governs a broad spectrum of records across a wide variety of financial institutions. Government access to records

of financial institutions may be obtained through consent, search warrant, administrative or judicial subpoena, court order or formal written request.

(a) FCI and Terrorism Exceptions. Specific exceptions exist for FCI and international terrorism (15 USC 3414(a)(1)(a) and (c) respectively). These exceptions apply to any government authority authorized to conduct foreign counterintelligence, positive intelligence or international terrorism activities. They allow un-consented checks of financial institution records upon presentation of an appropriately signed formal written request certifying compliance with the act. (LINK to template)

(b) Definition of Financial Institution. The definition of financial institution for the purposes of the exceptions outline above is broader than for the rest of the act (see 15 USC 3414(d)). The following are defined as financial institutions IAW 31 USC 5312(a)(2) and (c)(1).

(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813 (h)));
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) any credit union;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones, or jewels;
(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and settlements;
(V) the United States Postal Service;
(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which—
(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or

(ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

(c) Army Implementation Guidance. AR 190-6, Obtaining Information from Financial Institutions, dated 15 January 1982, implements DODD 2400.12 and the Right to Financial Privacy Act of 1978 (12 USC 3401 *et seq*). It provides additional guidance on obtaining information from financial institutions by consent, search warrant, judicial subpoena, and formal written request. Generic sample templates for each type of request are provided. A specific exception for Foreign Intelligence and Foreign Counterintelligence may be found at para 2-10. This paragraph also delegates signature authority for certificates of compliance with 12 USC 3414(a)(3) to Military Intelligence Group Commanders, investigative control office, CG (or DCG) INSCOM.

[redacted]

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

[redacted]

c. Financial Crimes Information Network (FINCEN) Checks. FINCEN checks are considered a NAC, therefore ACCO will coordinate all FINCEN checks. This is the only authorized channel for FINCEN queries. The following information must be provided to ACCO for each request: ACCO CCN; Full name, any/all AKA, relationship in case (subject/witness); Address and phone number; DPOB; SSAN; Race/ethnicity; Sex; Height/weight; Color of eyes and hair; Other identifying data if available, such as passport number; Financial institution(s) known to be utilized; If joint/bilateral case, list other agencies involved. Specify what type of product you desire from FINCEN e.g. analytical reports and/or data base extracts.

[redacted]

Subject: FW: NSLs and the SASC (U)

-----Original Message-----
From: [redacted]
Sent: Friday, February 02, 2007 3:38 PM
[redacted]
Subject: RE: NSLs and the SASC (U)

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, February 02, 2007 10:00 AM
[redacted]
Subject: FW: NSLs and the SASC (U)

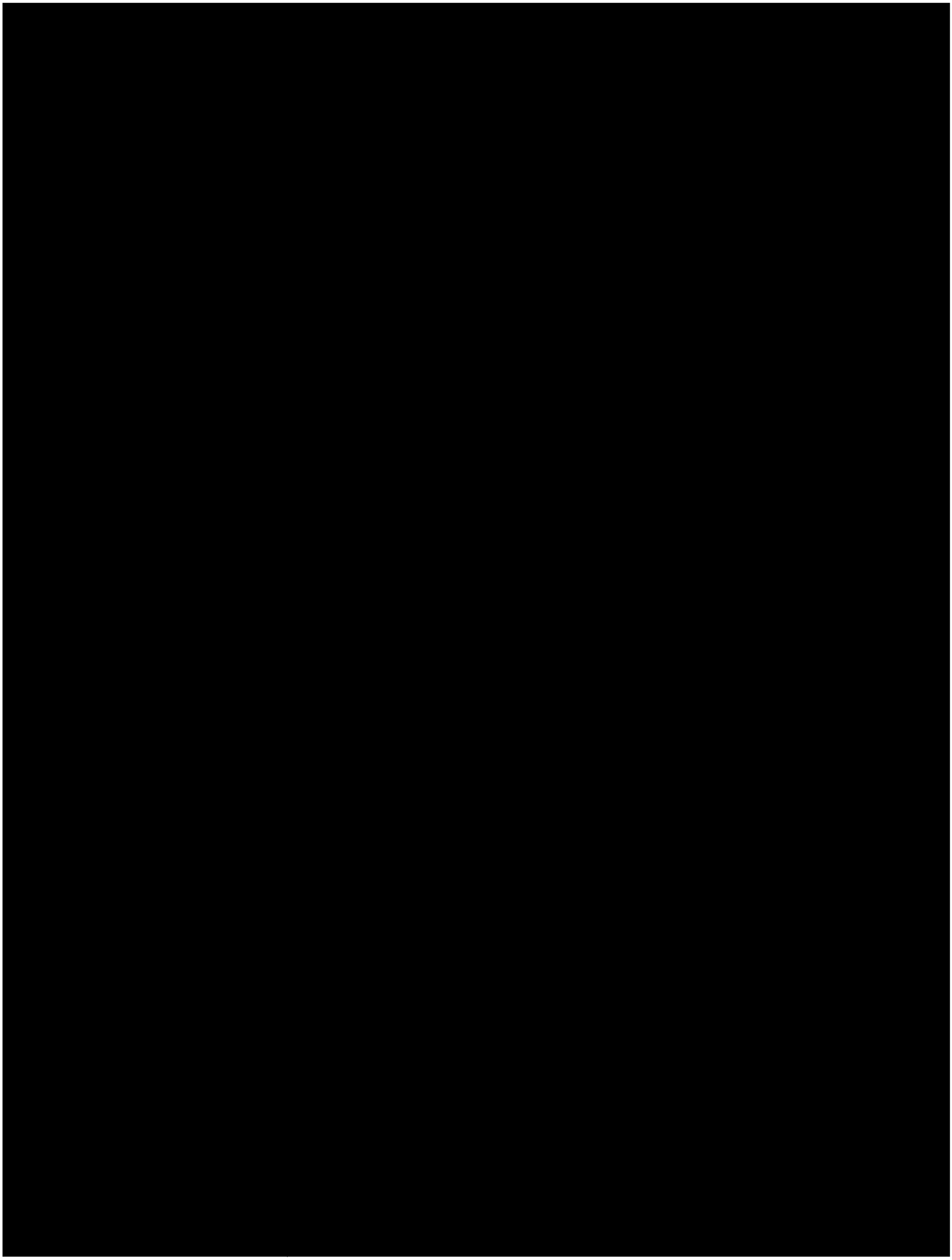
UNCLASSIFIED

[redacted]

V/R,
[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 30, 2007 5:12 PM
To: [redacted]
Subject: FW: NSLs and the SASC (U)

[redacted]



[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:59 AM
To: [redacted]
Cc: [redacted]
Subject: FW: NSLs and the SASC (U)

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:46 AM
[redacted]
Subject: NSLs and the SASC (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Please contact [redacted] if you have any questions.

Regards,

[redacted]

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
HEADQUARTERS, 902D MILITARY INTELLIGENCE GROUP
FORT GEORGE G. MEADE, MARYLAND 20755-5910

[redacted]

To Whom It May Concern,

Under the provisions of the Right to Financial Privacy Act of 1978 (hereinafter the ACT), Title 12, U.S.C. 3401 *et seq*., the Department of the Army requests that your institution provide financial and credit information, to include any record information, concerning the individual identified below.

[redacted]
Account Number: [redacted]

This letter certifies that the Department of the Army has complied with the applicable provisions of the Act. Title 12, U.S.C. 3417 (c) specifies that good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records. The authorization to endorse this certificate has been delegated to me by the Secretary of the Army, contained in paragraph 2-10b(1), U.S. Army Regulation 190-6, Obtaining Information From Financial Institutions.

Title 12, U.S.C. 3414 (a) (3) prohibits your institution, employees, or agents of your institution from disclosing to any person that we have sought or obtained access to a customer's financial records.

In accordance with Title 12, U.S.C. 3415, we will reimburse your institution for such costs as are reasonably necessary and which have been directly incurred in searching for, reproducing, or transporting books, papers, records, or other data required or requested to be reproduced.

Thank you for your cooperation and assistance given to the Department of the Army, this command, and the Special Agent who presented this certificate.

Sincerely,

[redacted]

On 25 January 2007, the Deputy Under Secretary of Defense, Counterintelligence and Security, tasked the Counterintelligence Field Activity to conduct a Program Review concerning service policy and procedures on the use of National Security Letters and NSL-Type Letters. This Executive Summary outlines the results of that review.

The process to obtain an NSL or Bank Record checks varies by service.

All three services advised they have regulations or instructions that cite their authority to issue NSL's or NSL-Type Letters (Bank Letters).

NCIS	General Administrative Order 00-JTAC-0002
AFOSI	[redacted]
Army MI	Army Regulation 381-20 Army Regulation 190-6

[redacted]

NCIS views NSL's as an investigative tool which should produce addition leads or help verify information during the course of an investigation. NCIS has steadily increased their use of NSL' over the last four years and they intend to expand their use through increased awareness training and HQ NCIS oversight of Special Interest or Director Special Interest Investigations. NCIS exercises its authority to issue National Security Letters (NSLs) under three statutes:

1. The Right to Financial Privacy Act, or RFPA (12 USC 3414, authority dating to 1978), which may be exercised in counterintelligence (including counterterrorism) investigations.
2. The Fair Credit Reporting Act, or FCRA (15 USC 1681v, authority dating to 2001), which may be exercised in support of counterterrorism investigations, activities, or analysis.
3. The National Security Act (50 USC 436, authority dating to 1994) that authorizes government investigative agencies to request as part of an authorized law enforcement investigation, counterintelligence inquiry, or security determination; certain financial, consumer reporting, and commercial information. The request must pertain to government personnel for which NCIS has investigative responsibility and who meet certain criteria, including recent access to classified information.

NCIS exercises these authorities only in certain circumstances:

1. Cases in which the NCIS has primary jurisdiction.
2. Cases in which the FBI has deferred primary jurisdiction to NCIS.
3. Cases in which the FBI asks NCIS to issue such an NSL in furtherance of a joint NCIS/FBI investigation.

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

(ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

(c) Army Implementation Guidance. AR 190-6, Obtaining Information from Financial Institutions, dated 15 January 1982, implements DODD 2400.12 and the Right to Financial Privacy Act of 1978 (12 USC 3401 *et seq*). It provides additional guidance on obtaining information from financial institutions by consent, search warrant, judicial subpoena, and formal written request. Generic sample templates for each type of request are provided. A specific exception for Foreign Intelligence and Foreign Counterintelligence may be found at para 2-10. This paragraph also delegates signature authority for certificates of compliance with 12 USC 3414(a)(3) to Military Intelligence Group Commanders, investigative control office, CG (or DCG) INSCOM.

[redacted]

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

[redacted]

c. Financial Crimes Information Network (FINCEN) Checks. FINCEN checks are considered a NAC, therefore ACCO will coordinate all FINCEN checks. This is the only authorized channel for FINCEN queries. The following information must be provided to ACCO for each request: ACCO CCN; Full name, any/all AKA, relationship in case (subject/witness); Address and phone number; DPOB; SSAN; Race/ethnicity; Sex; Height/weight; Color of eyes and hair; Other identifying data if available, such as passport number; Financial institution(s) known to be utilized; If joint/bilateral case, list other agencies involved. Specify what type of product you desire from FINCEN e.g. analytical reports and/or data base extracts.

billets or be required to use a Government mess when such use would be detrimental to the mission. TDY orders will reflect that the use of Government billeting and mess facilities would be detrimental to the mission.

e. Applicability. These provisions apply both overseas and within the United States.

8–9. Weapons

a. CI personnel may carry weapons openly or concealed as required in the performance of peacetime official duties, in accordance with AR 190–14, when authorized by a field grade officer. Commanders will ensure the individual has met the requirements of AR 190–14 and weapons qualification requirements. Weapons storage will comply with current regulatory requirements.

b. During deployments, crisis, transition to war, and hostilities, CI personnel will carry weapons as authorized and required by unit mission.

Section II
Authority of CI Special Agents

8–10. Freedom of movement

If emergency circumstances preclude advance notification, CI special agents assigned to another theater are not required to obtain specific theater clearance from overseas commanders prior to undertaking overseas travel in connection with their official duties. (See AR 1–40, para 1–2*b*(5).) In such cases, the senior intelligence officer of the Army theater component command will be notified as soon as possible of the travel.

8–11. Oath administration

A CI special agent is authorized to administer oaths when taking statements. The agent's title for oath administration is "Counterintelligence Special Agent, U.S. Army." Authorities are the Uniform Code of Military Justice (UCMJ); Article 136(b) for military and 5 USC 303(b) for civilian special agents.

8–12. Apprehension authority

a. Pursuant to 10 USC 807–809, 28 USC 535, Rules for Court-martial (RCM) 302, AR 600–40, and this regulation, CI special agents are authorized to apprehend any person subject to the UCMJ, regardless of location, if there is a reasonable belief that the person has committed a criminal offense under USAI investigative jurisdiction. CI special agents are also authorized to conduct investigative stops of any person subject to the UCMJ, regardless of location, if there is a reasonable suspicion that the person has committed a criminal offense under USAI investigative jurisdiction.

b. CI special agents are authorized to detain civilian personnel on military installations or facilities when there is a reasonable belief that the person has committed a criminal offense against the U.S. Army, and that offense is within USAI investigative jurisdiction. CI special agents are also authorized to conduct investigative stops of civilians on military installations or facilities, if there is a reasonable suspicion that the person has committed a criminal offense under USAI investigative jurisdiction. Civilians will be detained only until they can be released to the FBI.

c. Army CI special agents may not apprehend or detain civilians outside the limits of a military installation or facility within the United States. When an apprehension is necessary in the conduct of a CI investigation, an arrest warrant must be obtained and executed by a civil law enforcement officer. CI special agents may accompany the arresting official for the purpose of identifying the person to be arrested and to provide assistance as authorized in AR 500–51.

d. Apprehension of civilians off a military installation or facility outside the United States may be authorized if host nation authorities consent and the proper arrest warrant is obtained.

e. Personnel apprehended by CI special agents will be released to civil or military police, as appropriate, for processing, detention, or confinement.

8–13. Search and seizure authority

a. Searches and seizures within the confines of a U.S. military installation or facility will be conducted in accordance with the Military Rules of Evidence, Manual for Courts-martial (MCM); AR 190–22; or other applicable policy.

b. Searches and seizures outside a military installation or facility in the United States will be conducted in accordance with Rule 41, Federal Rules of Criminal Procedure, 28 CFR 60, and AR 190–22. Coordination with the supporting staff judge advocate and concurrence of the appropriate U.S. Attorney are mandatory prior to seeking a civil search warrant. CI special agents may accompany the civil law enforcement official, who will actually execute the search warrant.

c. Searches and seizures outside a military installation or facility outside the U.S. are subject to SOFA.

8–14. Involvement in civil legal proceedings

Requests for the appearance of CI special agents at depositions or in civil proceedings and for the subpoena of information exempt from release to the public will be processed in accordance with AR 27–40.

8–15. Access to records, information, and facilities

a. Upon presentation of the MI badge and credentials or MI representative credentials, CI special agents and CI assistants will be permitted access to Army records under the provisions of AR 340–21, as required for the conduct of CI investigations or operations. They are also authorized to make extracts or transcripts of specific information obtained from the records custodian. The actual records will remain under the control of the records custodian, who will make either the records or legible certified copies available for judicial, non-judicial, or administrative proceedings.

b. Access to private sector financial records is authorized under 12 USC 3401–3419, 15 USC 1681f, and AR 190–6, provided that the required notifications or exceptions have been executed.

c. Access to records of other Federal agencies is provided for under 5 USC 552.

d. CI special agents and CI assistants will be granted access to all Army facilities when necessary for CI investigations or operations, consistent with the applicable security directive and the individual's access. Persons presenting Special Agent badge and credentials possess a final TOP SECRET security clearance based on a Single Scope Background Investigation.

8–16. CI special agents assigned to Special Mission Units

CI special agents who are authorized the MI badge and credentials, and who are assigned to SMU, may also be issued the SMU badge and credentials at the SMU commander's discretion, UP AR 525–17(S).

Chapter 9
The U.S. Army Intelligence Badge and Credential Program

9–1. General

a. This chapter establishes policy for the procurement, issue, use, control, and disposition of U.S. Army intelligence badges and credentials (B&C) and representative credentials. It applies to all active and RC MI units and to personnel authorized to use B&C or representative credentials.

b. B&C and representative credentials identify the bearer as a duly accredited special agent or representative of U.S. Army intelligence who is performing official intelligence duties.

9–2. Program functions

a. The CG, PERSCOM and CG, ARPERCEN—

(1) Notifies the CG, INSCOM of the issuance or withdrawal of the SSI/MOS/civilian CI specialties.

(2) Furnishes copies of SSI/MOS orders on above personnel.

b. The CG, INSCOM—

"Records or information concerning your transactions which are held by the financial institution named in the attached process or request were supplied to or requested by the Government authority named in the process or request on (date). Notification was withheld pursuant to a determination by the (title of the court so ordering) under the Right to Financial Privacy Act of 1978 that such notice might (state reason). The purpose of the investigation or official proceeding was (state purpose with reasonable detail)."

(3) Paragraph 2–7*c*, the law enforcement office obtaining financial records will serve personally or mail to the customer a copy of the request and the notice required by paragraph 2–7*c*.

(4) Paragraph 2–8*b*, the law enforcement office transferring financial records will serve personally or mail to the customer the notice required by paragraph 2–8*b*(2). If the law enforcement office was responsible for obtaining the court order authorizing the delay, such office shall also serve personally or by mail to the customer the notice required in paragraph 2–6*c*.

e. Annual reports. The annual reporting requirements of paragraph 2–13 apply to delays of notice sought or granted under this paragraph.

2–10. Foreign intelligence and foreign counterintelligence activities.

a. Except as indicated below, nothing in this regulation applies to requests for financial information in connection with authorized foreign intelligence and foreign counterintelligence activities as defined in Executive Order 12036. Appropriate foreign intelligence and counterintelligence directives should be consulted in these instances.

b. However, to comply with the Financial Privacy Act of 1978, the following guidance will be followed for such requests. When a request for financial records is made—

(1) A military intelligence group commander, the chief of an investigative control office, or the Commanding General (CG) (or Deputy CG), US Army Intelligence and Security Command will certify to the financial institution that the requesting activity has complied with the provisions of 12 U.S.C. 3403(b).

(2) The requesting official will notify the financial institution from which records are sought that 12 U.S.C. 3414(a)(3) prohibits disclosure to any person by the institution, its agents, or employees that financial records have been sought or obtained.

c. The annual reporting requirements shown in paragraph 2–13 apply to any request for access under this paragraph.

2–11. Certification. A certificate of compliance with the Right to Financial Privacy Act of 1978 (app C) will be provided to the financial institution as a prerequisite to obtaining access to financial records under the following access procedures:

a. Customer consent (para 2–2).

b. Search warrant (para 2–4).

c. Judicial subpoena (para 2–5).

d. Formal written request (para 2–6).

e. Emergency access (para 2–7).

f. Foreign intelligence and foreign counterintelligence activities (para 2–10).

2–12. Penalties. Obtaining or disclosing financial records or financial information on a customer from a financial institution in violation of the act or this regulation may subject the Army to payment of civil penalties, actual damages, punitive damages as the court may allow, and cost with reasonable attorney fees. Military and civilian personnel who willfully or intentionally violate the act or this regulation may be subject to disciplinary action.

2–13. Right to Financial Privacy Act of 1978 Annual Report (RCS DD–COMP(A) 1538).

a. Major Army commanders will submit this report to HQDA(DAPE–HRE) concerning requests for financial information from financial institutions. Reports are to include all queries requested or information obtained under the provisions of this regulation by subordinate Army law enforcement offices (as defined in para 1–3*f*). Negative reports will be submitted.

[redacted]

AFOSI Manual 71-119 (Approved draft, dtd 11 Feb 02)
National Security Letters Exerpt

3.4. (U) National Security Letters (NSL)

3.4.1. (U) NSLs are issued to obtain telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act), records from financial institutions (pursuant to the Right to Financial Privacy Act), and information from credit bureaus (pursuant to the Fair Credit Reporting Act), each as amended by the USA Patriot Act. The previous law permitted government access to such records upon a showing of relevance and that the consumer is an agent of a foreign power. The USA Patriot Act removes the "agent of a foreign power" requirement, providing government access to a multitude of private records upon the FBI's certification that "the information sought is relevant to an authorized foreign counterintelligence investigation."

3.4.1.1. (U) All three NSLs are available when the information sought "is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a US person is not conducted solely on the basis of activities protected by the First Amendment.

3.4.1.2. (U) An NSL is not limited to seeking information on the subject of an investigation. Because an NSL is available when the information sought is "relevant" to an investigation, information concerning apparent associates of, or individuals in contact with, the subject of an investigation may also be obtained if relevant to the investigation.

3.4.2. (U) NSLs are generally obtained through the FBI. NSL authority is delegated within the FBI to Assistant Directors, Deputy Assistant Directors at FBI HQ and to the LA, NY, and Washington Field Offices.

3.4.2.1. (U) NSLs issued pursuant to the Electronic Communications Privacy Act and the Fair Credit Reporting Act must be issued through the FBI.

3.4.2.2. (U) An NSL requesting information pursuant to the Right to Financial Privacy Act (attachment 3 and 4) may be issued by AFOSI/CC pursuant to his authority to conduct counterintelligence activities. However, an AFOSI NSL is merely a request. The financial institution can refuse to comply. A request from the FBI pursuant to any of these three Acts is compulsory.

3.4.3. (U) Additional Authorities:

3.4.3.1. (U) Section 156 of the USA Patriot Act grants the government the authority to "by administrative subpoena, require the production of any tangible things (including books, records, papers, documents, and other items) that are relevant" to an intelligence or terrorism investigation.

3.4.3.2. (U) Likewise, Section 158 amends the Federal Education Rights and Privacy Act (FERPA) to permit access to educational records in the investigation of domestic or international terrorism, or national security. The prior law prohibited the release of personally identifying information about students from education records without the consent of the student or parents, subject to limited exceptions.

3.5. (U) Sharing Information

3.5.1. (U) Cooperating with Law Enforcement. Consistent with the limitations contained in DoD Directive 5525.5, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:

3.5.1.1. (U) Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities,

3.5.1.2. (U) Protecting DoD employees, information, property, and facilities, or

3.5.1.3. (U) Preventing, detecting, or investigating other violations of law.

3.5.2. (U) DoD intelligence components may provide law enforcement authorities incidentally acquired information reasonably believed to indicate a violation of law in accordance with DoD 5240.1-R, Procedure 12.

3.5.3. (U) Law Enforcement Cooperation with Intelligence. The USA PATRIOT Act expands the scope of criminal investigative information that may be shared with the intelligence community. This authority is subject to a sunset provision described in Section 224 of the Act. This authority will expire on December 31, 2005 if Congress does not re-authorize the provision.

3.5.3.1. (U) Section 203 of the Act says that "notwithstanding any other law" it is lawful for criminal investigators to share foreign intelligence information obtained in the course of a criminal investigation with any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

3.5.3.2. (U) Federal Rule of Criminal Procedure 6(e) has been amended to permit the same sort of disclosure for grand jury information involving intelligence information.

3.5.3.3. (U) The Federal wiretap law (Title III) has been amended to allow the same sort of disclosure when the matters involve foreign intelligence.

3.5.3.4 (U) Sharing of Rule 6(e) information and wiretap information must be accomplished in accordance with Guidelines to be drafted by the Attorney General.

3.5.3.5 (U) See para 3.3.1.5 regarding the continuing application of intelligence oversight requirements.

3.6. (U) Coordination. Any AFOSI investigative activity conducted in conjunction with NSL's or a FISA must be coordinated through HQ AFOSI/XOQI and HQ AFOSI/SJA prior to the activity.

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
HEADQUARTERS, 902D MILITARY INTELLIGENCE GROUP
FORT GEORGE G. MEADE, MARYLAND 20755-5910

[redacted]

To Whom It May Concern,

Under the provisions of the Right to Financial Privacy Act of 1978 (hereinafter the ACT), Title 12, U.S.C. 3401 *et seq.*, the Department of the Army requests that your institution provide financial and credit information, to include any record information, concerning the individual identified below.

[redacted]
Account Number: [redacted]

This letter certifies that the Department of the Army has complied with the applicable provisions of the Act. Title 12, U.S.C. 3417 (c) specifies that good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records. The authorization to endorse this certificate has been delegated to me by the Secretary of the Army, contained in paragraph 2-10b(1), U.S. Army Regulation 190-6, Obtaining Information From Financial Institutions.

Title 12, U.S.C. 3414 (a) (3) prohibits your institution, employees, or agents of your institution from disclosing to any person that we have sought or obtained access to a customer's financial records.

In accordance with Title 12, U.S.C. 3415, we will reimburse your institution for such costs as are reasonably necessary and which have been directly incurred in searching for, reproducing, or transporting books, papers, records, or other data required or requested to be reproduced.

Thank you for your cooperation and assistance given to the Department of the Army, this command, and the Special Agent who presented this certificate.

Sincerely,

[redacted]
Colonel, U.S. Army
Commanding

[redacted]

Dear Custodian of Records:

Pursuant to Executive Order 12333 and the Right to Financial Privacy Act (Act), 12 United States Code §§3401, et seq., you are requested to provide the Naval Criminal Investigative Service with the name, address and financial records pertaining to the customer or accounts listed below:

Customer Name: if available

Address: if available

Date of birth: if available

Social Security: if available

Account numbers: if available

Requested period: if applicable (you may be required to pay for the records/search)

Pursuant to Section 3403(b) of the Act, I certify that NCIS has complied with the Special Procedures Provision contained in Section 3414. In accordance with Section 3417(c), your good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these records.

Please note that disclosing this request to the customer or others without a need to know in order to process this request may result in danger to the national security of the United States and interference with a counterterrorism or counterintelligence investigation. Accordingly, your company or its officers, employees, or agents are prohibited from disclosing to the customer that these records have been sought or obtained.

As a result of the sensitive nature of this request, please contact NCIS Special Agent _____ at (xxx) xxx-xxxx to make arrangements to provide the records. Thank you for your cooperation in this matter.

Sincerely,

Director, DD, AD for CI, AD for CT, or DAD for CI, or DAD for CT

Ser XX/U00XX
19Dec06

[redacted]

Dear [redacted]

I am a supervisory official designated by the General Counsel of the Department of the Navy to make the certification necessary under 15 U.S.C. § 1681v to compel disclosure of requested information and provide your agency with safe harbor.

In accordance with 15 U.S.C. § 1681v, I hereby certify that the information herein requested is necessary for an investigation of and/or analysis related to international terrorism.

Therefore, pursuant to Executive Order 12333 and Title 15 U.S.C. § 1681v of the Fair Credit Reporting Act you are directed to provide the Naval Criminal Investigative Service (NCIS) with a consumer report and all other information you possess in your files for the below listed consumers:

Consumer Name:

Date of Birth:

Social Security Number:

Address:

Please note that disclosing this request to the customer or others without a need to know in order to process this request may result in danger to the national security of the United States and interference with a counterterrorism or counterintelligence investigation. Accordingly, your company or its officers, employees, or agents are prohibited from disclosing to the customer that these records have been sought or obtained.

DEPARTMENT OF THE AIR FORCE
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

[redacted]
Air Force Office of Special Investigations
1535 Command Drive, Suite C301
Andrews AFB, MD 20762-7002

Dear [redacted]

The Air Force Office of Special Investigations (AFOSI) is a Federal agency authorized to conduct foreign counterintelligence activities by Executive Order 12333 and Department of Defense Directive 5240.2. Pursuant to Title 12, United States Code, Section 3414(a) you are requested to provide the following account information pertaining to the below-named person:

All personal account information including, but not limited to, account transactions, individuals authorized to use the accounts and their personal information, account deposits, withdrawals, credits and account reports. Transaction information should include the date, business, locations, and the amount of charges

[redacted]

Please forward the requested documents via US Postal Service to:

[redacted]
Air Force Office of Special Investigations
Unit 5695
APO, AE 09470-5695

Regardless of whether you provide this information, please be advised that Section 3414(a)(3) of Title 12 prohibits your institution or its officers, agents, or employees from disclosing to any person that these financial records have been sought or obtained.

A certification pursuant to Section 3403(b) indicating that AFOSI has complied with all requirements of the Right to Financial Privacy Act in making this request is attached. Under Section 3417(c) of Title 12, good faith reliance upon this certification relieves your institution and its employees or agents of any liability to your customer in connection with the disclosure of the requested financial records.

[redacted]

Attachment
Certification of Compliance

"Eyes of the Eagle."

DEPARTMENT OF THE AIR FORCE
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

Special Agent
Air Force Office of Special Investigations
Headquarters

Dear [redacted]

I certify, pursuant to Title 12, United States Code, Section 3403(b), that the Special Procedures Provisions of the Right to Financial Privacy Act (codified in Section 3414 of Title 12) have been followed with regard to this request for the financial records of [redacted]

Regardless of whether you provide this information, please be advised that Section 3414(a)(3) of Title 12 prohibits your institution or its officers, agents, or employees from disclosing to any person that these financial records have been sought or that may have obtained.

Under Section 3417(c) of Title 12, good faith reliance upon this certification relieves your institution and its employees or agents of any liability to your customer in connection with the disclosure of the requested financial records.

[redacted]

AFOSI Process for Use of National Security Letters

The AFOSI process for issuing an NSL is as follows:

1. The case agent submits a draft NSL to their respective detachment leadership for review. Reviewing officials have full access to the investigative case file and information in their investigative database (CI2MS).
2. The draft NSL is then processed through the respective Region for review. Reviewing officials at every level have full access to the investigative database (CI2MS).
3. The Region forwards the draft to the respective Integration Desk at HQ AFOSI. The Integration Desk reviews the request for investigative sufficiency.
4. The Integration Desk forwards the request to the HQ AFOSI Legal Unit for legal review [redacted]
5. The request is then forwarded through remaining command official as follows:
    a. Director of Counterintelligence
    b. Director of Operations
    c. AFOSI Commander for signature.
6. HQ AFOSI mails the NSL-Type Letter to the financial institution's headquarters. (Note: the case agent will contact the institution and notify the appropriate office that the letter is enroute)

The turn-around time from the initial request to the time HQ AFOSI mails the letter is usually within seventy-two hours.

[redacted]

[redacted]

[redacted]

Subject: Updated: CHANGE2: SASC NSL Briefing
Location: TBD

Start: Thu 1/25/2007 3:00 PM
End: Thu 1/25/2007 4:00 PM

Recurrence: (none)

Meeting Status: Accepted

24 Jan // [redacted]

Rally Point for those Attending:

Russell 228 at 1445
****
23 Jan // [redacted]
TIME: 1500-1600
PLACE: SR-228, Russell Senate Office Building
POC: Creighton Greene, 202-224-6115.

We're expecting 5-7 other staffers

ODUSD(CI&S) Attendees

[redacted]

NCIS Rep:

[redacted]

CIFA Rep:

[redacted]

Army Reps:

[redacted]

Air Force Reps:

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 18, 2007 7:19 AM
To: [redacted]
Cc:
Subject: FW: DRAFT Brief (U)

Importance: High

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 6:50 AM
To: [redacted]
Cc: [redacted]
Subject: FW: DRAFT Brief (U)

[redacted]

Cheers,
[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 6:19 AM
To: [redacted]
Cc:
Subject: RE: DRAFT Brief (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Cheer and thanks.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 17, 2007 7:43 PM
To: [redacted]
Cc: [redacted]
Subject: RE: DRAFT Brief (U)

[redacted]

[redacted]

Just my thoughts. Have a good night.

Cheers,

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, January 17, 2007 5:39 PM
To:
Cc: [redacted] CIV OSD OUSDI
Subject: DRAFT Brief (U)

Classification: UNCLASSIFIED

[redacted] per our discussion

[redacted] where I am just throwing stuff on a page.

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 8:59 AM
To: [redacted]
Cc: [redacted]
Subject: RE: NSLs and the SASC (U)
Importance: High
Attachments: 07-01-25 Program Management Review.pdf

07-01-25 Program Management Re...

Recipients on the "To" Line: in reference to the NSL issue, Acting DUSD(CI&S) has directed CIFA to undertake a program review of the utilization of NSLs by the Service CI components (see attached memo from Acting DUSD(CI&S) dated Jan 25, 2007. [redacted] of the CIFA Program Management Directorate will be leading this effort on behalf of CIFA. It is requested that you designate a POC for this review and that you ensure that any information provided in response to the taskers identified in the below e-mail from [redacted] are made available as well to [redacted] for the purpose of this review.

Your cooperation and timely response to this matter is greatly appreciated.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:46 AM
To: [redacted]

Subject: NSLs and the SASC (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Please contact [redacted] if you have any questions.

Regards,

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, January 23, 2007 11:06 AM
To: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

Summary of the HAC-D briefing on NSLs -- FYI. Note Service attendees for reference regarding the NSL review CIFA will be tasked with conducting. Recommend your contacts for the review as follows:

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 10:06 AM
To: [redacted]
Cc: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

FYI.

Hopefully, there won't be too many more.

I really appreciate your help on this.

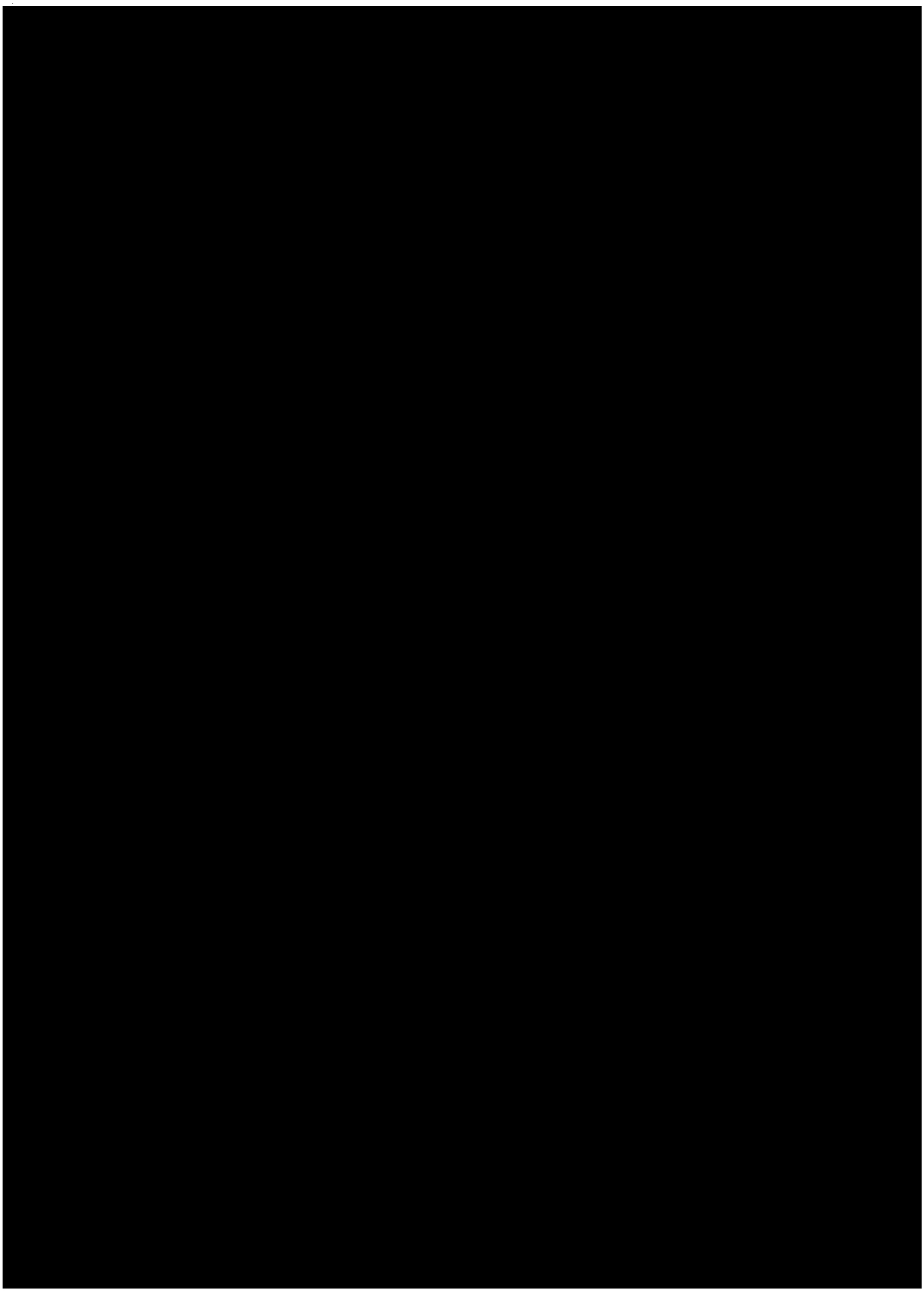
[redacted]

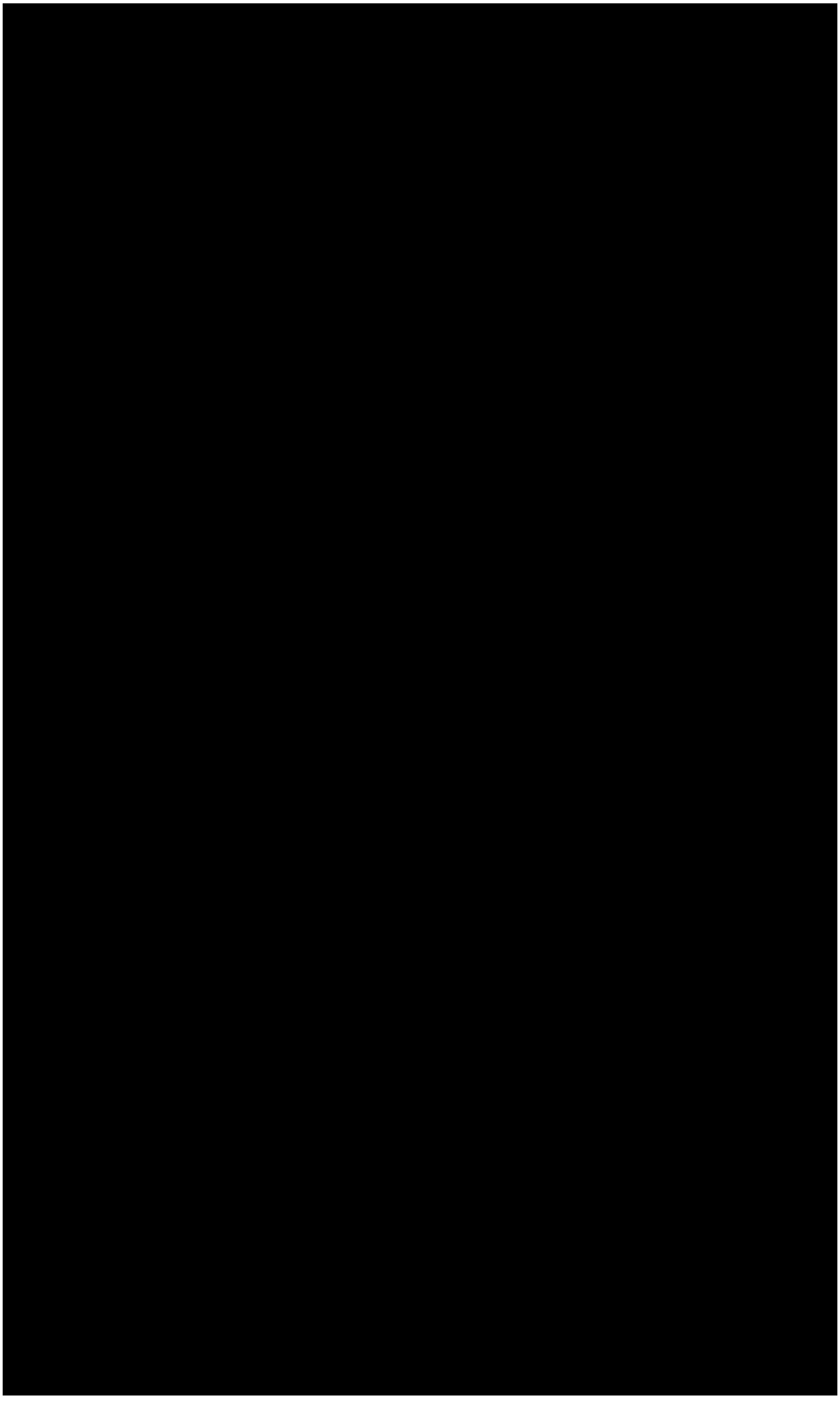
[redacted]

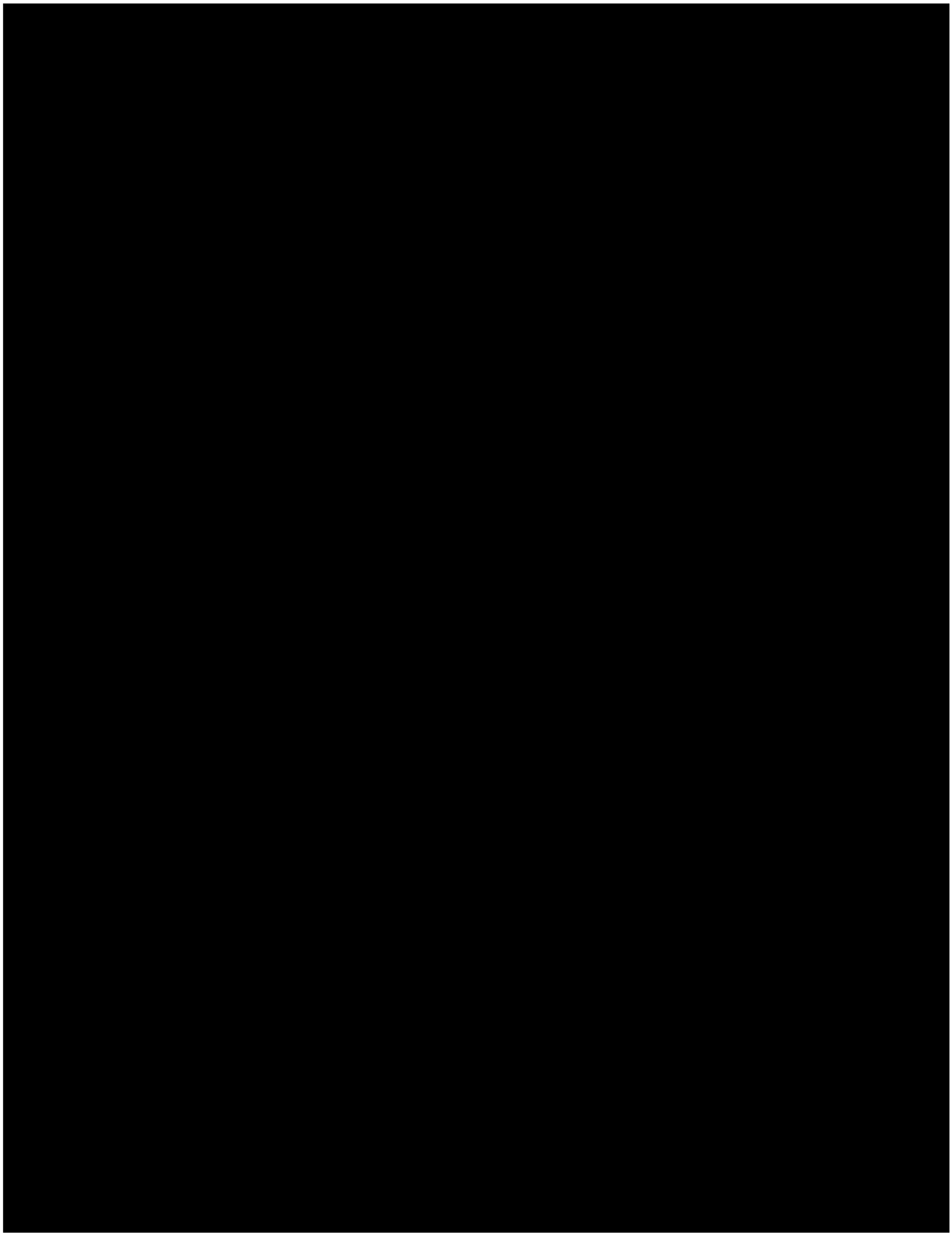
-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 9:45 AM
[redacted]
Subject: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

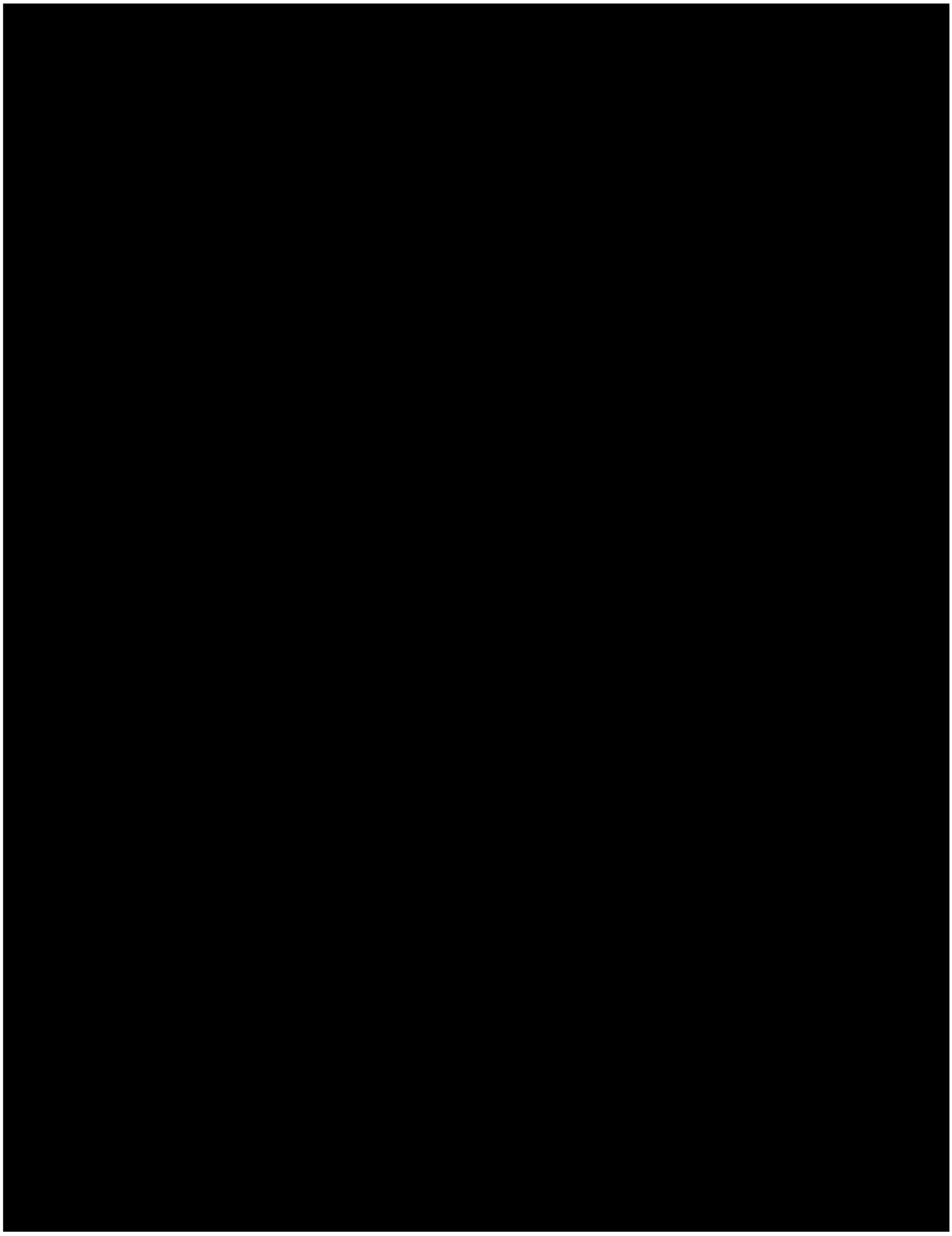
FOR OFFICIAL USE ONLY

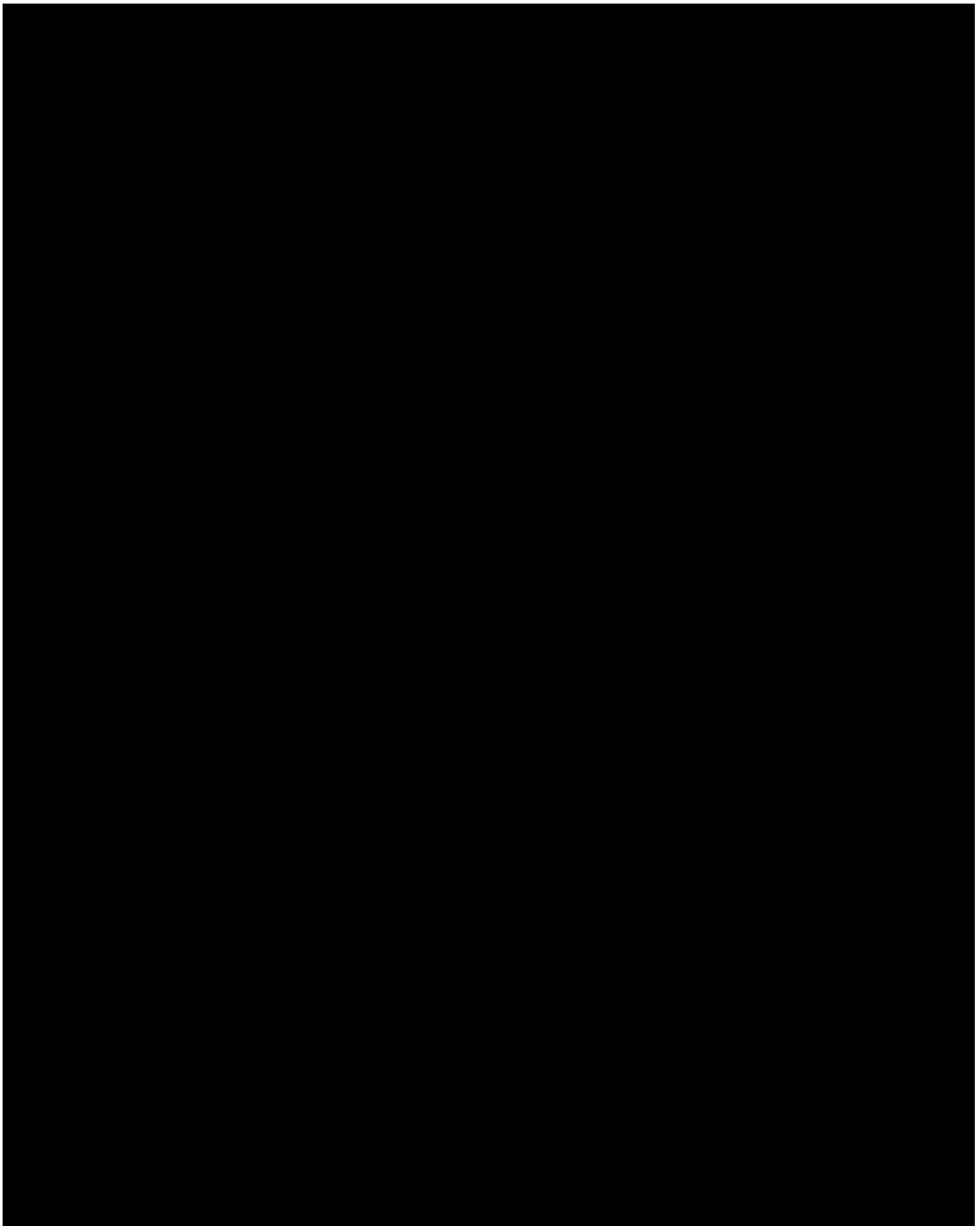
[redacted]

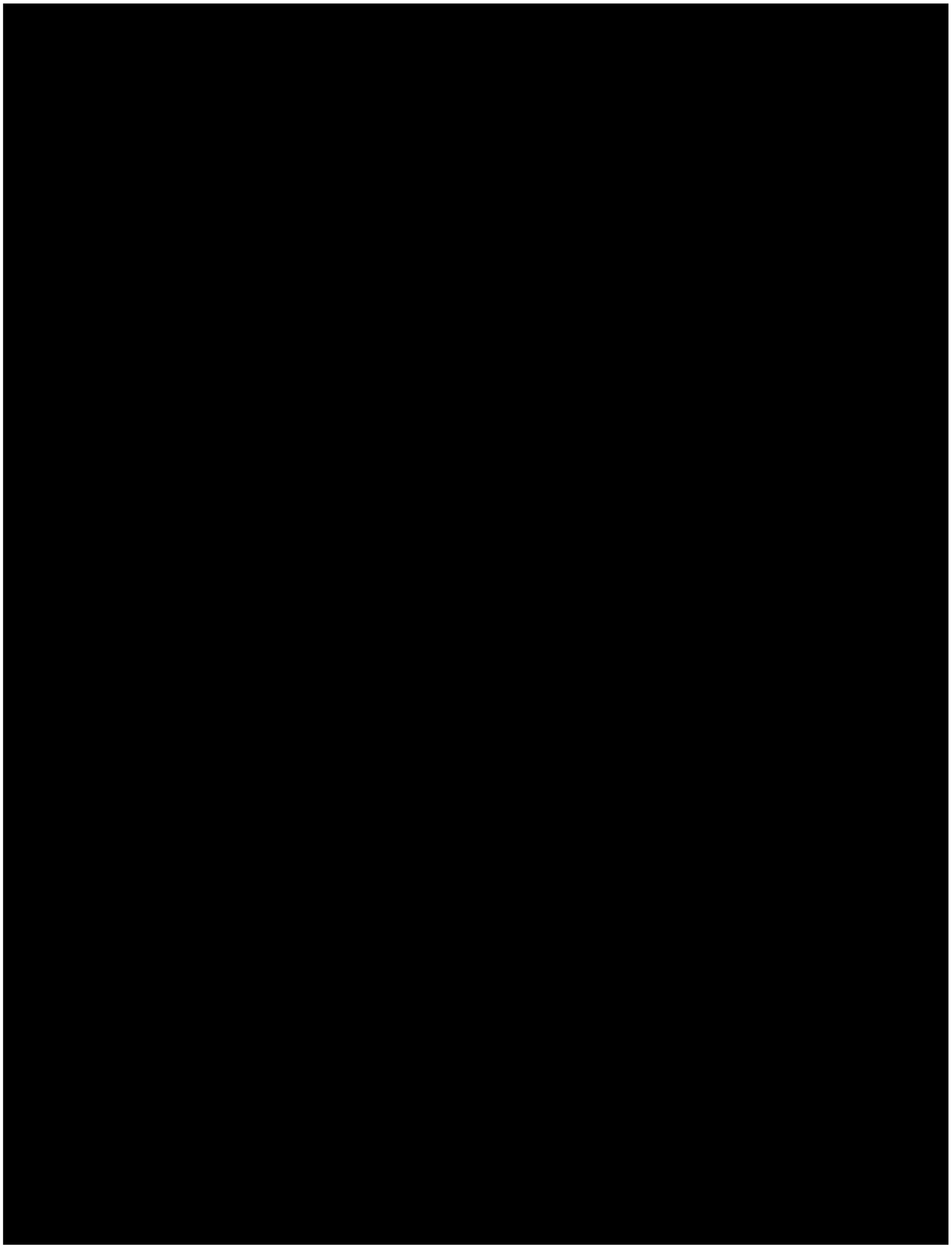


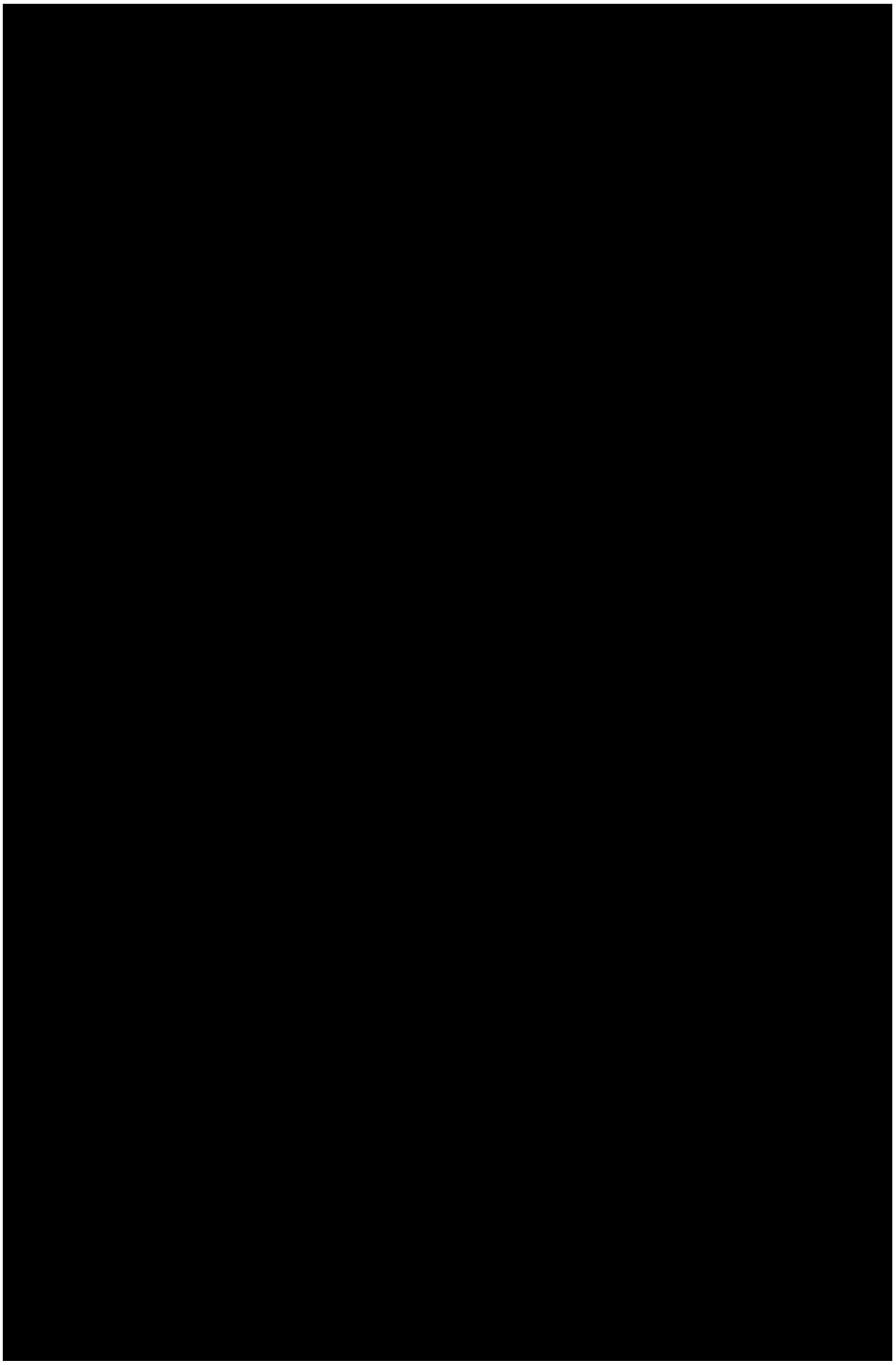




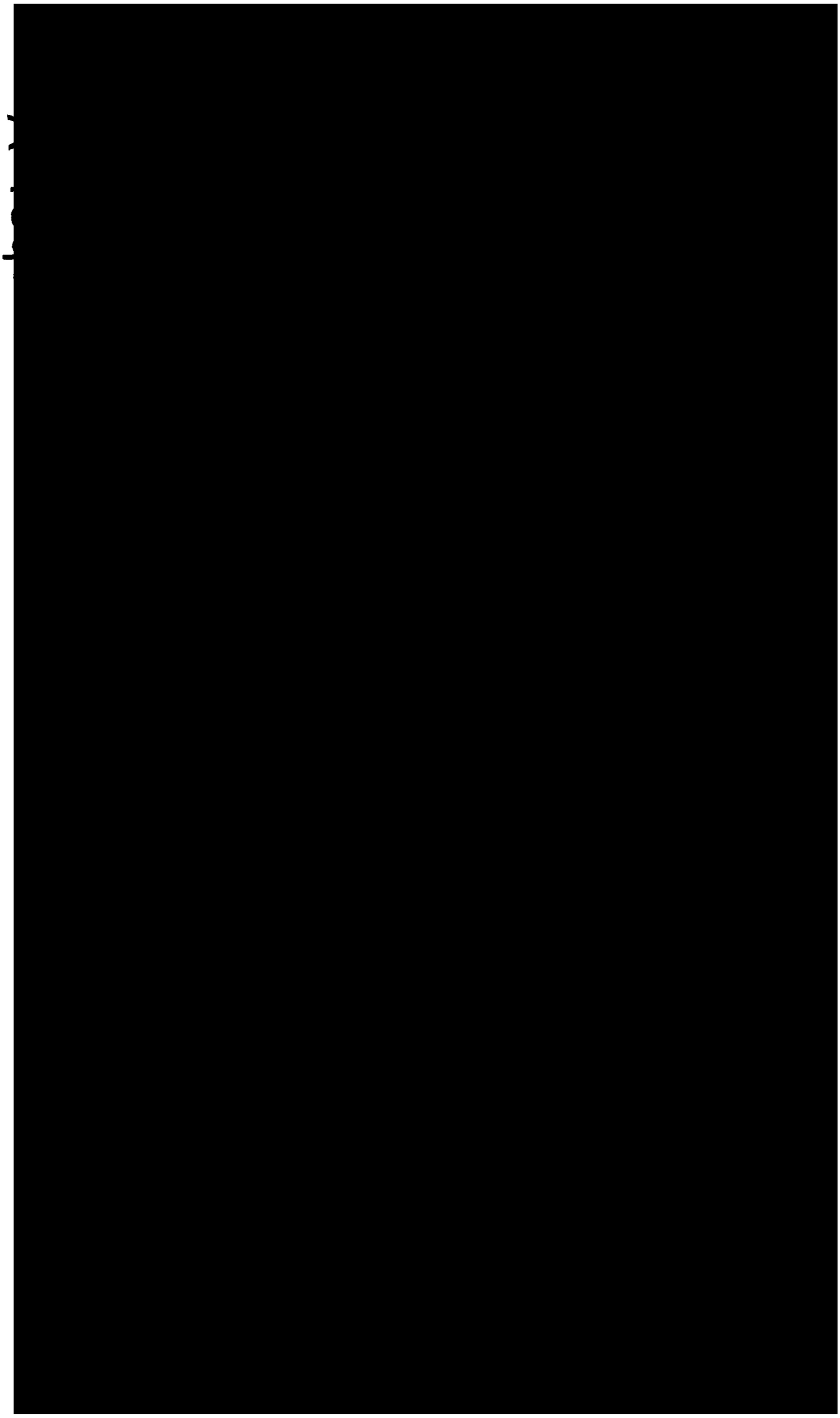








[redacted]



[redacted]

ness and

[redacted]

From: [redacted]
Sent: Wednesday, March 14, 2007 2:08 PM
To: [redacted]
Cc:
Subject: RE: HPSCI News Release: House Intelligence Committee to Hold Hearings on National Security Letters (U)

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 1:07 PM
To: [redacted]
Subject: RE: HPSCI News Release: House Intelligence Committee to Hold Hearings on National Security Letters (U)

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 12:55 PM
To: [redacted]
Subject: FW: HPSCI News Release: House Intelligence Committee to Hold Hearings on National Security Letters (U)

FYI...

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 11:24 AM
To: [redacted]
Cc: [redacted]
Subject: FW: HPSCI News Release: House Intelligence Committee to Hold Hearings on National Security Letters (U)

UNCLASSIFIED

Did not see you folks on the original send out.

PRESS RELEASE

FOR IMMEDIATE RELEASE: March 9, 2007
http://intelligence.house.gov/Media/PDFS/ReyesRelease030907.pdf

House Intelligence Committee to Hold Hearings on National Security Letters

Washington, D.C. - The U.S. Department of Justice Inspector General released a report today on the Federal Bureau of Investigation's (FBI) use of National Security Letters. Congressman Silvestre Reyes, D-TX, Chairman of the House Permanent Select Committee on Intelligence, released the following statement in response to today's report:

"This morning, Department of Justice Inspector General Glenn Fine briefed me on the Congressionally-mandated reviews of the use of National Security Letters (NSLs) to obtain telephone, Internet, credit and financial records, and Section 215 Orders for Business Records.

"In my opinion, these reports present a highly troubling picture of mismanagement, lack of effective controls, and shoddy recordkeeping of NSLs within the FBI. As a result, a large number of NSL requests were issued for sensitive records in violation of the law, policies and guidelines. In addition, the overall number of NSLs has been grossly underreported to Congress. Most troubling, the IG found that in more than 700 cases, the FBI issued 'exigent letters' promising that a grand jury subpoena or an NSL would follow - but they never did. And the IG found, in many cases, that there was no emergency or that the situation was not exigent. I expect more of the FBI and its leaders, especially since during the last Congress when we had the FBI in for hearings on this subject, we expressed our concern regarding the potential abuse of NSLs and emphasized that strict procedures be followed. Apparently, our concerns were well-founded.

"I, and many other Members of Congress, have previously expressed concern with orders issued under Section 215 of the USA Patriot Act.
These orders permit investigators to demand information and records - like who borrowed a library book or who used a library Internet terminal. If not carefully handled, such information in the hands of the government has the potential to infringe upon American citizens' privacy rights. The Inspector General's (IG) findings concern me gravely.

"These mistakes, while perhaps not intentional, must be rectified. I intend to hold briefings and hearings to understand the scope of these problems and to ensure corrective action has been taken.

"I also spoke to Attorney General Alberto Gonzales and FBI Director Robert Mueller about these reports. Both pledged to me that they would accept the IG's recommendations and fix the problems that plague the system.

"The American people expect their government, and particularly their law enforcement agencies, to follow the law and protect their privacy and liberties. Congress must now do its job and conduct vigorous oversight of this situation."

[redacted]

From: [redacted]
Sent: Wednesday, March 14, 2007 3:18 PM
To: [redacted]
Subject: RE: SASC NSL Report ~~(FOUO)~~

[redacted]

Nice catch! I made the changes...

Thanks,

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 3:15 PM
To: [redacted]
Subject: FW: SASC NSL Report ~~(FOUO)~~

Sirs,
FYI

[redacted]

-----Original Message-----
From: [redacted] CIV OSD OUSDI [mailto: [redacted]
Sent: Monday, March 12, 2007 3:23 PM
To: [redacted]
Cc: [redacted]
Subject: SASC NSL Report ~~(FOUO)~~

FOR OFFICIAL USE ONLY

FYI, this is what we submitted to the SASC.

<<SASC Financial Requests 1990-2007 070305.doc>>

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, March 14, 2007 1:39 PM
To: DP Office Chiefs; DP Division Chiefs
Subject: FW: HPSCI Hearing Invitation

Attachments: invite.pdf

invite.pdf (184 KB)

FYI

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 12:07 PM
[redacted]
Subject: HPSCI Hearing Invitation

Good afternoon --- attached is the official invitation from the HPSCI for the March 22 CI hearing. It provides information on possible topics and witnesses/attendees.

V/R

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, March 14, 2007 1:38 PM
To: [redacted]
Subject: FW: HPSCI News Release: House Intelligence Committee to Hold Hearings on National Security Letters

fyi.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 11:51 AM
To: EXCOM; [redacted]
Cc: [redacted]
Subject: HPSCI News Release: House Intelligence Committee to Hold Hearings on National Security Letters

Good Morning,

FYI.

[redacted]

PRESS RELEASE

FOR IMMEDIATE RELEASE: March 9, 2007
http://intelligence.house.gov/Media/PDFS/ReyesRelease030907.pdf

House Intelligence Committee to Hold Hearings on National Security Letters

Washington, D.C. - The U.S. Department of Justice Inspector General released a report today on the Federal Bureau of Investigation's (FBI) use of National Security Letters. Congressman Silvestre Reyes, D-TX, Chairman of the House Permanent Select Committee on Intelligence, released the following statement in response to today's report:

"This morning, Department of Justice Inspector General Glenn Fine briefed me on the Congressionally-mandated reviews of the use of National Security Letters (NSLs) to obtain telephone, Internet, credit and financial records, and Section 215 Orders for Business Records.

"In my opinion, these reports present a highly troubling picture of mismanagement, lack of effective controls, and shoddy recordkeeping of NSLs within the FBI. As a result, a large number of NSL requests were issued for sensitive records in violation of the law, policies and guidelines. In addition, the overall number of NSLs has been grossly underreported to Congress. Most troubling, the IG found that in more than 700 cases, the FBI issued 'exigent letters' promising that a grand jury subpoena or an NSL would follow - but they never did. And the IG found, in many cases, that there was no emergency or that the situation was not exigent. I expect more of the FBI and its leaders, especially since during the last Congress when we had the FBI in for hearings on this subject, we expressed our concern regarding the potential abuse of NSLs and emphasized that strict procedures be followed. Apparently, our concerns were well-founded.

"I, and many other Members of Congress, have previously expressed concern with orders

issued under Section 215 of the USA Patriot Act.
These orders permit investigators to demand information and records - like who borrowed a library book or who used a library Internet terminal. If not carefully handled, such information in the hands of the government has the potential to infringe upon American citizens' privacy rights. The Inspector General's (IG) findings concern me gravely.

"These mistakes, while perhaps not intentional, must be rectified. I intend to hold briefings and hearings to understand the scope of these problems and to ensure corrective action has been taken.

"I also spoke to Attorney General Alberto Gonzales and FBI Director Robert Mueller about these reports. Both pledged to me that they would accept the IG's recommendations and fix the problems that plague the system.

"The American people expect their government, and particularly their law enforcement agencies, to follow the law and protect their privacy and liberties. Congress must now do its job and conduct vigorous oversight of this situation."

[redacted]

From: [redacted]
Sent: Wednesday, March 14, 2007 1:37 PM
To: [redacted]
Cc:
Subject: FW: NSL Point Paper for Brenner

Importance: High

Attachments: DoD NSL Point Paper for Dr. Brenner.doc

DoD NSL Point Paper for Dr. Br...

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 9:50 AM
To: [redacted]
Subject: NSL Point Paper for Brenner
Importance: High

[redacted]

Please let me know if you concur with GC recommended changes. Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 8:47 AM
To: [redacted]
Cc: [redacted]
Subject: FW: NSL Point Paper for Brenner
Importance: High

Ref your Siprnet e-mail this morning, this is a re-send of yesterday's e-mail forwarding the NSL point paper for Brenner.

[redacted]

---Original Message-----
From: [redacted]
Sent: Tuesday, March 13, 2007 9:21 AM
To: [redacted]
Cc:
Subject: NSL Point Paper for Brenner

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, March 14, 2007 7:29 AM
To: [redacted]
Subject: FW: HOT! Newsweek Query on National Security Letters (U)

fyi.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 7:24 AM
To: [redacted]
Subject: RE: HOT! Newsweek Query on National Security Letters (U)

[redacted]

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 14, 2007 7:06 AM
To: [redacted]
Subject: FW: HOT! Newsweek Query on National Security Letters (U)

[redacted]

Please work quickly and get the answer to me.. [redacted] can give you the answer...Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, March 13, 2007 5:57 PM
[redacted]

[redacted]

Subject: RE: HOT! Newsweek Query on National Security Letters (U)

UNCLASSIFIED

[redacted]

Regards,

-----Original Message-----
From: [redacted]
Sent: Tuesday, March 13, 2007 5:01 PM
To: [redacted]
Cc: [redacted]
Subject: HOT! Newsweek Query on National Security Letters
Importance: High

[redacted]

V/R
[redacted]

[redacted]

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

From: Hosenball, Mark [mailto:mhosen@newsweek.com]
Sent: Tuesday, March 13, 2007 4:25 PM
To: [redacted]
Subject: newsweek inquiry

Following our telephone conversation of a couple of minutes ago, I would like answers to the following questions:

Q1. What Defense Department agencies use National Security Letters to gather information ? Please identify by name all specific DoD law enforcement or intelligence agencies that do so.

A1: The following DoD components are authorized to makes requests for information under the NSL statutes in support of counterintelligence and counterterrorism investigations:

- U.S. Army Criminal Investigation Command
- U.S. Army Counterintelligence
- Naval Criminal Investigative Service
- U.S. Air Force Office of Special Investigations

Q2. Under what legal or administrative authority do DoD agencies use National Security Letters to gather information ? Please specify the specific authority used by each agency to issue such requests for information.

A2: DoD makes requests for information under authorities of the "National Security Letter statutes" - Right to Financial Privacy Act; the Fair Credit Reporting Act, and the National Security Act - but does not use the specific term National Security Letter in its investigatory practice.

Q3. Do National Security Letters issued by DoD agencies carry administrative or statutory compulsions which effectively require the recipient of the letter to turn over the requested information ? Or are recipients of such letters only requested voluntarily to turn over the information ? If this practice varies from agency to agency please specify who does what.

A3: DoD sends written requests for information to institutions and entities under the NSL statutes as permitted by the laws mentioned above. Because these are requests for information rather than court orders, a DoD request under the NSL statutes cannot be compelled absent
court involvement.

Q4. What kind of information is gathered by DoD agencies using National Security Letters (compulsory or voluntarily) ? Please specify which agencies gather what kinds of information for what purposes (for example, counter-intelligence, force protection, counter-terrorism, personnel security, etc).

A4: The ability to request certain business transaction information is invaluable to DoD in conducting counterintelligence and counterterrorism investigations. These statutory tools may provide key leads for counterintelligence and counterterrorism investigations. The requests are used in authorized national security investigations for limited types of information, such as customer and consumer transaction information, from specified entities, such as U.S. financial institutions, U.S. telecommunications companies, and credit agencies.

Q5. How many National Security Letters have been issued over the last year/five years by each specific agency which uses this procedure to gather information ?

A5:

Q6. Have any of the individual agencies which use National Security Letters to gather information conducted, or been subjected to, any audits or inspections either by internal DoD watchdog agencies (such as DoD IG) or any other governmental watchdog (such as Congress, Justice Department, ODNI or GAO) regarding their use of National SEcurity letters to gather information ? If so, please furnish details of the audit or inspection and please characterize the results or conclusions of such inquiries or audits.

A6:

Q7. It has been reported to me that the agency CIFA is now facing possible renewal of the DoD Directive that constitutes its official charter. Please furnish me with details of the charter renewal process, whether CIFA is seeking to expand its authorities and/or activities, and whether other agencies are seeking to take away or claim back elements of CIFA's current operational authorizations or authority.

A7:

I may have further questions as my research on this issue progresses.
Please reply to me by return e-mail or you can phone me at 202-626-2036.

Many thanks for your attention to this inquiry.

Yours faithfully,

Mark Hosenball
Correspondent
Newsweek Washington Bureau

[redacted]

From: [redacted]
Sent: Monday, March 12, 2007 3:23 PM
To: [redacted]
Cc:
Subject: SASC NSL Report (~~FOUO~~)

Attachments: SASC Financial Requests 1990-2007 070305.doc

SASC Financial Requests 1990-2...

FOR OFFICIAL USE ONLY

FYI, this is what we submitted to the SASC.

<<SASC Financial Requests 1990-2007 070305.doc>>

[redacted]

[redacted]

From: [redacted]
Sent: Friday, March 09, 2007 12:23 PM
To: [redacted]
Cc:
Subject: FW: FBI-centric NSL Article (U)

Importance: High

FYI at this time -- but stand by!!!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 11:41 AM
To: [redacted]
Cc:
Subject: RE: FBI-centric NSL Article (U)

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 11:39 AM
To: [redacted]
Cc: [redacted]
Subject: RE: FBI-centric NSL Article (U)

Sir,

[redacted]

Cheers,
[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 11:13 AM
To: [redacted]
Cc:
Subject: RE: FBI-centric NSL Article (U)

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 11:11 AM
To: [redacted]
Cc: [redacted]
Subject: RE: FBI-centric NSL Article (U)

Sirs,

[redacted]

V/R

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 10:55 AM
To: [redacted]
Cc: [redacted]
Subject: FW: FBI-centric NSL Article (U)

Sir,

[redacted]

Cheers,
[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 10:28 AM
To: [redacted]

Subject: FW: FBI-centric NSL Article (U)

UNCLASSIFIED

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 10:10 AM
To: [redacted]
Cc: [redacted]
Subject: FW: FBI-centric NSL Article (U)

UNCLASSIFIED

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 09, 2007 8:37 AM
[redacted]
Subject: FBI-centric NSL Article

This article is on the front page (above the fold) of today's Washington Post. DNI is mentioned in third paragraph from the bottom. Other than that, this article is completely FBI-related, but I thought you might be interested because it might stir the pot.

V/R,
[redacted]

Frequent Errors In FBI's Secret Records Requests Audit Finds Possible Rule Violations By John Solomon and Barton Gellman Washington Post Staff Writers Friday, March 9, 2007; A01 A Justice Department investigation has found pervasive errors in the FBI's use of its power to secretly demand telephone, e-mail and financial records in national security cases, officials with access to the report said yesterday.
The inspector general's audit found 22 possible breaches of internal FBI and Justice Department regulations -- some of which were potential violations of law -- in a sampling of 293 "national security letters."
The letters were used by the FBI to obtain the personal records of U.S. residents or visitors between 2003 and 2005. The FBI identified 26 potential violations in other cases.
Officials said they could not be sure of the scope of the violations but suggested they could be more widespread, though not deliberate. In nearly a quarter of the case files Inspector General Glenn A. Fine reviewed, he found previously unreported potential violations.
The use of national security letters has grown exponentially since the Sept. 11, 2001, attacks. In 2005 alone, the audit found, the FBI issued more than 19,000 such letters, amounting to 47,000 separate requests for information.
The letters enable an FBI field office to compel the release of private information without the authority of a grand jury or judge. The USA Patriot Act, enacted after the 2001 attacks, eliminated the requirement that the FBI show "specific and articulable"

reasons to believe that the records it demands belong to a foreign intelligence agent or terrorist.
That law, and Bush administration guidelines for its use, transformed national security letters by permitting clandestine scrutiny of U.S.
residents and visitors who are not alleged to be terrorists or spies.
Now the bureau needs only to certify that the records are "sought for"
or "relevant to" an investigation "to protect against international terrorism or clandestine intelligence activities."
According to three officials with access to the report, Fine said the possible violations he discovered did not "manifest deliberate attempts to circumvent statutory limitations or departmental policies."
But Fine found that FBI agents used national security letters without citing an authorized investigation, claimed "exigent" circumstances that did not exist in demanding information and did not have adequate documentation to justify the issuance of letters.
In at least two cases, the officials said, Fine found that the FBI obtained full credit reports using a national security letter that could lawfully be employed to obtain only summary information. In an unknown number of other cases, third parties such as telephone companies, banks and Internet providers responded to national security letters with detailed personal information about customers that the letters do not permit to be released. The FBI "sequestered" that information, a law enforcement official said last night, but did not destroy it.
Alan Raul, vice chairman of the White House Privacy and Civil Liberties Oversight Board and a former Reagan White House lawyer , said in an interview that the Bush administration has asked the board to review and recommend changes in the FBI's use of national security letters.
"The processes seem to be seriously in need of tune-up," Raul said. "We hope to play a role in helping the FBI get to where it knows it needs to be."
Lanny Davis, another board member and a former attorney in the Clinton White House , said his recent briefing by the FBI left him "very concerned about what I regard to be serious potential infringements of privacy and civil liberties by the FBI and their use of national security letters. It is my impression that they too regard this as very serious."
Fine's audit, which was limited to 77 case files in four FBI field offices, found that those offices did not even generate accurate counts of the national security letters they issued, omitting about one in five letters from the reports they sent to headquarters in Washington. Those inaccurate numbers, in turn, were used as the basis for required reports to Congress.
Officials said they believe that the 48 known problems may be the tip of the iceberg in an internal oversight system that one of them described as "shoddy."
The report identified several instances in which the FBI used a tool known as "exigent letters" to obtain information urgently, promising that the requests would be covered later by grand jury subpoenas or national security letters. In several of those cases, the subpoenas were never sent, the review found.
The review also found several instances in which agents claimed there were exigent circumstances when none existed. The FBI recently ended the practice of using exigent letters in national security cases, officials said last night.
The report, mandated by Congress over the Bush administration's objections, is to be presented to several House and Senate committees today. But senior officials, speaking with permission on the condition that they not be identified, said the Bush administration has already responded vigorously to the audit's findings.
Attorney General Alberto R. Gonzales learned of the findings three weeks ago and "was incensed when he was told the contents of the report,"
according to a Justice Department official.
"The attorney general commends the work of the inspector general in uncovering serious problems in the FBI's use of NSLs," said Tasia Scolinos, a spokeswoman for Gonzales. "He has told [FBI Director Robert S. Mueller III] that these past mistakes will not be tolerated, and has ordered the FBI and the department to restore accountability and to put in place safeguards to ensure greater oversight and controls over the use of national security letters."
FBI and Justice Department officials have long described national security letters as an indispensable tool in combating terrorism, and Fine's report, according to one official who cited excerpts, said investigators told the inspector general that the letters "contributed significantly to many counterterrorism and counterintelligence investigations." Fine did not make an independent assessment of the efficacy of the letters as investigative tools.
FBI procedures require that any possible violation of law or regulation on national security letters be reported to the President's Intelligence Oversight Board within 14 days of discovery. Of the 26 breaches it discovered before Fine's review, the FBI referred

19 to the oversight board.
Among the responses officials highlighted last night is a tracking database under development by the FBI to ensure that its accounting of national security letters is accurate. One official said the FBI would begin deployment of the system in four of its 56 field offices by the end of the year. Meanwhile, the official said, each office will be required to "hand count" the numbers every month.
Gonzales, officials said, has ordered the department's national security division and inspections division to begin audits next month of a sampling of national security letters in every field office. About 15 offices should be audited by the end of the year, the official said.
Gonzales has also ordered that he chief counsel of every field office personally sign off on every national security letter, a practice that has been encouraged but not required until now.
The office of Director of National Intelligence Mike McConnell has established a working group to consider how much of the information gathered by national security letters should be retained and whether any of it should be purged. After the Patriot Act was passed, the Bush administration eliminated the FBI's requirement that irrelevant personal information from case files be discarded after cases are closed.
Mueller has ordered improved training of agents involved in national security cases and better record-keeping. Last May, changes began with the fixing of databases.
A senior group of FBI inspectors has been asked to review the conduct of agents and their supervisors to determine if any should be disciplined for mistakes.

[redacted]

From: [redacted]
Sent: Friday, March 02, 2007 4:30 PM
To: [redacted]
Cc: [redacted]

Subject: RE: NSL Program Review Package (U)

I guess sometimes its worth a good rant!!

Have a great weekend.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 02, 2007 3:55 PM
To: [redacted]
Subject: RE: NSL Program Review Package (U)

No further action required...thanks [redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 02, 2007 2:08 PM
To: [redacted]
Subject: RE: NSL Program Review Package (U)

[redacted]

Grab a beer and relax...I'll take it from here...I'll let you know what happens...thanks for the info!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 02, 2007 2:04 PM
To: [redacted]
Cc: [redacted]
Subject: RE: NSL Program Review Package (U)

I really have to contain myself on this one!!

[redacted]

[redacted]

Now that I got that out.....!!!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 02, 2007 1:11 PM
To: [redacted]
Cc: [redacted]
Subject: NSL Program Review Package (U)
Importance: High

[redacted]

[redacted]

[redacted]

UNCLASSIFIED

[redacted]

Just got your subject package, looks great and early!

[redacted]

This leads to my second question

It's an ACTION MEMO. What ACTION are you requesting?

V/r
[redacted]

[redacted]

From: [redacted]
Sent: Friday, February 23, 2007 4:14 PM
To: [redacted]
Cc:
Subject: RE: Draft CIFA NSL Report

Attachments: Footnote 1.doc

Footnote 1.doc (26 KB)

[redacted]

My proposed footnote 1 is attached. Please feel free to edit as you see appropriate.

Thanks,

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 22, 2007 10:32 AM
To: [redacted]
Cc: [redacted]
Subject: RE: Draft CIFA NSL Report

We have a meeting with [redacted] tomorrow (Friday) at 1600 to discuss the status. You are welcome to join us if you are available. Technically, the report is due to [redacted] March 1.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 22, 2007 9:41 AM
To: [redacted]
Cc: [redacted]
Subject: RE: Draft CIFA NSL Report

How close are we to going smooth? What is our due date?

Thanks,

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 22, 2007 8:17 AM
To: [redacted]
Cc:
Subject: Draft CIFA NSL Report

[redacted] attached is the current draft of out NSL Report. Would appreciate your thoughts, particularly in view of our converstation this morning.

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, February 22, 2007 11:12 AM
To: [redacted]
Cc:
Subject: RE: Draft CIFA NSL Report

Thanks....[redacted] wants to discuss with me this afternoon....more to follow.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 22, 2007 10:32 AM
To:
Cc: [redacted]
Subject: RE: Draft CIFA NSL Report

We have a meeting with [redacted] tomorrow (Friday) at 1600 to discuss the status. You are welcome to join us if you are available. Technically, the report is due to [redacted] March 1.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 22, 2007 9:41 AM
To:
Cc: [redacted]
Subject: RE: Draft CIFA NSL Report

How close are we to going smooth? What is our due date?

Thanks,

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 22, 2007 8:17 AM

To: [redacted]
Cc:
Subject: Draft CIFA NSL Report

[redacted] attached is the current draft of out NSL Report. Would appreciate your thoughts, particularly in view of our converstation this morning.

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, February 21, 2007 2:09 PM
To: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Attachments: 07-01-25 Program Management Review.pdf

07-01-25 Program Management Re...

Here's the NSL tasker from OSD

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 10:47 AM
[redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Revised:

Lead: DP
Assist: DC, DS, DT

Due to DQ: 1 Mar 07

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Wednesday, February 21, 2007 2:02 PM
To: [redacted]
Subject: NSL Report to SSCI and HAC-D (U)

Attachments: SSCI-HACD Follow-on Q&A 070215.doc

SSCI-HACD
low-on Q&A 07021!

UNCLASSIFIED

[redacted]

V/R,

[redacted]

<<SSCI-HACD Follow-on Q&A 070215.doc>>

~~SECRET~~

Department of Defense Response
to the Senate Select Committee on Intelligence and
the House Appropriations Committee – Defense
Following January 2007 Briefings on
National Security Letters (NSLs)

Q1: What is the percentage, by Service, of the total investigations that use NSLs?[1]

- **Army CI (FY 2000-Present):**
  - Total No. of Investigations: [redacted]
  - Total No. Using NSLs:
  - Percentage:
- **AF Office of Special Investigations (OSI) (FY 2000-Present):**
  - Total No. of Investigations: [redacted]
  - Total No. Using NSLs:
  - Percentage:
- **NCIS: Pending**

Q2: What is the breakout of statutes used for each NSL or request made pursuant to the RFPA (see note 1)?

- **Army CI: [See Footnotes 1 & 2]**
  - Total: [redacted]

---

[1] Congress has defined the term "National Security Letter" in section 119(g) of the PATRIOT Improvement and Reauthorization Act of 2006, and specifically did not include in the NSL definition requests made by authorized government agencies, such as the Department of Defense (DoD), under the Right to Financial Privacy Act (RFPA), 12 USC § 3414 (a)(1)-(4). As such, DoD requests made pursuant to the RFPA are not included in the above Service totals.

[2] For completeness, of the total number of investigations, Army CI records indicate that [redacted] investigations used a request made pursuant to the RFPA.

[3] For completeness, of the total number of investigations, Army CI investigations that used a request made pursuant to the RFPA was [redacted] of total number of investigations.

[4] For completeness, of the total number of investigations, AFOSI records indicate that [redacted] investigations used a request made pursuant to the RFPA.

[5] For completeness, of the total number of investigations, AFOSI investigations that used a request made pursuant to the RFPA was [redacted] of total number of investigations.

THIS PAGE IS UNCLASSIFIED WHEN SEPARATED FROM TAB D

Prepared by: [redacted] CI Directorate, OUSD(I)/CI&S, [redacted]

~~SECRET~~

- 12 USC § 3414: [redacted]

❖ **AF OSI [See Footnotes 4 & 5]:**

- Total: [redacted]
- 12 USC § 3414:
- 50 USC § 436:

❖ **NCIS: Pending**

Q3: What is the number of NSLs that DoD has asked FBI to issue in conjunction with a DoD investigation?

❖ DoD does not ask FBI to issue NSLs in conjunction with a DoD investigation. For DoD investigations, the military service organizations authorized to conduct counterintelligence investigations determine whether, in a particular investigation, use of NSLs is appropriate. If so, the request for information is made by the DOD organization.

❖ As the representatives from the Army CI and AFOSI stated during the January 2007 briefings, some investigations are conducted jointly with the FBI. During these joint investigations, it is not uncommon for the investigators to divide investigative tasks between agencies. However, this division of workload is not considered by the Department or the Military Services to be a DoD "request" for FBI to issue NSLs. Moreover, the Military Services do not maintain records of the number of FBI-issued NSLs in joint investigations.

Q4: What are the relevant DoD Directives governing use of NSLs?

❖ DoD Directive 5200.12, "Obtaining Information from Financial Institutions," December 2, 2004 (TAB A-1)

❖ DoD Instruction 5200.15, "Guidance on Obtaining Information from Financial Institutions", December 2, 2004 (TAB A-2)

Q5: Please provide a copy of each Service's procedures for issuing NSL-type requests.

❖ Army CI Investigation Handbook – Financial Checks Excerpt (TAB B-1)

❖ AF OSI Manual 71-119 (Approved draft, dtd 11Feb 02) (TAB B-2)

❖ NCIS – PENDING (TAB B-3)

THIS PAGE IS UNCLASSIFIED WHEN SEPARATED FROM TAB D

Prepared by: [redacted] CI Directorate, OUSD(I)/CI&S, [redacted]

Q6: Please provide examples of an NSL from each Service.

- ❖ Department of the Army Example (TAB C-1)
- ❖ Department of the Navy Examples (TAB C-2)
- ❖ Department of the Air Force Examples (TAB C-3)

Q7: Please provide a copy of the 1979 MOA with the FBI and the 1996 amendment.

- ❖ April 5, 1979 Memorandum of Understanding: Coordination of Counterintelligence Matters Between FBI & DoD (TAB D-1) – **Marked CONFIDENTIAL**
- ❖ 1996 Supplement to 1979 FBI/DoD Memorandum of Understanding: Coordination of Counterintelligence Matters Between FBI & DoD (TAB D-2) – **Marked SECRET**

THIS PAGE IS UNCLASSIFIED WHEN SEPARATED FROM TAB D

Prepared by: [redacted] CI Directorate, OUSD(I)/CI&S, [redacted]

[redacted]

From: [redacted]
Sent: Tuesday, February 20, 2007 3:47 PM
To: [redacted]
Cc:
Subject: RE: NSL - Army Write-up

Attachments: 4.jpg; imstp_usa1.gif

4.jpg (15 KB) imstp_usa1.gif (18 KB)

[redacted] Got it. I have updated the entries.

Thanks a bunch

[redacted]

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

From: [redacted]
Date: 2/20/2007 3:04:15 PM
To: [redacted]
Cc:
Subject: RE: NSL - Army Write-up

[redacted] Needs some adjustment with office terminology.

[redacted]

Hope this helps.
v/r
[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 15, 2007 12:17 PM
To: [redacted]
Cc:
Subject: NSL - Army Write-up

[redacted]
Please review the attached for accuracy and let me know what needs to be changed.
Thanks for your help

[redacted]

<<Army MI Write-up.doc>>

FREE Emoticons for your email - by IncrediMail! Click Here!
<http://www.incredimail.com/index.asp?id=99000>

[redacted]

From: [redacted]
Sent: Tuesday, February 20, 2007 9:38 AM
To: [redacted]
Subject: RE: NSL Help

[redacted]

-----Original Message-----
From: [redacted]

Sent: Monday, February 19, 2007 10:35 PM
To: [redacted]
Subject: FW: NSL Help

From: [redacted]
Sent: Monday, February 19, 2007 10:35:02 PM
To: [redacted]
Cc: [redacted]
Subject: Fw: NSL Help
Auto forwarded by a Rule

Sent from my BlackBerry Wireless Handheld

[redacted]

-----Original Message-----
From: [redacted]
To: [redacted]
CC: [redacted]
Sent: Mon Feb 19 22:27:33 2007
Subject: NSL Help

[redacted]

I have attac <<DoD Guidance.doc>> hed two documents that are extracts from th <<DEFINITIONS AND STATUTES.doc>> e report I am preparing. If you would, please give them a look and provide feedback on the questions I have listed.

Thanks in advance

[redacted]

PS: I am playing [redacted] this week, that is why the email is coming form my comcast address. I will also send it via blackberry from my work address.

<http://www.incredimail.com/index.asp?id=99000>

<<imstp_usa1.gif>>

[redacted]

From: [redacted]
Sent: Tuesday, February 20, 2007 7:39 AM
To: [redacted]
Cc:
Subject: FW: HASC NSL Briefing

Importance: High

Note [redacted] request to set up a meeting Friday to discuss the status of the NSL review. Hopefully you can have a solid draft to present to him at that time?

I'll have [redacted] schedule a time on Friday.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, February 19, 2007 10:07 AM
To: [redacted]
Cc:
Subject: RE: HASC NSL Briefing

[redacted]

Sounds like it went a lot better. Could you please sked a quick update next Fri (23 Feb) re progress on our DUDSI tasker re the NSLs.

Cheers,

[redacted]

From: [redacted]
Sent: Thursday, February 15, 2007 3:45 PM
[redacted]
Subject: HASC NSL Briefing

Just returned from the HASC NSL briefing. No real issues -- very different than the SASC reception we received a couple of weeks ago! The staffers were very cordial; they allowed [redacted] to give his overview; and they then asked some very basic questions for clarification. No due outs for CIFA other than they would like to see the results of the NSL review we are conducting. The staffers did emphasize that they would like to see some overarching DoD policy on the use of NSLs.

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Monday, February 19, 2007 10:52 PM
To: [redacted]
Cc:
Subject: NSL Help

Attachments: 4.jpg; DEFINITIONS AND STATUTES.doc; DoD Guidance.doc; imstp_usa1.gif

4.jpg (15 KB) DEFINITIONS AND STATUTES.doc (... DoD Guidance.doc (33 KB) imstp_usa1.gif (18 KB)

I was wondering if you could give me a hand on the legal side since you seem to have this issue down pat?

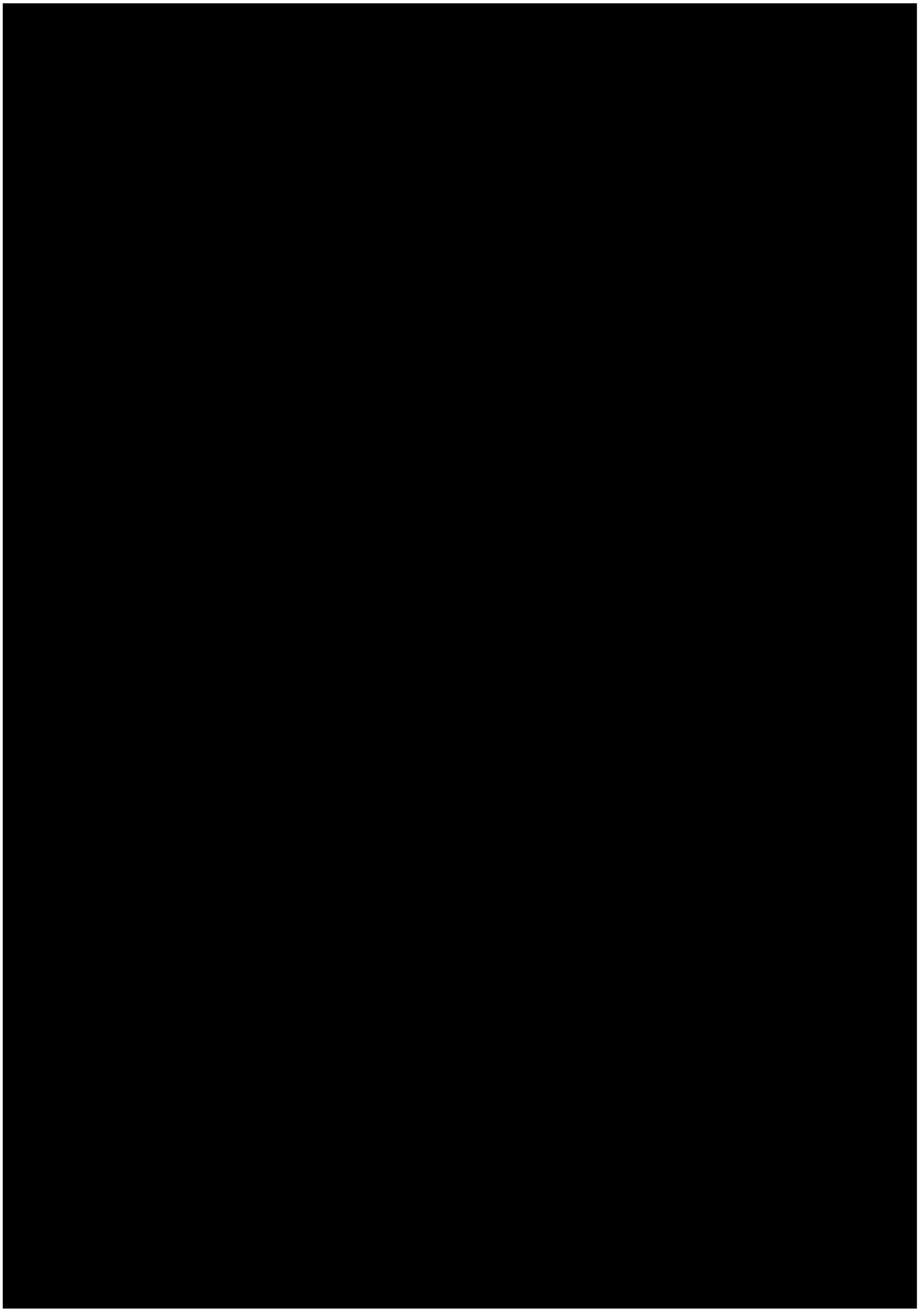
I have attached two documents that are extracts from the report I am preparing. If you would, please give them a look and provide feedback on the questions I have listed.

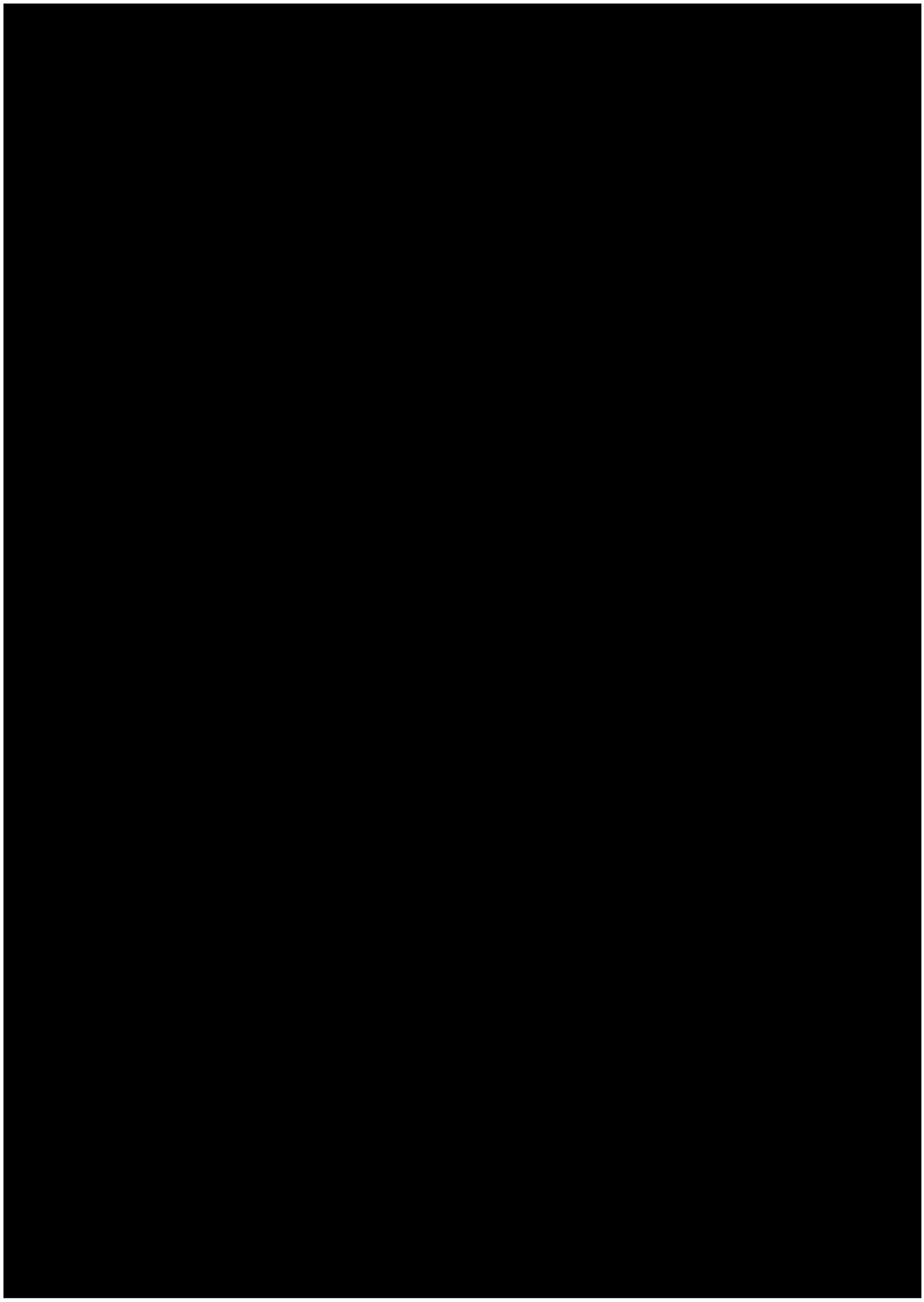
Thanks in advance

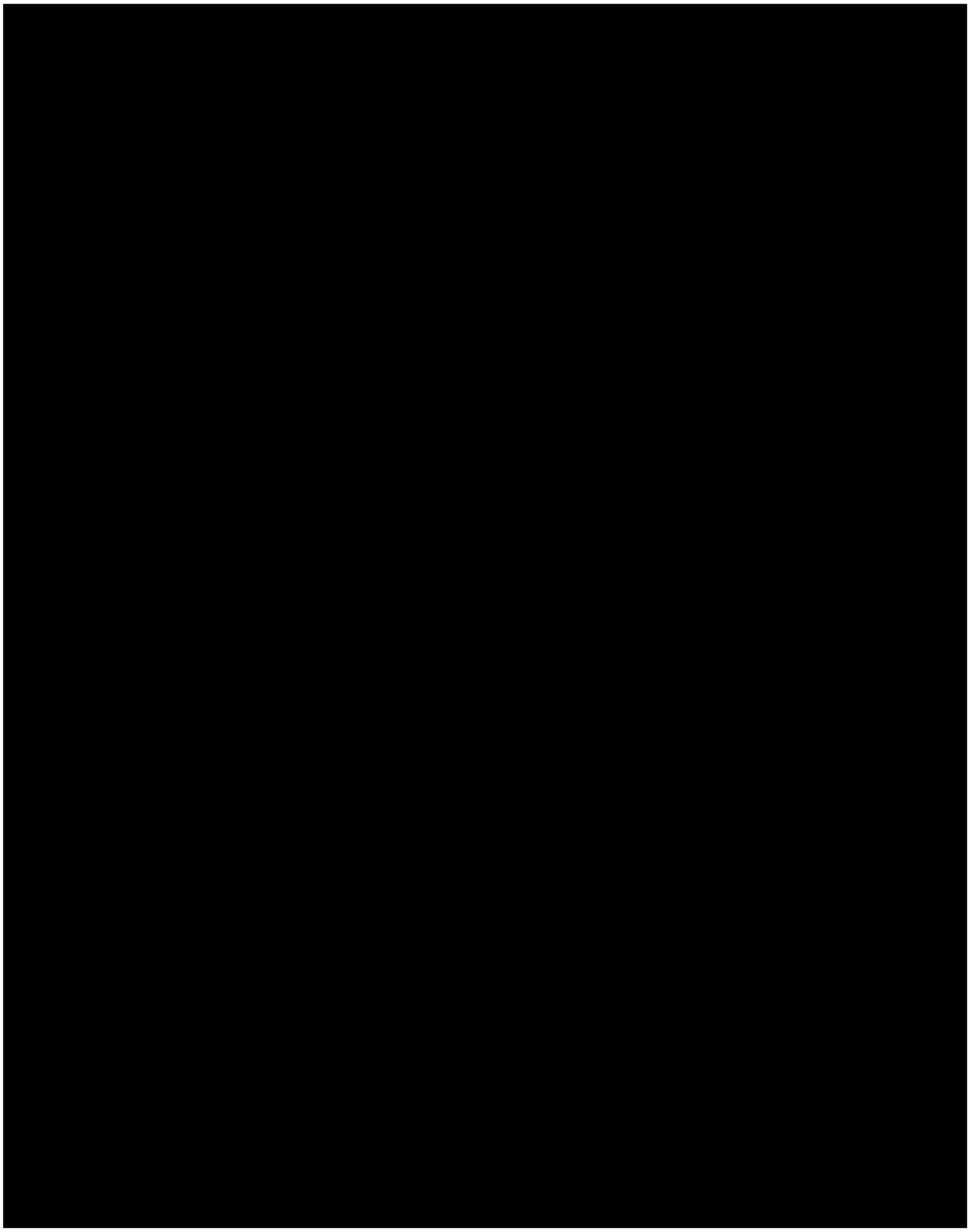
[redacted]

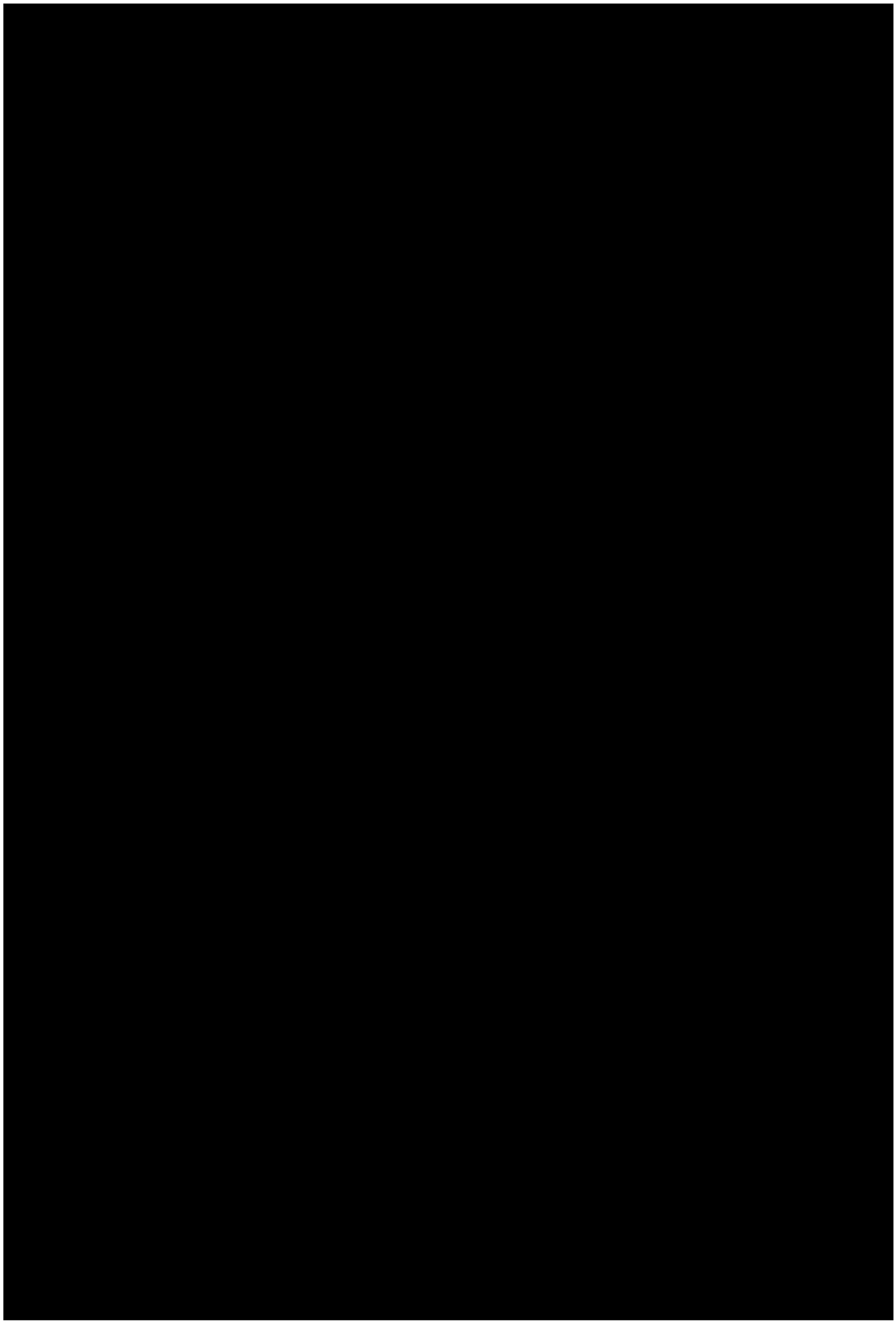
PS: I am playing [redacted] this week, that is why the email is coming form my comcast address. I will also send it via blackberry from my work address.

FREE Emoticons for your email - by IncrediMail! Click Here!
<http://www.incredimail.com/index.asp?id=99000>









[redacted]

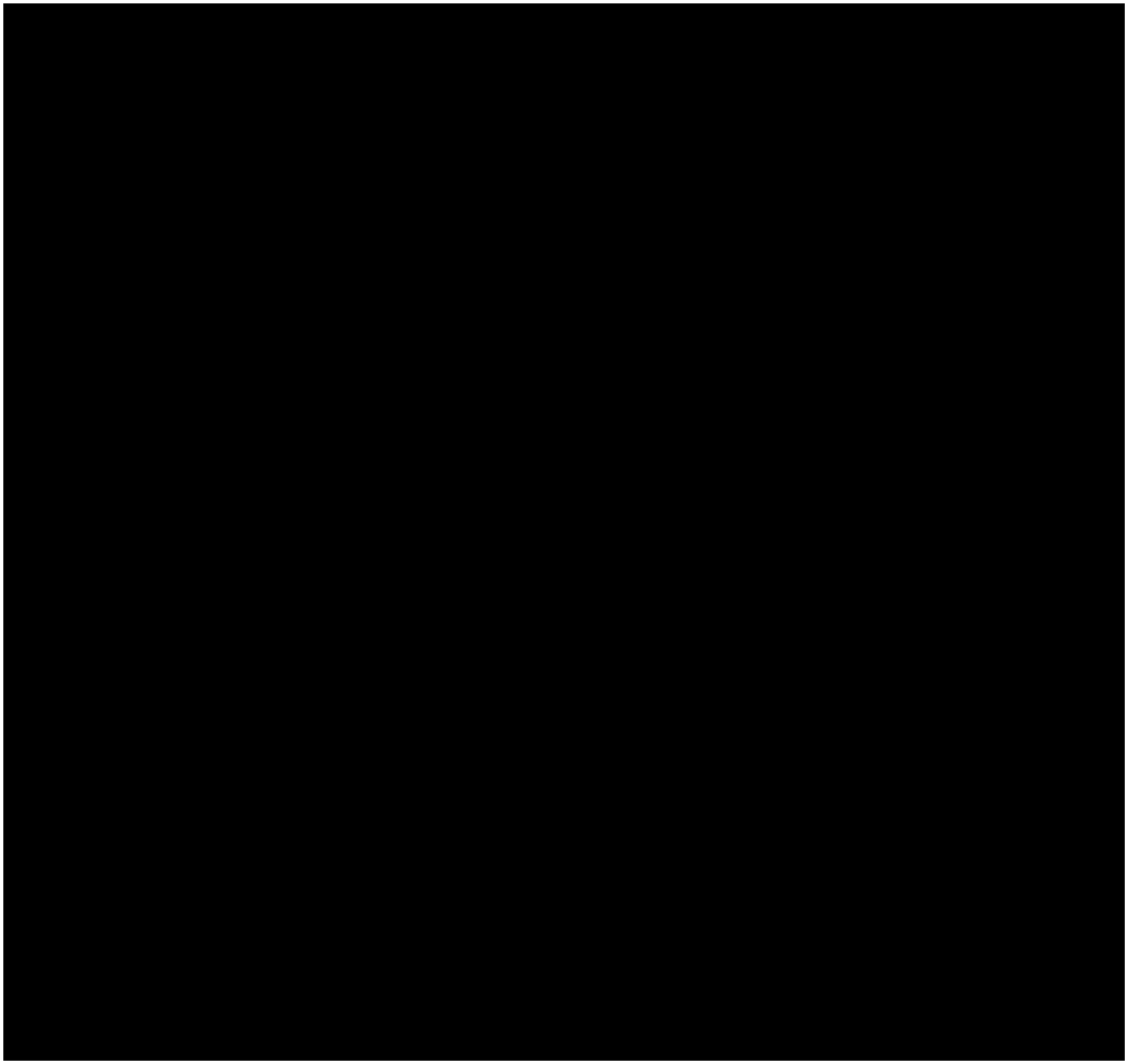
From: [redacted]
Sent: Thursday, February 15, 2007 5:01 PM
To: [redacted]
Cc:
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HASC Minority Staff, 15 FEB 07

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 15, 2007 4:52 PM
[redacted]
Subject: QUICKLOOK: Meeting on National Security Letters (NSLs) with HASC Minority Staff, 15 FEB 07

[redacted]



[redacted]

From: [redacted]
Sent: Thursday, February 15, 2007 3:46 PM
To: [redacted]
Cc:
Subject: RE: HASC NSL Briefing

Thanks. Appreciate you carrying this rock in your rucksack for us.

-----Original Message-----
From: [redacted]
Sent: Thursday, February 15, 2007 3:45 PM
[redacted]
Subject: HASC NSL Briefing

Just returned from the HASC NSL briefing. No real issues -- very different than the SASC reception we received a couple of weeks ago! The staffers were very cordial; they allowed [redacted] to give his overview; and they then asked some very basic questions for clarification. No due outs for CIFA other than they would like to see the results of the NSL review we are conducting. The staffers did emphasize that they would like to see some overarching DoD policy on the use of NSLs.

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, February 15, 2007 3:42 PM
To: [redacted]
Subject: RE: AFOSI NSL Write-up

Attachments: AFOSI Write-up - XOQ Final Draft 15 Feb 07.doc

AFOSI Write-up - XOQ Final Dra... [redacted]

Attached are our changes to your insert. Additionally, I did not breakdown the number of CI/CT cases from 2000 - present; however, gave an overall number to OSD.

v/r [redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, February 13, 2007 11:14 AM
To: [redacted]
Subject: AFOSI NSL Write-up

[redacted]

Please take a look at the following insert and let me know if I need to correct anything.

Thanks <<AFOSI Write-up.doc>>

[redacted]

SERVICE POLICY AND PROCEDURES

AFOSI

Philosophy: Most stateside AFOSI CI and CT investigations are conducted jointly with the FBI. An AFOSI NSL is merely a request for information where the financial institution can refuse to comply. A request from the FBI pursuant to any of the three statutes is compulsory. Therefore, if a request can be processed through the FBI, AFOSI will do so. To, date, AFOSI cannot cite any CI or CT investigations where the FBI has refused to issue an NSL on a joint investigation. Another benefit to processing the letter through the FBI is the available analytic support provided by the FBI that leads to a finished product being delivered back to the investigative agent.

[redacted]

Process: The AFOSI process for issuing an NSL is as follows:

1. The case agent submits a draft NSL to their respective detachment leadership for review. Reviewing supervisory officials have full access to the investigative case file and information in their investigative database (CI2MS).
2. The draft NSL is processed through the respective Regional Headquarters for review. Reviewing officials at every level have full access to the investigative database (CI2MS).
3. The Regional Headquarters forwards the draft to the respective Counterintelligence (CI) Investigations Desk Officer on the Integration Desk at HQ AFOSI. The CI Investigations Desk Officer ~~Integration Desk~~ reviews the request for investigative sufficiency.
4. The CI Investigations Desk Officer ~~Integration Desk~~ forwards the request to the HQ AFOSI Legal Unit for legal review [redacted] If the request is not legally sufficient it is not recommended fro approval and sent back to the case agent with an explanation.
5. After the request is found legally sufficient, the request is forwarded through remaining command officials as follows:
    a. Director of Counterintelligence
    b. Director of Operations
    c. AFOSI Commander or Vice Commander for signature.
6. HQ AFOSI mails the NSL to the financial institution's headquarters. (Note: the case agent will contact the institution and notify the appropriate office that the letter is enroute)

Process Time: The turn-around time from the initial request to the time HQ AFOSI mails the letter is usually within seventy-two hours.

Approval Authorities: The Commanding General or Vice Commander.

[redacted]

From: [redacted]
Sent: Thursday, February 15, 2007 2:06 PM
To: [redacted]
Cc:
Subject: RE: Navy NSL Write-up

Attachments: Navy Write-up mds comments.doc

Navy Write-up mds comments.doc... [redacted]

Please see my changes. Advise if you have questions.

R/
[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, February 15, 2007 11:50
To: [redacted]
Cc:
Subject: Navy NSL Write-up

[redacted]

Please review the attached document and make corrections where you feel they are needed. Please shoot these back to me when you get a chance.

Thanks <<Navy Write-up.doc>>

[redacted]

SERVICE POLICY AND PROCEDURES CONTINUED

Naval Criminal Investigative Service (NCIS)

Philosophy: NCIS exercises its authority to issue NSLs under all three statutes that pertain to DoD. They view NSLs as an invaluable investigative tool which they use not only to verify existing information, but to serve as a lead generation tool. According to DoD statistics, NCIS issues more letters than the other DoD agencies. They effectively and efficiently employ NSL's through detailed program management, investigative oversight, and training. The attorneys in the National Security Law Unit are responsible for providing the legal review of the letters. One of the attorneys is embedded within the Counterintelligence Directorate, enabling her to be involved in all steps of the investigative process and remain intimately familiar of the status of an investigation as it progresses. NCIS plans to increase the utilization of this investigative and lead generation process through program direction, timely investigative review, and increased awareness training.

Deleted: the use

Deleted: legal review unit

Deleted: ir

Deleted: investigative oversight and management directorate

Deleted: which enables them

Deleted: as

Instruction/Regulations: General Administrative Order OOJ-0002, [redacted]

Comment [m1]: We have a draft GEN that should be out within the next week or two updating the policy outlined in OOJ-0002. The basic policy is the same, but the earlier document was issued in Feb 03, and as you know, several changes have occured since then.

Deleted: 00-JTAC-002

Process: The NCIS process for issuing an NSL under each of the applicable statutes is as follows:

1. The case agent submits a draft NSL along with the supporting documentation to the appropriate NCIS desk officer (CI or CT). In many cases, these investigations have already been identified as Special Interest or Director Special Interest cases. Because of this status the HQ NCIS desk officers and the legal unit are intimately familiar with the case.

Deleted: most

2. If the desk officer finds the documentation meets all requirements, it is forwarded to an attorney in the NCIS National Security Law Unit (NSLU) for a legal review.

3. The NSLU attorney reviews the documentation to ensure all criteria of the relevant statute are met and that the draft NSL contains all required information.

4. If the NSLU legal review supports the request for an NSL, the documentation is forwarded to senior officials at NCIS headquarters for final review and signature. The total number of headquarters officials authorized to sign an NSL within NCIS varies depending upon which statute is invoked.

5. Assuming an authorized senior NCIS official signs the NSL, the case agent or desk officer must contact the intended recipient of the NSL before it can be transmitted (usually electronically), to assure the recipient is appropriately sensitized to both investigative and privacy considerations.

Process Time: The turn-around time from the initial request to the time HQ NCIS transmits the letter is usually within twenty-four hours.

Approval Authorities: The NCIS Director, NCIS Deputy Directors, and Executive Assistant Directors for CI and CT have approval authority for all three statutes that pertain to DoD. The Deputy Assistant Directors for CI and CT may sign letters pursuant to 12 U.S.C. § 3414 and 15 USC § 1681v.

[redacted]

[redacted]

From: [redacted]
Sent: Friday, February 09, 2007 1:01 PM
To: [redacted]
Subject: NSL Chart

Attachments: CI%20Investigative%20Tools%20Chart[1].pdf

CI%20Investigative%20Tools%20C...

You probably already have this, but here you go anyway...

V/R,

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Friday, February 09, 2007 11:03 AM
To: [redacted]
Subject: NSL Stuff Part III of III (U)

Attachments: 07-01-19 NSL Talking Points.doc; 07-01-19 OUSD(I) NSL Briefing.ppt; NSL Congressional Q&A to Congress 070125.doc

07-01-19 NSL Talking Points.do...

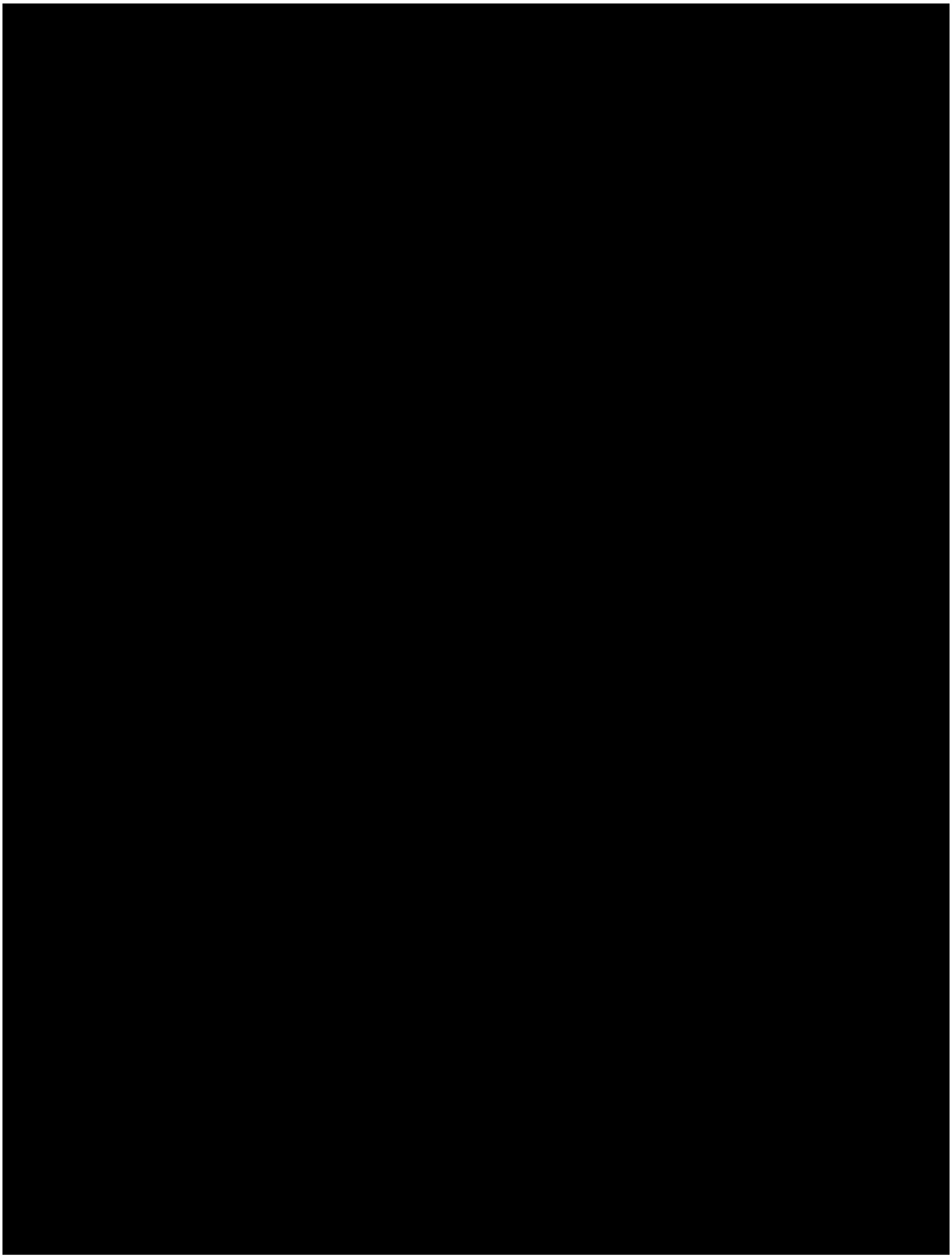
07-01-19 OUSD(I) NSL Briefing....

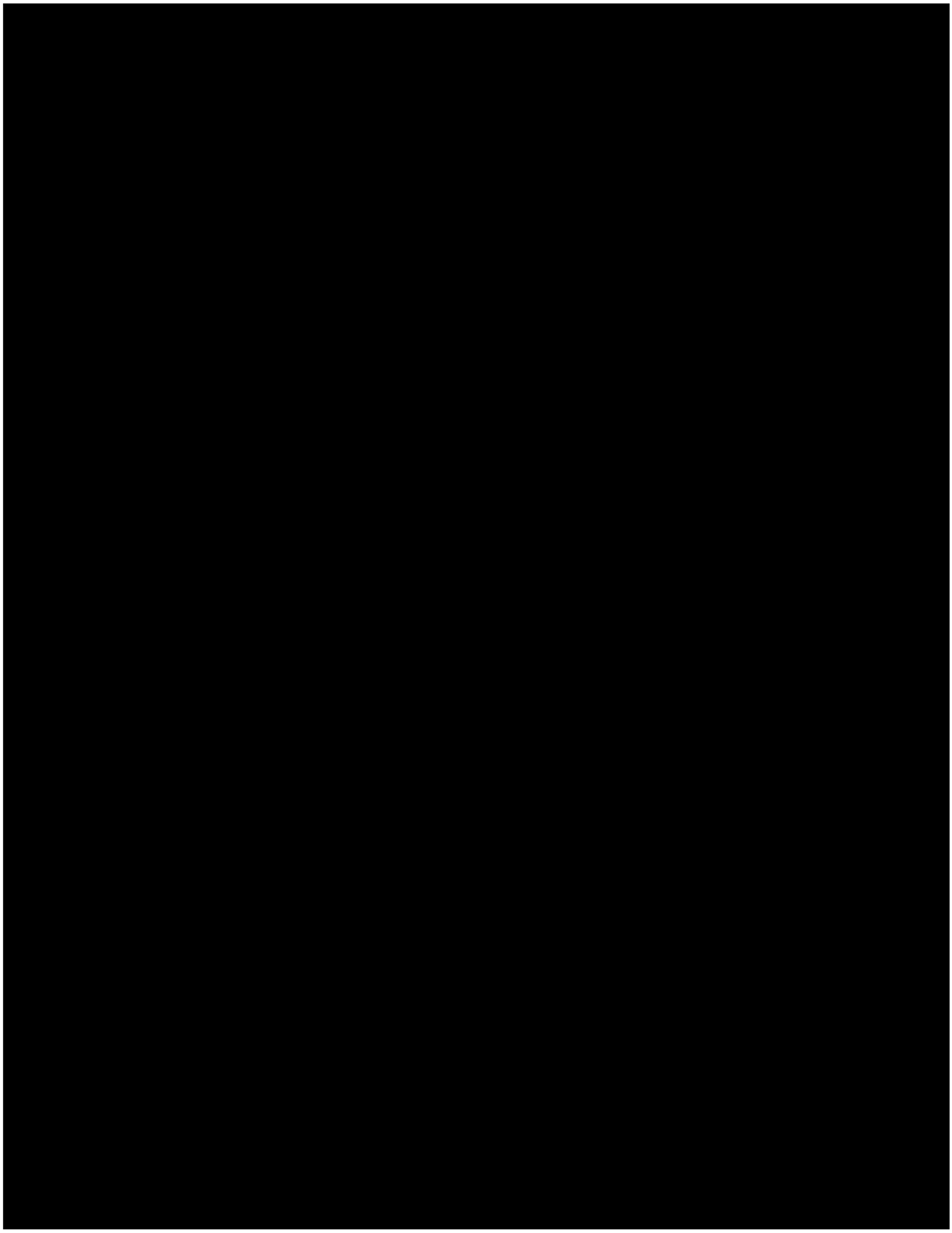
NSL Congressional Q&A to Congr...

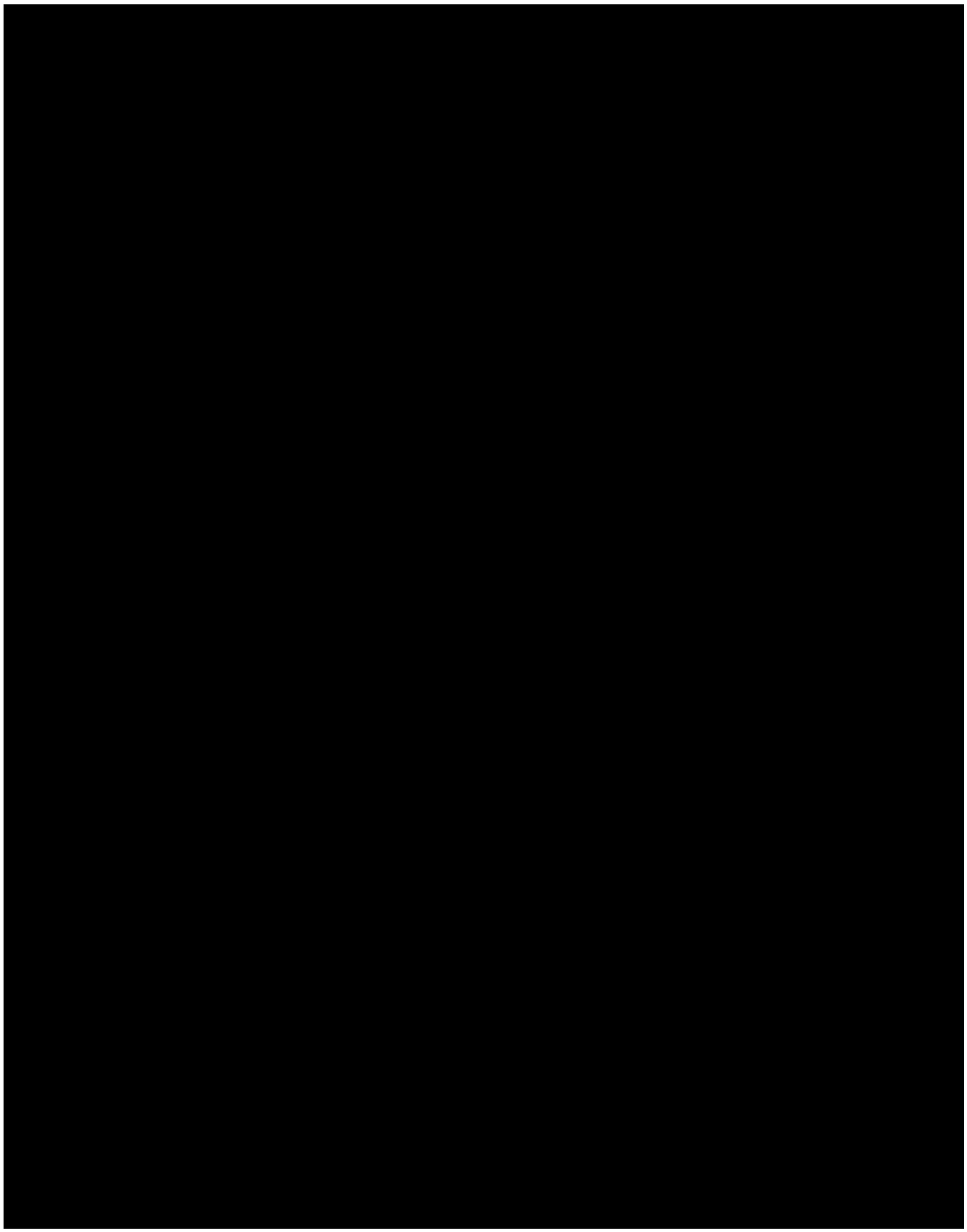
UNCLASSIFIED

<<07-01-19 NSL Talking Points.doc>> <<07-01-19 OUSD(I) NSL Briefing.ppt>> <<NSL Congressional Q&A to Congress 070125.doc>>

[redacted]

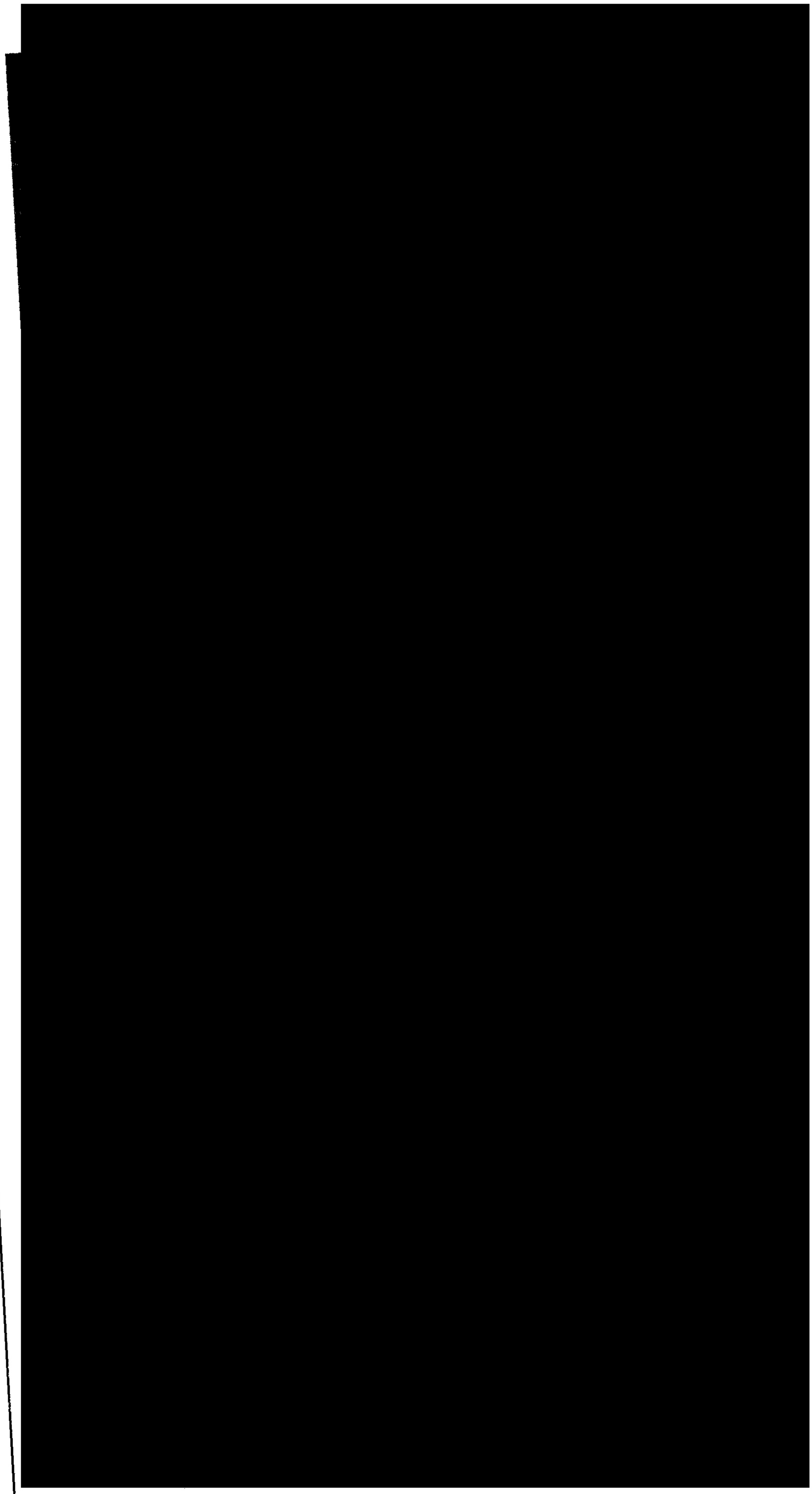






[redacted]

[redacted]



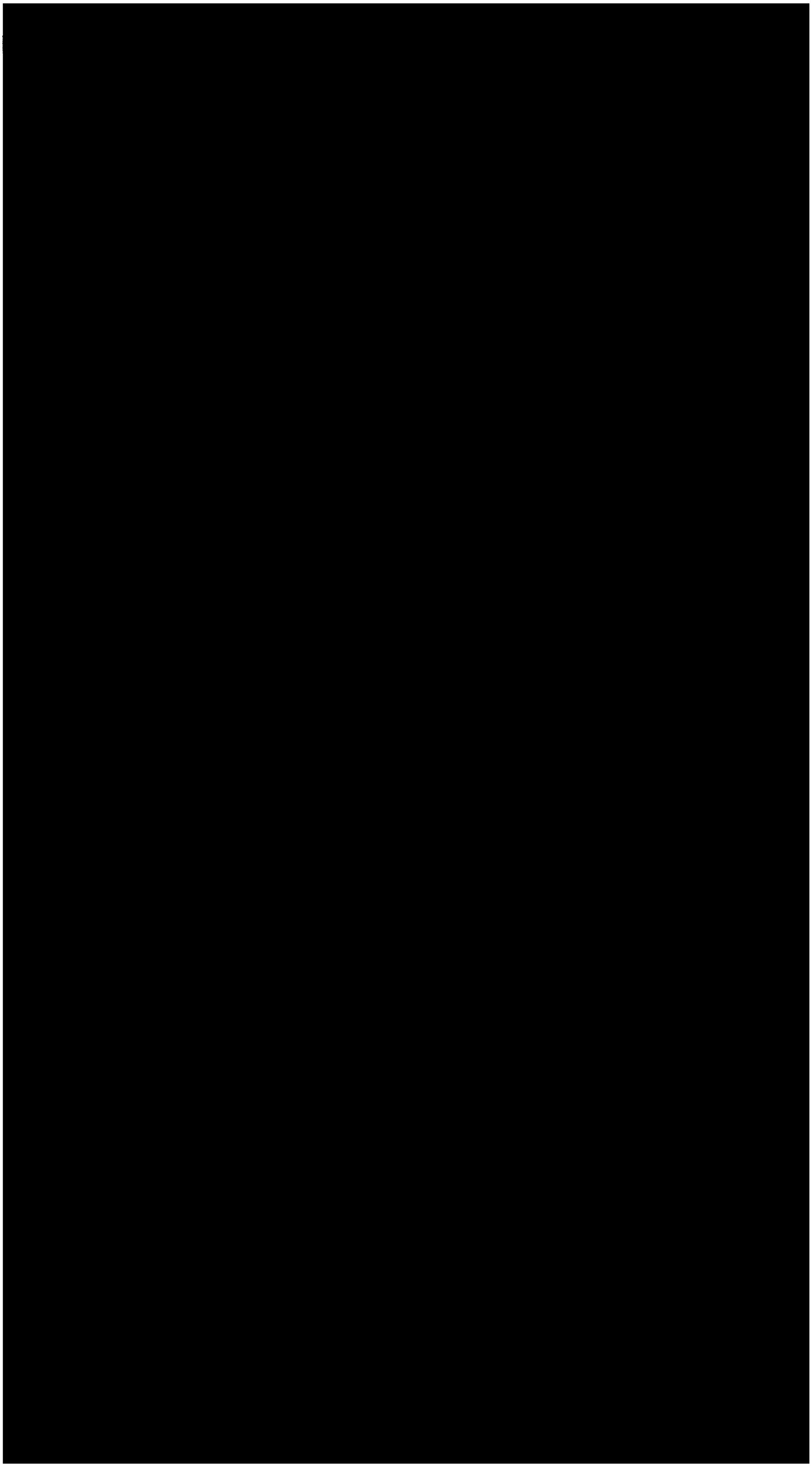
[redacted]

[redacted]

[redacted] USD (CI&S), OUSD (I)

[redacted]

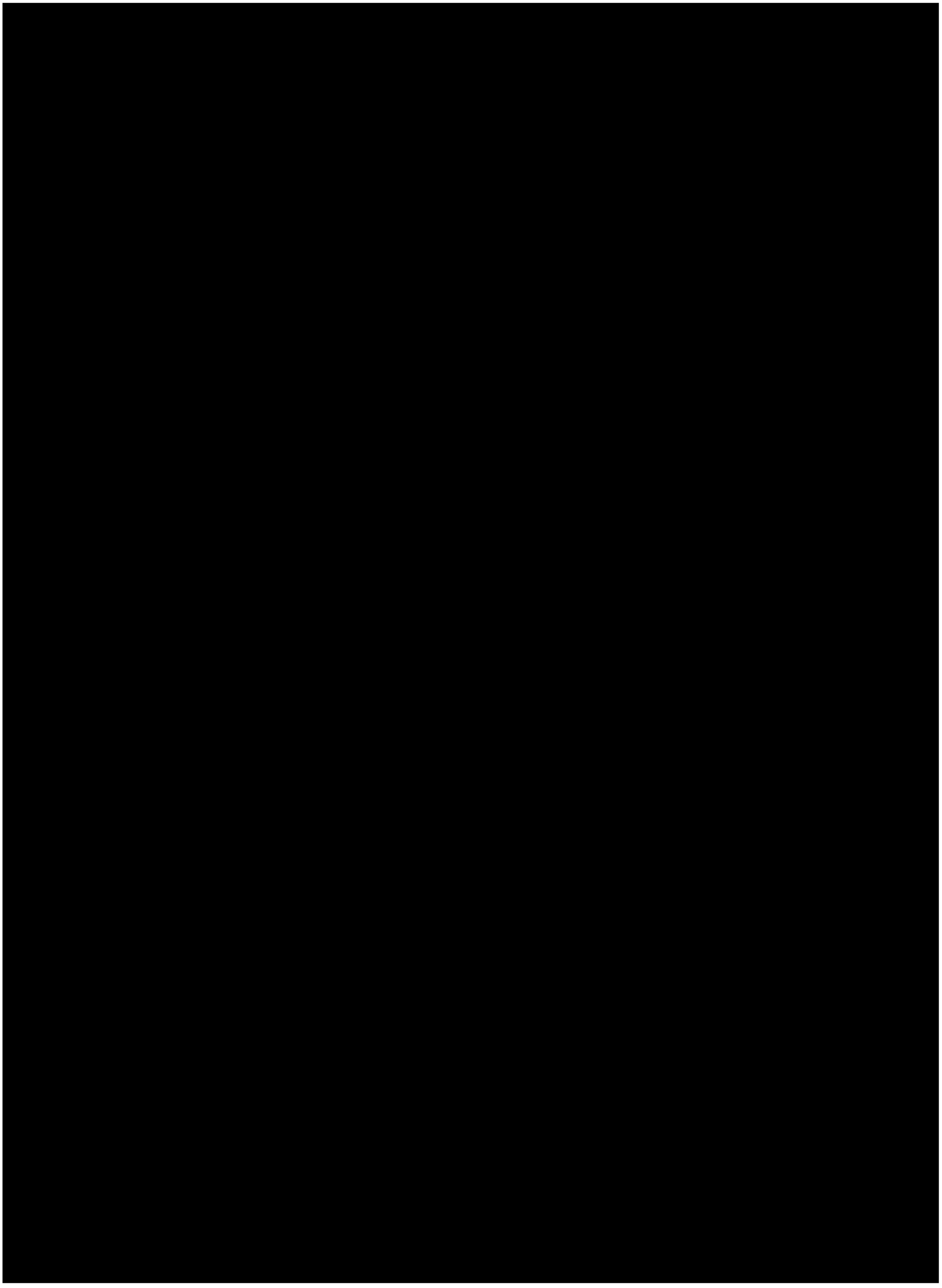
- National [redacted]

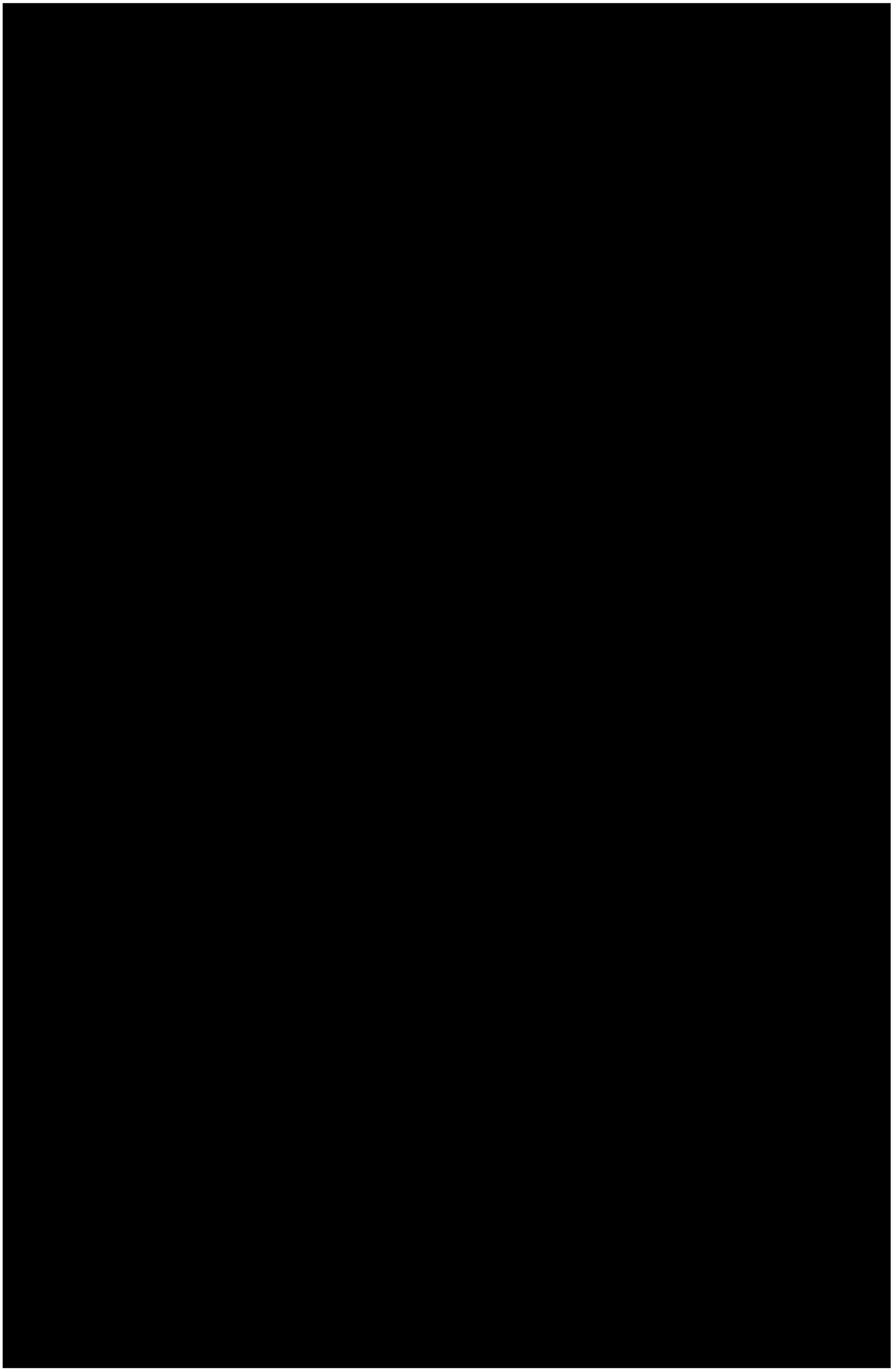


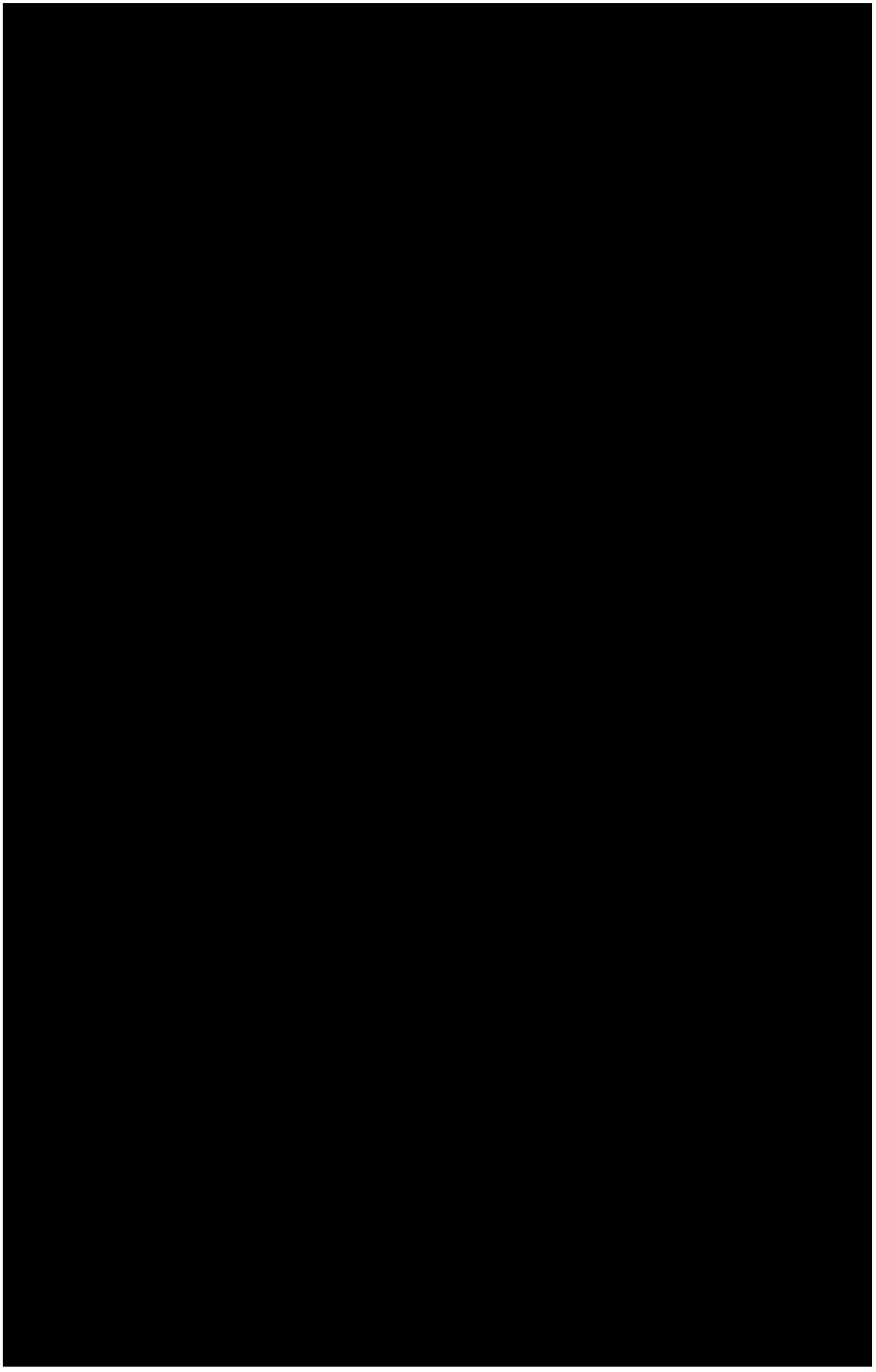
[redacted]

[redacted]

- Enforcement of

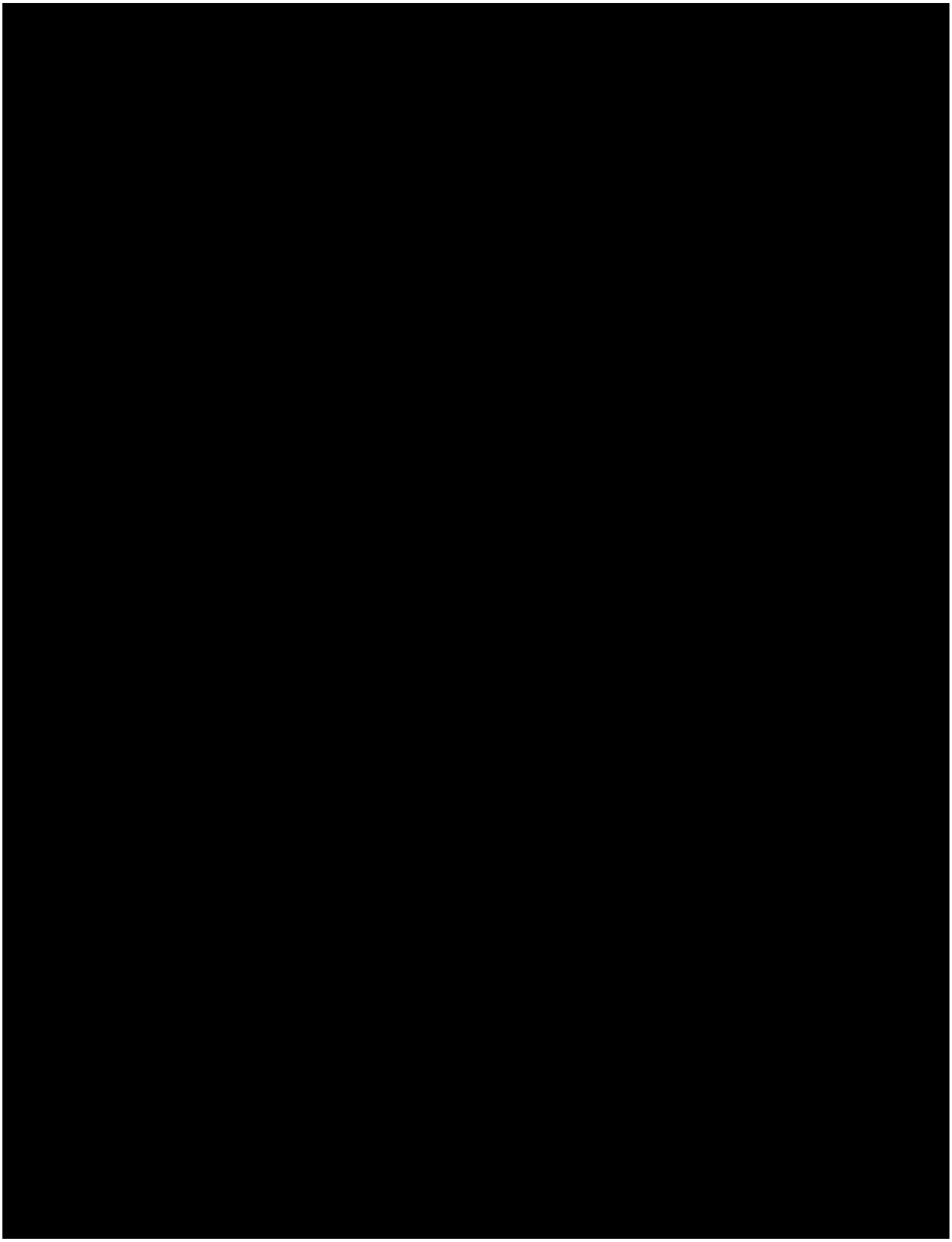


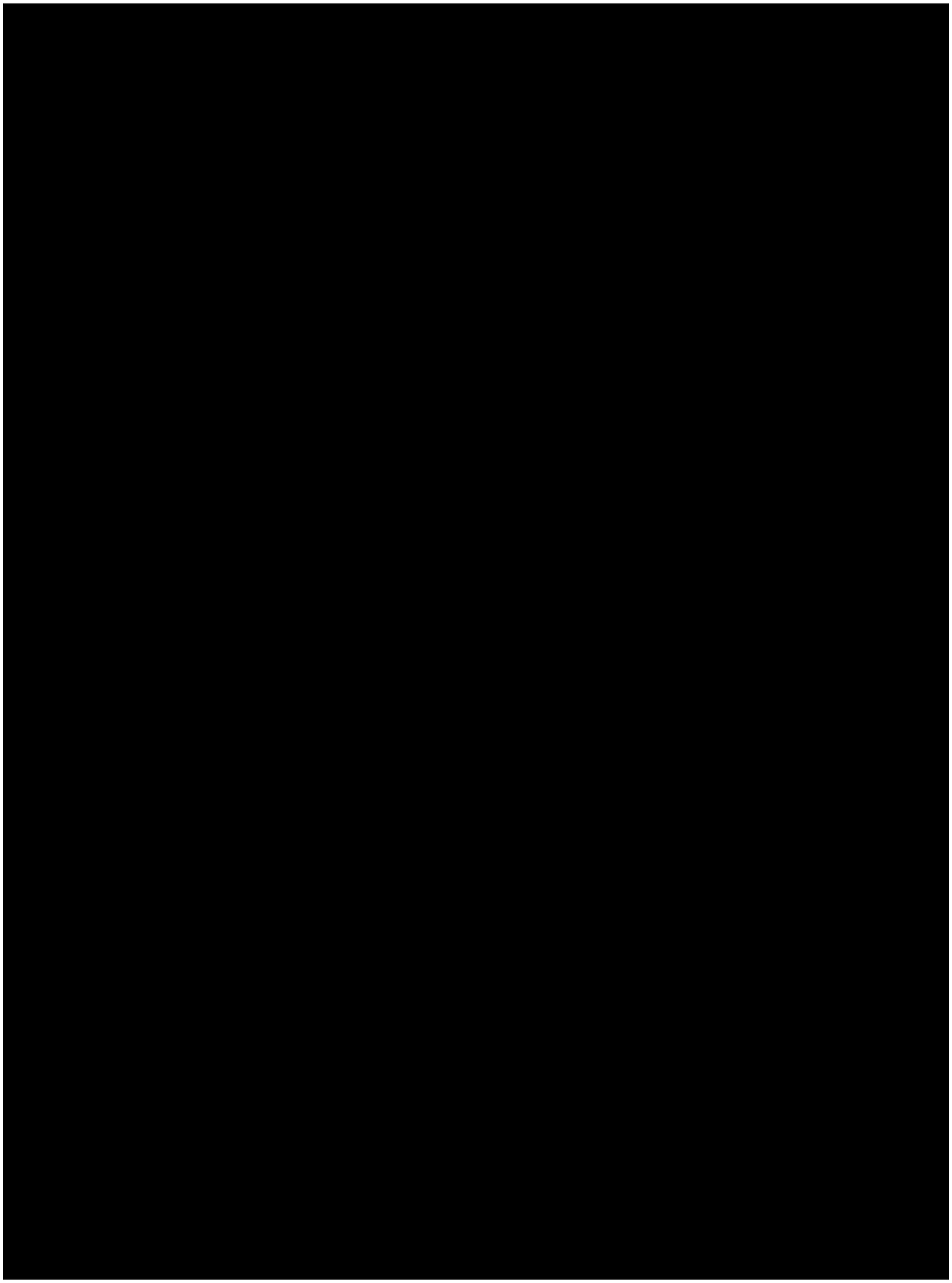


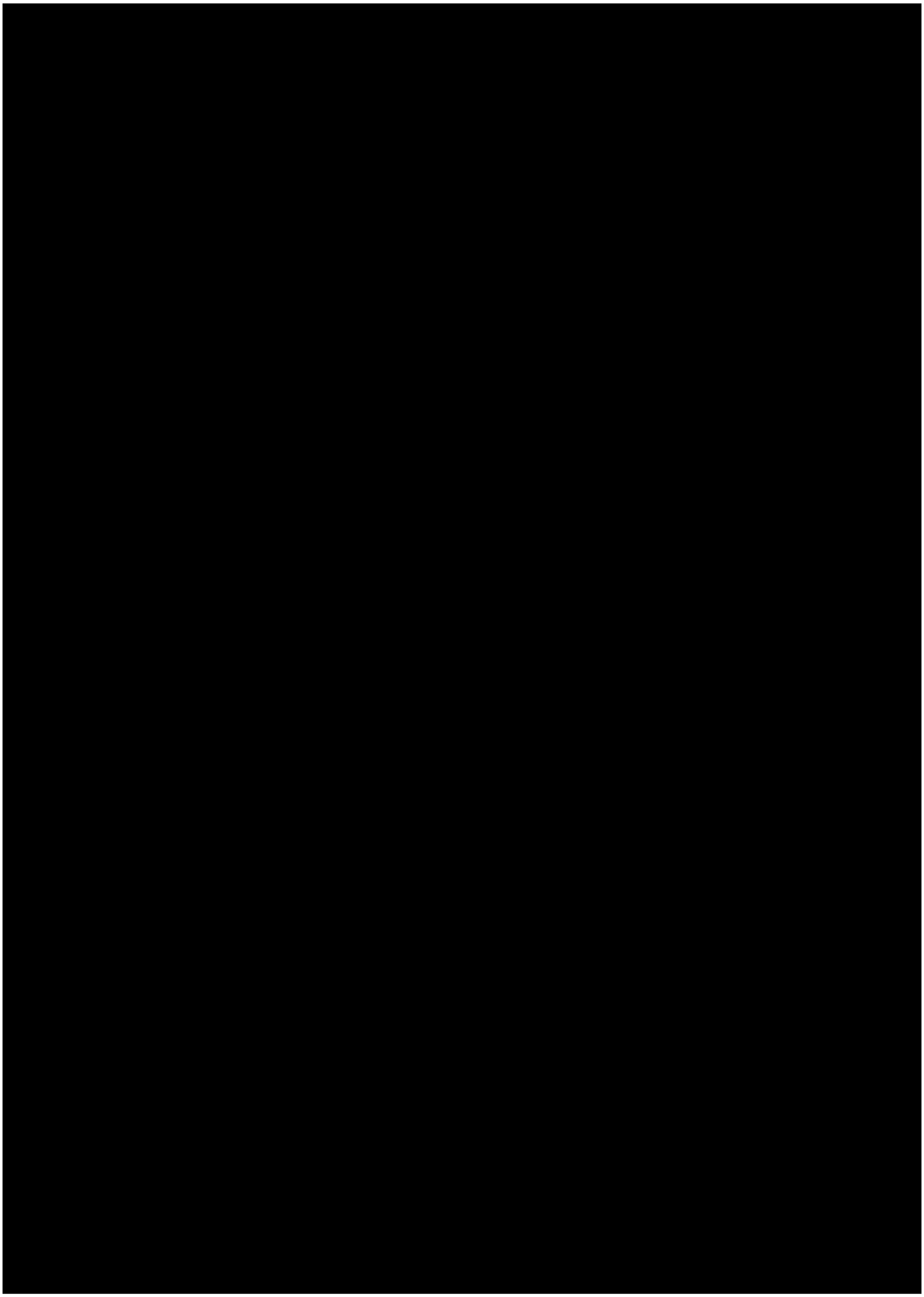


[redacted]

policy in this area.







[redacted]

From: [redacted]
Sent: Friday, February 09, 2007 11:02 AM
To: [redacted]
Subject: NSL Docs Part II (U)

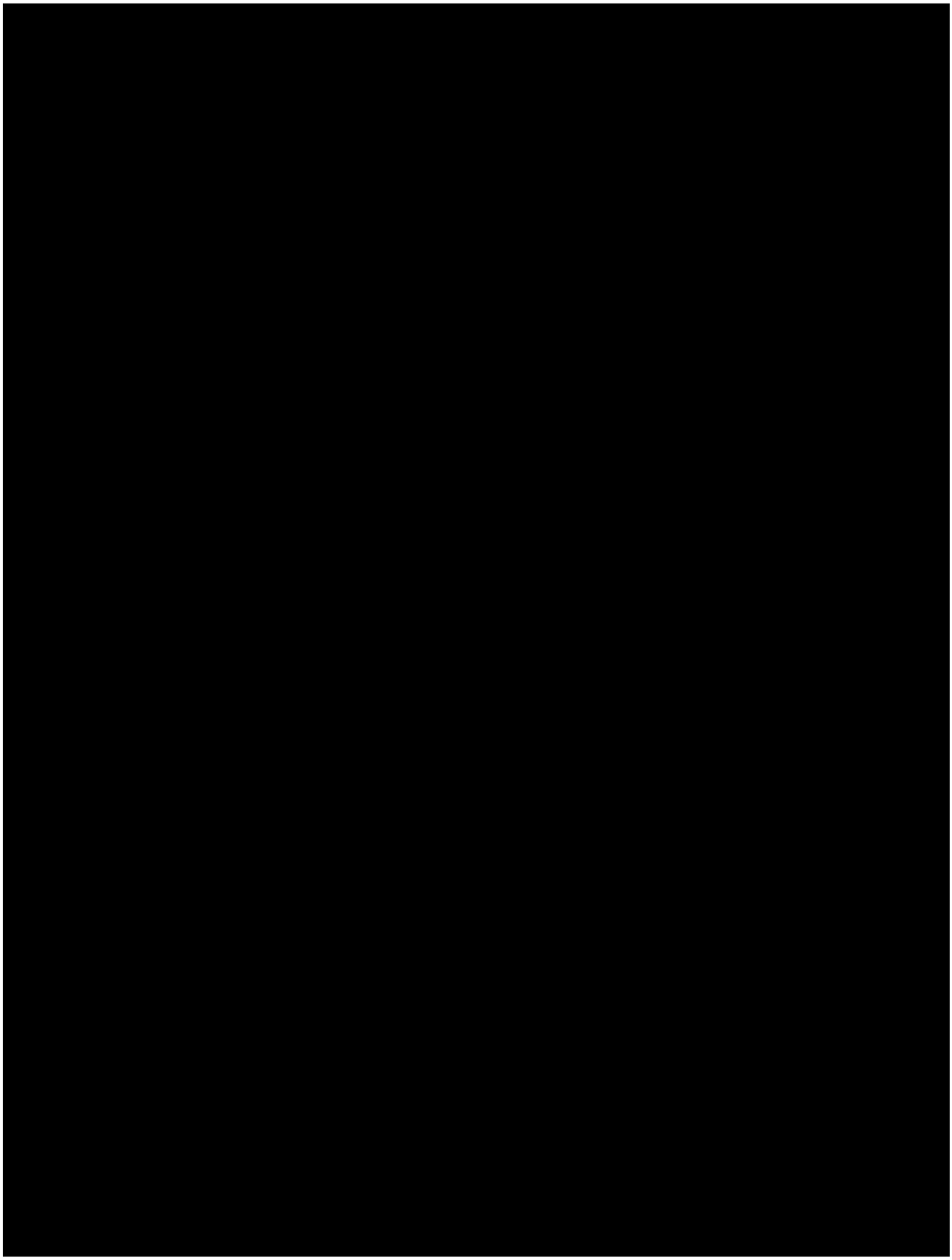
Attachments: 07-01-13 DoD NSL Fact Sheet Released.doc; 07-01-16 DoD NSL Fact Sheet Released.doc; 07-01-19 NSL Reporting Stats to SAC-D Staffers on 24 Jan.doc

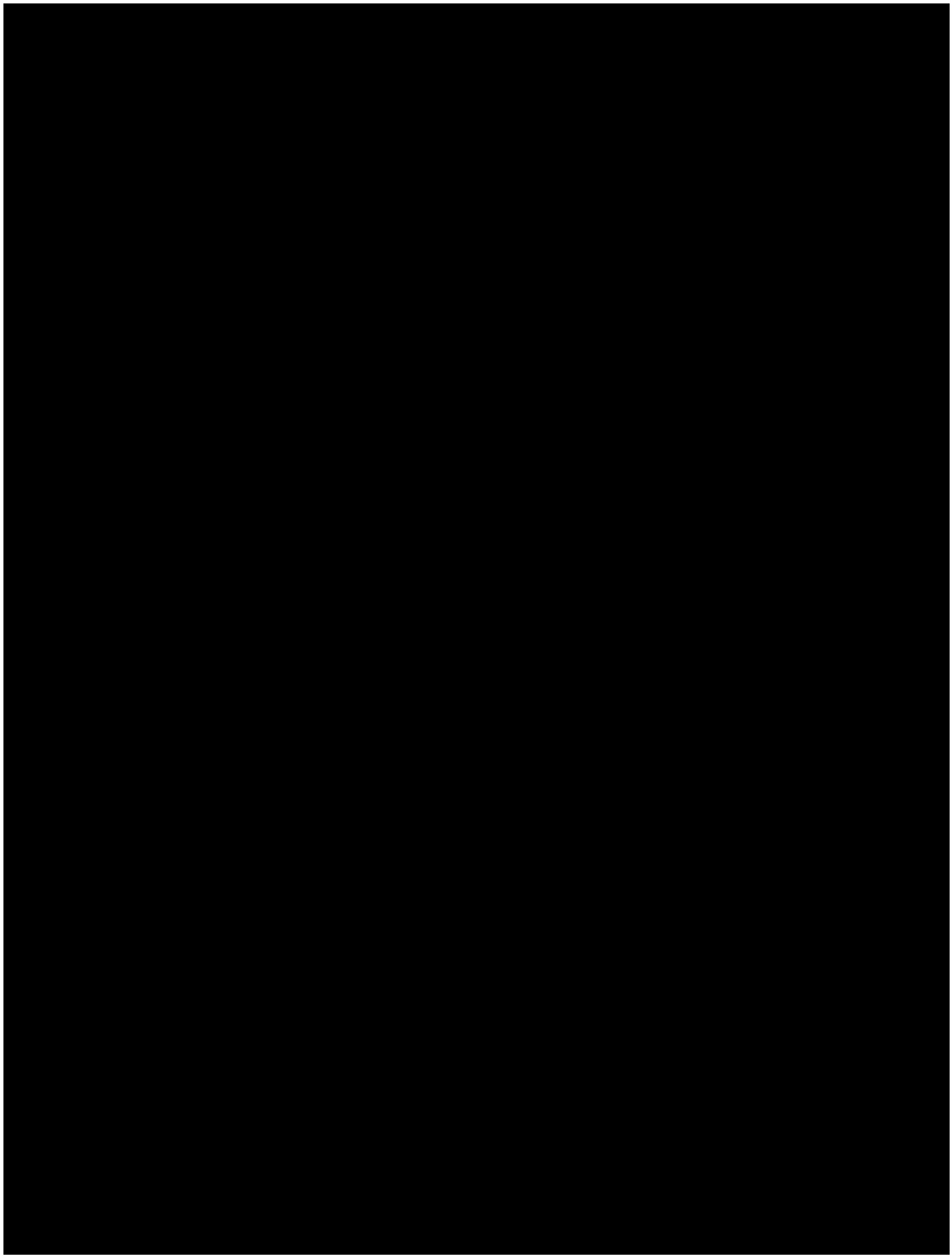
UNCLASSIFIED

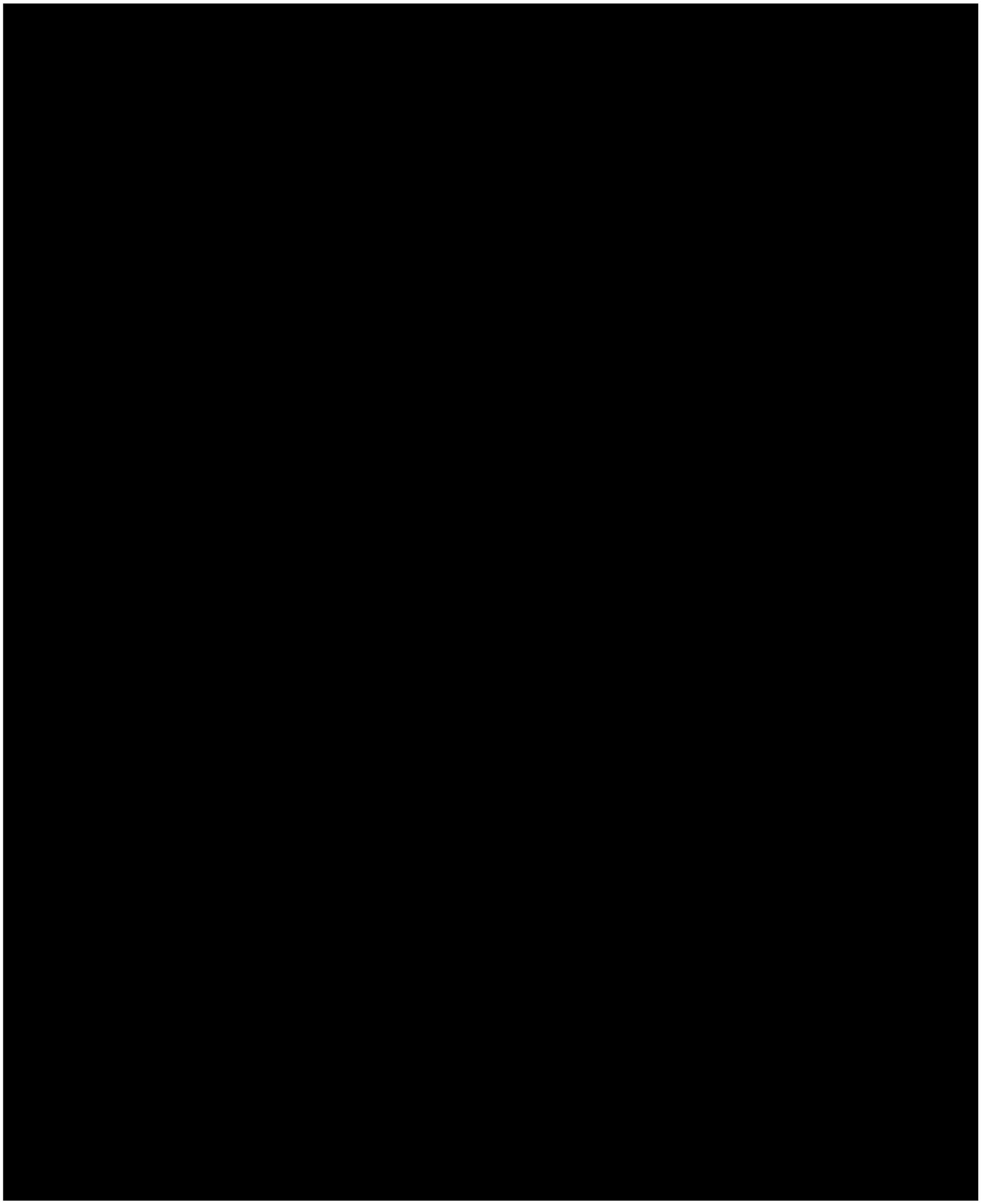
Will start sending what we've published so far.

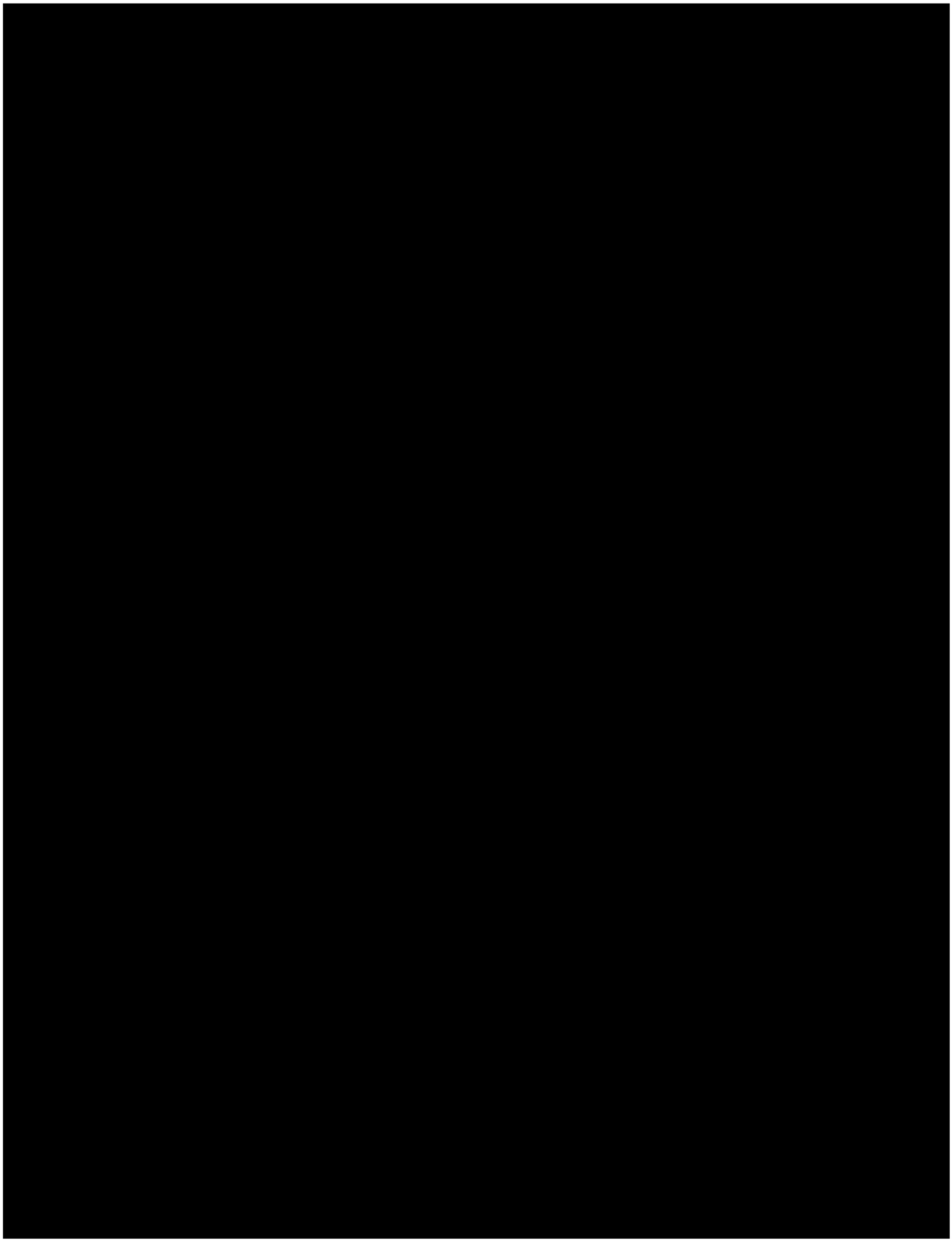
[redacted]

<<07-01-13 DoD NSL Fact Sheet Released.doc>> <<07-01-16 DoD NSL Fact Sheet Released.doc>>
<<07-01-19 NSL Reporting Stats to SAC-D Staffers on 24 Jan.doc>>









[redacted]

From: [redacted]
Sent: Friday, February 09, 2007 11:01 AM
To: [redacted]
Subject: NSL Documents (U)

Attachments: Army CI draft Financial Checks Handbook.doc; NCIS NSL process.doc

Army CI draft Financial Checks...

NCIS NSL process.doc (28 KB)

UNCLASSIFIED

As requested. I also have a few on SIPR, will send them, too.

[redacted]

<<Army CI draft Financial Checks Handbook.doc>> <<NCIS NSL process.doc>>

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

15-10 Financial Checks

a. Legal and Regulatory Framework. The right to privacy extends to the financial aspects of a person's life. Because the U.S. financial system is complex and consists of several different types of institutions each covered by different laws and regulations; it will come as no surprise that there are also several portions of the USC that government's ability to access those records. In the following paragraphs the major relevant portions of the USC are identified and discussed with an emphasis on the authorities, exceptions and procedures that allow CI agents to access them.

(1) Fair Credit Reporting Act (15 USC 1681). The Fair Credit Reporting Act was passed to ensure the privacy, as well as the fair and accurate reporting of consumer credit information for a multitude of purposes including employment and credit worthiness. The act significantly restricts the ability of the government to perform un-consented checks of consumer reporting agency records (AKA credit reporting services). Generally, these records can be obtained only with consent or by a warrant, judicial or administrative subpoena or other court order.

(a) Exception for Identifying Data. A general exemption (15 USC 1681f) allows all governmental agencies (including Army CI) access to limited identification information. Upon the presentation of a formal written request, consumer reporting agencies will provide, name and address, former addresses, places of employment and former places of employment for named consumers. This limited authority can be used for all authorized investigative and operational purposes. (LINK to template of Request)

(b) FBI CI Exception. The original act provided the FBI a specific exception for disclosures for CI purposes (15 USC 1681u). A similar general exception for military CI services does not exist. However, the FBI exception specifically authorized the FBI to disseminate results of their checks to appropriate investigative authorities within the military as may be necessary for the conduct of a joint foreign CI investigation. Additionally, it authorizes the FBI to provide information to the military for SUBJECTs who fall under the UCMJ.

(c) Exception for International Terrorism. The PATRIOT Act added a broader exception for international terrorism (15 USC 1681v), which allows **any government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism** to conduct un-consented checks of these records. Army CI may utilize this exception. A formal written request certifying compliance with the code is required. (LINK to Consumer Reporting Services Template)

(2) Right to Financial Privacy Act of 1978 (12 USC 3401-3422). The Right to Financial Privacy Act is the primary source of financial privacy rights and governs a broad spectrum of records across a wide variety of financial institutions. Government access to records

of financial institutions may be obtained through consent, search warrant, administrative or judicial subpoena, court order or formal written request.

(a) FCI and Terrorism Exceptions. Specific exceptions exist for FCI and international terrorism (15 USC 3414(a)(1)(a) and (c) respectively). These exceptions apply to any government authority authorized to conduct foreign counterintelligence, positive intelligence or international terrorism activities. They allow un-consented checks of financial institution records upon presentation of an appropriately signed formal written request certifying compliance with the act. (LINK to template)

(b) Definition of Financial Institution. The definition of financial institution for the purposes of the exceptions outline above is broader than for the rest of the act (see 15 USC 3414(d)). The following are defined as financial institutions IAW 31 USC 5312(a)(2) and (c)(1).

(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813 (h)));
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) any credit union;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones, or jewels;
(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and settlements;
(V) the United States Postal Service;
(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which—
(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or

> **(ii)** is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
> **(Y)** any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
> **(Z)** any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

(c) Army Implementation Guidance. AR 190-6, Obtaining Information from Financial Institutions, dated 15 January 1982, implements DODD 2400.12 and the Right to Financial Privacy Act of 1978 (12 USC 3401 *et seq*). It provides additional guidance on obtaining information from financial institutions by consent, search warrant, judicial subpoena, and formal written request. Generic sample templates for each type of request are provided. A specific exception for Foreign Intelligence and Foreign Counterintelligence may be found at para 2-10. This paragraph also delegates signature authority for certificates of compliance with 12 USC 3414(a)(3) to Military Intelligence Group Commanders, investigative control office, CG (or DCG) INSCOM.

[redacted]

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

[redacted]

c. Financial Crimes Information Network (FINCEN) Checks. FINCEN checks are considered a NAC, therefore ACCO will coordinate all FINCEN checks. This is the only authorized channel for FINCEN queries. The following information must be provided to ACCO for each request: ACCO CCN; Full name, any/all AKA, relationship in case (subject/witness); Address and phone number; DPOB; SSAN; Race/ethnicity; Sex; Height/weight; Color of eyes and hair; Other identifying data if available, such as passport number; Financial institution(s) known to be utilized; If joint/bilateral case, list other agencies involved. Specify what type of product you desire from FINCEN e.g. analytical reports and/or data base extracts.

NCIS PROCESS FOR USE OF NSLs

NCIS exercises its authority to issue National Security Letters (NSLs) under three statutes: The Right to Financial Privacy Act, or RFPA (12 USC 3414, authority dating to 1978), which may be exercised in counterintelligence (including counterterrorism) investigations; the Fair Credit Reporting Act, or FCRA (15 USC 1681v, authority dating to 2001), which may be exercised only in support of counterterrorism (CT) investigations, activities, or analysis; and the National Security Act (50 USC 436, authority dating to 1994), which authorizes investigative agencies to request - as part of an authorized law enforcement investigation, counterintelligence (CI) inquiry, or security determination - certain financial, consumer reporting, and commercial information pertaining to government personnel for which they have investigative responsibility and who meet certain criteria, including recent access to classified information. NCIS exercises these authorities only in cases for which it has investigative jurisdiction.

The NCIS process for issuing an NSL under these statutes is as follows:

1. The case agent submits a draft NSL, along with supporting documents, to the appropriate NCIS headquarters desk officer (CI or CT).

2. If the desk officer finds the documentation meets all requirements, it is forwarded to an attorney in the National Security Law Unit (NSLU) at NCIS headquarters for a legal review.

3. The NSLU attorney reviews the documentation to ensure that all the criteria of the relevant statute are met and that the draft NSL contains all required information.

4. If the NSLU legal review supports the request for an NSL, the documentation is forwarded to one of a small number of senior officials, all at NCIS headquarters, for final review and signature. The total number of senior officials authorized to sign an NSL within NCIS varies depending upon which statute is invoked, but in no case exceeds seven.

5. Assuming an authorized senior NCIS official signs the NSL, the case agent or desk officer must contact the intended recipient of the NSL before it can be transmitted, in order to assure that the recipient is appropriately sensitized to both investigative and privacy considerations.

NCIS is a federal law enforcement agency within the Department of the Navy (DON). It has exclusive investigative jurisdiction for CI, including acts of espionage and terrorism, within the DON. It is comprised overwhelmingly of civilians and has an exclusively civilian leadership structure. The Director, NCIS is a career law enforcement professional who reports directly to the Secretary of the Navy.

[redacted]

From: [redacted]
Sent: Thursday, February 08, 2007 9:54 AM
To: [redacted]
Subject: NSL info

Attachments: NSL stats.doc; NCIS NSL process1.doc

NSL stats.doc (56 KB)

NCIS NSL process1.doc (32 KB [redacted]

I hope your meetings with Army and AF went well. Attached are the figures we have to date. Please do not disseminate them. They are for use in your report only as our official response for the Hill go through Office of Leg Affiars and DoN OGC.

Please advise if you have questions.

R/

[redacted]

<<NSL stats.doc>> <<NCIS NSL process1.doc>>

NCIS PROCESS FOR USE OF NSLs

NCIS exercises its authority to issue National Security Letters (NSLs) under three statutes: The Right to Financial Privacy Act, or RFPA (12 USC 3414, authority dating to 1978), which may be exercised in counterintelligence (including counterterrorism) investigations; the Fair Credit Reporting Act, or FCRA (15 USC 1681v, authority dating to 2001), which may be exercised in support of counterterrorism investigations, activities, or analysis; and the National Security Act (50 USC 436, authority dating to 1994) that authorizes government investigative agencies to request - as part of an authorized law enforcement investigation, counterintelligence inquiry, or security determination - certain financial, consumer reporting, and commercial information pertaining to government personnel for which they have investigative responsibility and who meet certain criteria, including recent access to classified information. NCIS exercises these authorities only in certain circumstances: (1) In those cases in which the agency has primary jurisdiction; (2) In those cases in which the FBI has deferred primary jurisdiction to NCIS; or (3) In those cases in which the FBI asks NCIS to issue such an NSL in furtherance of a joint NCIS-FBI investigation.

The NCIS process for issuing an NSL under each of the applicable statutes is as follows:

1. The case agent submits a draft NSL, along with the supporting documentation, to the appropriate NCIS desk officer (CI or CT).

2. If the desk officer finds the documentation meets all requirements, it is forwarded to an attorney in the NCIS National Security Law Unit (NSLU) for a legal review.

3. The NSLU attorney reviews the documentation to ensure that all the criteria of the relevant statute are met and that the draft NSL contains all required information.

4. If the NSLU legal review supports the request for an NSL, the documentation is forwarded to one of a small number of senior officials at NCIS headquarters for final review and signature. The total number of headquarters officials authorized to sign an NSL within NCIS varies depending upon which statute is invoked, but in no case exceeds seven.

5. Assuming an authorized senior NCIS official signs the NSL, the case agent or desk officer must contact the intended recipient of the NSL before it can be transmitted, in order to assure that the recipient is appropriately sensitized to both investigative and privacy considerations.

[redacted]

From: [redacted]
Sent: Wednesday, January 31, 2007 7:57 AM
To: [redacted]
Subject: FW: Financial Checks (aka: NSLs)

Attachments: Financial Checks-540012p[1].pdf; Financial Checks-i540015p[1].pdf

Financial ecks-540012p[1].pd

Financial ecks-i540015p[1].p

[redacted] Did not mean to leave you out. Don't know if you have these already, if not enjoy!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 31, 2007 7:53 AM
To: [redacted]
Subject: FW: Financial Checks (aka: NSLs)

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 30, 2007 6:17 PM
To: [redacted]
Subject: Financial Checks (aka: NSLs)

Attached are the DoD Directive and DoD manual that cover financial checks.

[redacted] let me know that you received. I often get a kickback response when I actually think you got the email.

[redacted]

From: [redacted]
Sent: Tuesday, January 30, 2007 3:30 PM
To: [redacted]
Subject: FW: NSLs and the SASC (U)

FYI.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 30, 2007 3:23 PM
[redacted]
Subject: RE: NSLs and the SASC (U)

[redacted] - Our poc will continue to be [redacted] our National Security Lawyer..... Thanks r[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:59
[redacted]
Subject: RE: NSLs and the SASC (U)
Importance: High

Recipients on the "To" Line: in reference to the NSL issue, Acting DUSD(CI&S) has directed CIFA to undertake a program review of the utilization of NSLs by the Service CI components (see attached memo from Acting DUSD(CI&S) dated Jan 25, 2007. [redacted] of the CIFA Program Management Directorate will be leading this effort on behalf of CIFA.
It is requested that you designate a POC for this review and that you ensure that any information provided in response to the taskers identified in the below e-mail from [redacted] are made available as well to [redacted] for the purpose of this review.

Your cooperation and timely response to this matter is greatly appreciated.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:46 AM
[redacted]
Subject: NSLs and the SASC (U)

Classification: UNCLASSIFIED

[redacted]

Please contact [redacted] if you have any questions.

Regards,

[redacted]

[redacted]

From: [redacted]
Sent: Monday, January 29, 2007 8:20 AM
To: [redacted]
Cc:
Subject: RE: NSLs and the SASC (U)

Yes, concur.

-----Original Message-----
From: [redacted]
Sent: Monday, January 29, 2007 7:27 AM
To: [redacted]
Cc: [redacted]
Subject: RE: NSLs and the SASC (U)

[redacted]

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 3:50 PM
To: [redacted]
Subject: FW: NSLs and the SASC (U)
Importance: High

FYI,...

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 9:33 AM
To: [redacted]
Subject: FW: NSLs and the SASC (U)
Importance: High

[redacted] fyi this is another review we've been directed to undertake. [redacted] has the lead in [redacted] Office.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:59 AM
To: [redacted]

[redacted]

[redacted]

Subject: RE: NSLs and the SASC (U)
Importance: High

Recipients on the "To" Line: in reference to the NSL issue, Acting DUSD(CI&S) has directed CIFA to undertake a program review of the utilization of NSLs by the Service CI components (see attached memo from Acting DUSD(CI&S) dated Jan 25, 2007. [redacted] of the CIFA Program Management Directorate will be leading this effort on behalf of CIFA. It is requested that you designate a POC for this review and that you ensure that any information provided in response to the taskers identified in the below e-mail from [redacted] are made available as well to [redacted] for the purpose of this review.

Your cooperation and timely response to this matter is greatly appreciated.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 8:46 AM
To: [redacted]

Subject: NSLs and the SASC (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Please contact [redacted] if you have any questions.

Regards,

[redacted]

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 10:46 AM
To: [redacted]
Cc:
Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

No problem. We will get you a name soonest.

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 9:26 AM
To: [redacted]
Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

I have tasked my policy coord shop to assist your lead POC [redacted] and [redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 7:45 AM
[redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

[redacted] reference my previous e-mail regarding this tasker we were expecting from [redacted] relating to the NSL issue we've been briefing to the various Congressional committees. DP will take the lead on this [redacted] leading), but we would appreciate DC designating someone to assist (ideally from [redacted] shop). I note that [redacted] did not designate DC in the assist line, but I have asked her to retransmit the tasker officially to include DC.

[redacted] would appreciate your assistance as well from a JCITA and a policy perspective. Request you designate a POC to assist [redacted] on this. Thanks!

This has high level Congressional interest and DNI interest and we need to get this done quickly and thoroughly.

Thanks!

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 10:09 AM
To: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

[redacted]

Let me know if you need a Policy assist with this tasker. We're happy to help.

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 9:26 AM
To: [redacted]

Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

I have tasked my policy coord shop to assist your lead POC [redacted] and [redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 7:45 AM
[redacted]

Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

[redacted] reference my previous e-mail regarding this tasker we were expecting from [redacted] relating to the NSL issue we've been briefing to the various Congressional committees. DP will take the lead on this [redacted] leading), but we would appreciate DC designating someone to assist (ideally from [redacted] shop). I note that [redacted] did not designate DC in the assist line, but I have asked her to retransmit the tasker officially to include DC.

[redacted] would appreciate your assistance as well from a JCITA and a policy perspective. Request you designate a POC to assist [redacted] on this. Thanks!

This has high level Congressional interest and DNI interest and we need to get this done quickly and thoroughly.

Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 8:08 AM
To: [redacted]
Cc:

Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

The DCAC action officer for this task is [redacted]

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 7:54 AM
To: CILEC Management Team; CILEIO Admin; CMIT DAG
Cc: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

FOR DCAC; Support DCC

!. (U) Your office has been assigned the following task: Support DP in preparing response on NSLs. (see below and attached)

2. (U) Please enter this task into your weekly spreadsheet. Advise [redacted] and the CILEC Management Team of your action officer within 24 hours.

3. (U) This task requires that DC provide input to DP as requested by DP. Contact [redacted] for details. Advise [redacted] of proposed responses.

4. (U) Suspense for contacting [redacted] is 1200 26 Jan.

Per:

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 7:45 AM
[redacted]

Cc: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

[redacted] reference my previous e-mail regarding this tasker we were expecting from [redacted] relating to the NSL issue we've been briefing to the various Congressional committees. DP will take the lead on this [redacted] leading), but we would appreciate DC designating someone to assist (ideally from [redacted] shop). I note that [redacted] did not designate DC in the assist line, but I have asked her to retransmit the tasker officially to include DC.

[redacted] would appreciate your assistance as well from a JCITA and a policy perspective. Request you designate a POC to assist [redacted] on this. Thanks!

This has high level Congressional interest and DNI interest and we need to get this done quickly and thoroughly.

Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 7:57 AM
To: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Importance: High

Attachments: 07-01-25 Program Management Review.pdf

07-01-25 Program Management Re...

FYI -

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 7:54 AM
To: CILEC Management Team; CILEIO Admin; CMIT DAG
Cc: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

FOR DCAC; Support DCC

!. (U) Your office has been assigned the following task: Support DP in preparing response on NSLs. (see below and attached)

2. (U) Please enter this task into your weekly spreadsheet. Advise [redacted] and the CILEC Management Team of your action officer within 24 hours.

3. (U) This task requires that DC provide input to DP as requested by DP. Contact [redacted] for details. Advise [redacted] of proposed responses.

4. (U) Suspense for contacting [redacted] is 1200 26 Jan.

Per:

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 7:45 AM
[redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

[redacted] reference my previous e-mail regarding this tasker we were expecting from [redacted] relating to the NSL issue we've been briefing to the various Congressional committees. DP will take the lead on this [redacted] leading), but we would appreciate DC designating someone to assist (ideally from [redacted] shop). I note that [redacted] did not designate DC in the assist line, but I have asked her to retransmit the tasker officially to include DC.

[redacted] would appreciate your assistance as well from a JCITA and a policy perspective. Request you designate a POC to assist [redacted] on this. Thanks!

This has high level Congressional interest and DNI interest and we need to get this done quickly and thoroughly.

Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 7:25 AM
To: [redacted]
Cc:
Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

You're right about DC - I missed it -- I told her to include DC; not sure why she put DT and DS. I'll have her resend.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 5:36 PM
To: [redacted]
Cc: [redacted]
Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Sir,
It's a good letter, but I wish they would have CC'd the Services.
Not sure why [redacted] did not put DC down for an "assist". We're planning on asking for their help...
V/R
[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 5:11 PM
To: [redacted]
Cc: [redacted]
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

Clock starts ticking today. Note 1 March suspense to Front Office.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Friday, January 26, 2007 7:21 AM
To: [redacted]
Subject: FW: (U)

Importance: High

See [redacted] e-mail/comments below re the NSL review.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 26, 2007 6:23 AM
To: [redacted]
Cc: [redacted]
Subject: (U)

Classification: UNCLASSIFIED

[redacted]

Cheers,

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 25, 2007 5:36 PM
To: [redacted]
Cc:
Subject: RE: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Sir,
It's a good letter, but I wish they would have CC'd the Services.
Not sure why [redacted] did not put DC down for an "assist". We're planning on asking for their help...
V/R
[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 5:11 PM
To: [redacted]
Cc:
Subject: FW: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)
Importance: High

Clock starts ticking today. Note 1 March suspense to Front Office.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 4:05 PM
[redacted]
Subject: CIFA Task 010-07: Program Management Review of DoD's Use of NSLs (USI000069-07) (U)

Lead: DP
Assist: DS, DT

Due to DQ: 1 Mar 07

[redacted]

From: [redacted]
Sent: Thursday, January 25, 2007 5:08 PM
To: [redacted]
Subject: FW: NSL-SASC Staffers (U)

fyi.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 5:04 PM
To: [redacted]
Cc: [redacted]
Subject: NSL-SASC Staffers (U)

Classification: UNCLASSIFIED

Sir,

[redacted]

V/R,

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 25, 2007 2:22 PM
To: [redacted]
Cc:
Subject: RE: NSL Review (U)

Wilco.
V/R
[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 1:34 PM
To: [redacted]
Subject: RE: NSL Review (U)

Looks like it! We have to give this priority given the high level attention this whole "non-issue" issue is getting. Needs to be a thorough scrub.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 1:30 PM
To: [redacted]
Cc:
Subject: RE: NSL Review (U)

Looks like the clock is about to start!

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 1:28 PM
To: [redacted]
Cc:
Subject: FW: NSL Review (U)

Fyi.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 1:10 PM
To: [redacted]
Cc:
Subject: NSL Review (U)

Classification: UNCLASSIFIED

Per our earlier discussions, the memo requesting the review is signed and should be in your box in a matter of minutes or so. Thanks for the help; should be interesting.

Regards.

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 25, 2007 1:28 PM
To: [redacted]
Cc:
Subject: FW: NSL Review (U)

Fyi.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 25, 2007 1:10 PM
To: [redacted]
Cc:
Subject: NSL Review (U)

Classification: UNCLASSIFIED

Per our earlier discussions, the memo requesting the review is signed and should be in your box in a matter of minutes or so. Thanks for the help; should be interesting.

Regards.

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, January 24, 2007 2:02 PM
To: DP CAFS Office
Cc: [redacted]
Subject: Fyi -- lawful use

Fyi...

USA Today
January 24, 2007
Pg. 12
Pentagon 'Committed To Lawful Use'
USA TODAY's editorial "No court order needed" was misleading in its portrayal of the Defense Department's ability to request financial and credit-related information as part of counterintelligence and counterterrorism investigations (Our view, Security and civil liberties debate, Thursday).
The Defense Department is proud of the servicemen and women and civilian personnel who protect our nation from threats of harm, both foreign and domestic, at great cost and sacrifice to themselves. But as history has shown, the threat of infiltration by espionage and the danger to department personnel from terrorism are real. The Defense Department has a responsibility to ensure the security of its information, installations, resources and employees at home and abroad. This is both an operational requirement and a matter of national security for the American people.
As part of this effort, specific organizations in each of the military services are charged with investigating counterintelligence and counterterrorism threats to the Pentagon. As history has also shown, unusual financial activity of people affiliated with the Defense Department can be an indication of espionage or terrorist-related activity.
One valuable tool used in counterintelligence and counterterrorism investigations within the department is the ability to request financial and credit-related information. This tool was extended to investigatory entities other than the FBI by Congress in 2001. Our use of this tool has been focused, limited and judicious.
But the key here is that, contrary to recent press reports, the Pentagon's authority to request such information is limited. It applies only to Defense Department-affiliated investigations concerning the department's affiliated persons. In making such requests, the department ensures that its use is part of a lawful investigation and the department is complying with the standards and requirements of the law. Additionally, the department's application of this authority is done in close coordination with the FBI.
The department is keenly aware of its role in protecting the nation, its citizens and their liberties. The Defense Department is committed to the lawful use of all available resources in that effort.
Bryan G. Whitman, Deputy Assistant Secretary of Defense for Public Affairs, Washington

V/R,
[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, January 23, 2007 4:42 PM
To: [redacted]
Cc:
Subject: RE: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

You are absolutely correct -- [redacted] inflicted this on us by putting it on the table in that forum as well as in the SSCI forum and will probably do so again tomorrow with the SAC-D.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 3:13 PM
To:
Cc: [redacted]
Subject: RE: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

As discussed earlier you are correct; we have not rec the official DUSDI written request to conduct the NSL review and therefore the clock has not started ticking.

Looking at the below email from [redacted] it appears the HAC/D did not put us on the hook to conduct the NSL review, it looks like that is a self inflicted DoD requirement.

Cheers,
[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 11:09 AM
To:
Cc: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

[redacted] just want to clarify that CIFA will not officially begin the NSL review until we get written direction from [redacted] to undertake the review -- is that correct? I want to ensure that the 45-day clock has not yet begun ticking.

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 10:06 AM
To: [redacted]
Cc:
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

FYI.

Hopefully, there won't be too many more.

I really appreciate your help on this.

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 9:45 AM
[redacted]
Cc: [redacted]
Subject: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

FOR OFFICIAL USE ONLY

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, January 23, 2007 11:06 AM
To: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 10:06 AM
To: [redacted]
Cc: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

FYI.

Hopefully, there won't be too many more.

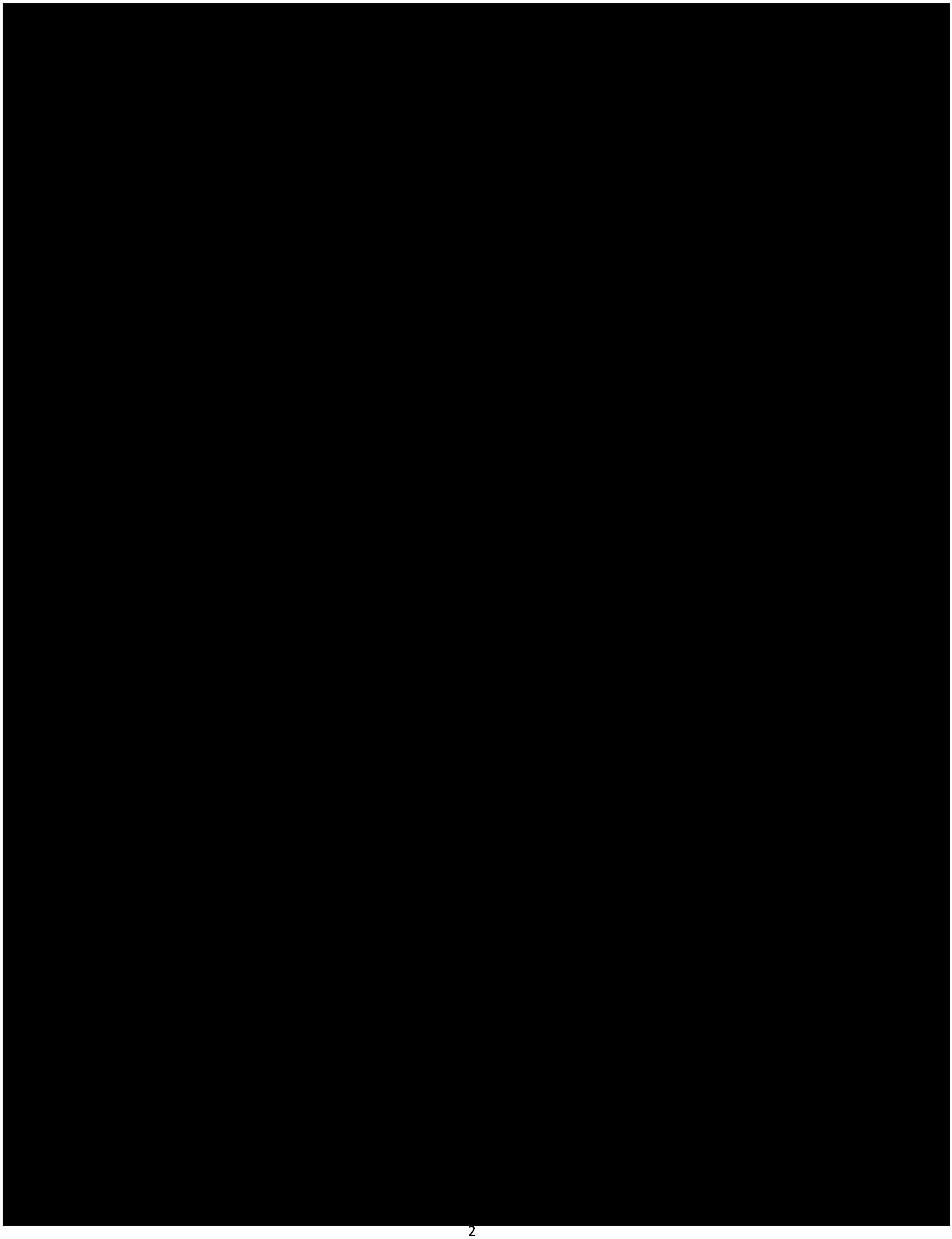
I really appreciate your help on this.

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 9:45 AM
[redacted]
Cc: [redacted]
Subject: QUICKLOOK: Meeting on National Security Letters (NSLs) with HAC/D, 19 January 2007 (U)

FOR OFFICIAL USE ONLY



[redacted]

From: [redacted]
Sent: Tuesday, January 23, 2007 11:24 AM
To: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with SSCI Staff, 19 January 2007 (U)

Summary of SSCI briefing -- FYI.

Note due outs and SSCI interest areas in context of the NSL review we will be tasked to undertake.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 11:20 AM
To: [redacted]
Cc: [redacted]
Subject: FW: QUICKLOOK: Meeting on National Security Letters (NSLs) with SSCI Staff, 19 January 2007 (U)

FYI.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 23, 2007 11:18 AM
To: [redacted]
Cc: [redacted]
Subject: QUICKLOOK: Meeting on National Security Letters (NSLs) with SSCI Staff, 19 January 2007 (U)

UNCLASSIFIED

[redacted]

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Monday, January 22, 2007 9:26 AM
To: [redacted]
Subject: FW: HAC-D and SSCI briefings by ADUSD (CI&S) and Team (U)

FYI

-----Original Message-----
From: [redacted]
Sent: Monday, January 22, 2007 9:19 AM
To: [redacted]
Subject: FW: HAC-D and SSCI briefings by ADUSD (CI&S) and Team (U)

fyi.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 19, 2007 8:24 PM
To: [redacted]
Subject: Re: HAC-D and SSCI briefings by ADUSD (CI&S) and Team (U)

We will be happy to do our part in both efforts. Congrats on results.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
[redacted]
Sent: Fri Jan 19 17:07:43 2007
Subject: FW: HAC-D and SSCI briefings by ADUSD (CI&S) and Team (U)

[redacted]

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, January 19, 2007 4:49 PM
To: [redacted]
Subject: FW: HAC-D and SSCI briefings by ADUSD (CI&S) and Team (U)

Classification: UNCLASSIFIED

Sorry.

-----Original Message-----
From: [redacted]
Sent: Friday, January 19, 2007 4:27 PM
To: [redacted]
Cc: [redacted]
Subject: HAC-D and SSCI briefings by ADUSD (CI&S) and Team (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

V/R,

[redacted]

[redacted]

From: [redacted]
Sent: Friday, January 19, 2007 4:57 PM
To: [redacted]
Subject: NSL review

[redacted]
Heads up.
[redacted] just returned from Capitol Hill and reports that while the briefing went well, [redacted] did commit us to doing a review of DoD use of the NSLs. We've got 45 days to complete the review.
You'll have the lead...and we'll ask [redacted] for a person to assist.
We will get the names of the Service POCs next week (we already know that the Army POC is [redacted]
This may actually turn out to be a good opportunity. We'll discuss Monday.
[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 18, 2007 12:29 PM
To: [redacted]
Cc: [redacted]

Subject: RE: Briefing to Congress (U)

Will do!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 12:27 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Briefing to Congress (U)

[redacted]

V/R [redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 12:17 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Briefing to Congress (U)

[redacted]

Cheers,

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 11:49 AM
To: [redacted]
Subject: FW: Briefing to Congress (U)
Importance: High

The latest version of [redacted] briefing.

Note Slide 14: He did not make the language change as [redacted] recommended.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 11:32 AM
To: [redacted]
Subject: Briefing to Congress (U)

Classification: UNCLASSIFIED

[redacted]

Regards and thanks.

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 18, 2007 12:15 PM
To: [redacted]
Subject: FW: Briefing to Congress (U)

fyi

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 12:12 PM
To: [redacted]
Subject: RE: Briefing to Congress (U)

Classification: UNCLASSIFIED

Missed it. It is now in as:

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 12:01 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Briefing to Congress (U)

[redacted] I note that slide 14, last bullet does not contain the language [redacted] proposed to you earlier.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 11:32 AM
To: [redacted]
Subject: Briefing to Congress (U)

Classification: UNCLASSIFIED

[redacted]

Regards and thanks.

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 18, 2007 11:49 AM
To: [redacted]
Cc: [redacted]
Subject: FW: Briefing to Congress (U)

Importance: High

Attachments: 07-01-19 OUSD(I) NSL Briefing.ppt

07-01-19 OUSD(I) NSL Briefing....

The latest version of [redacted] briefing.

Note Slide 14: He did not make the language change as [redacted] recommended.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 11:32 AM
To: [redacted]
Subject: Briefing to Congress (U)

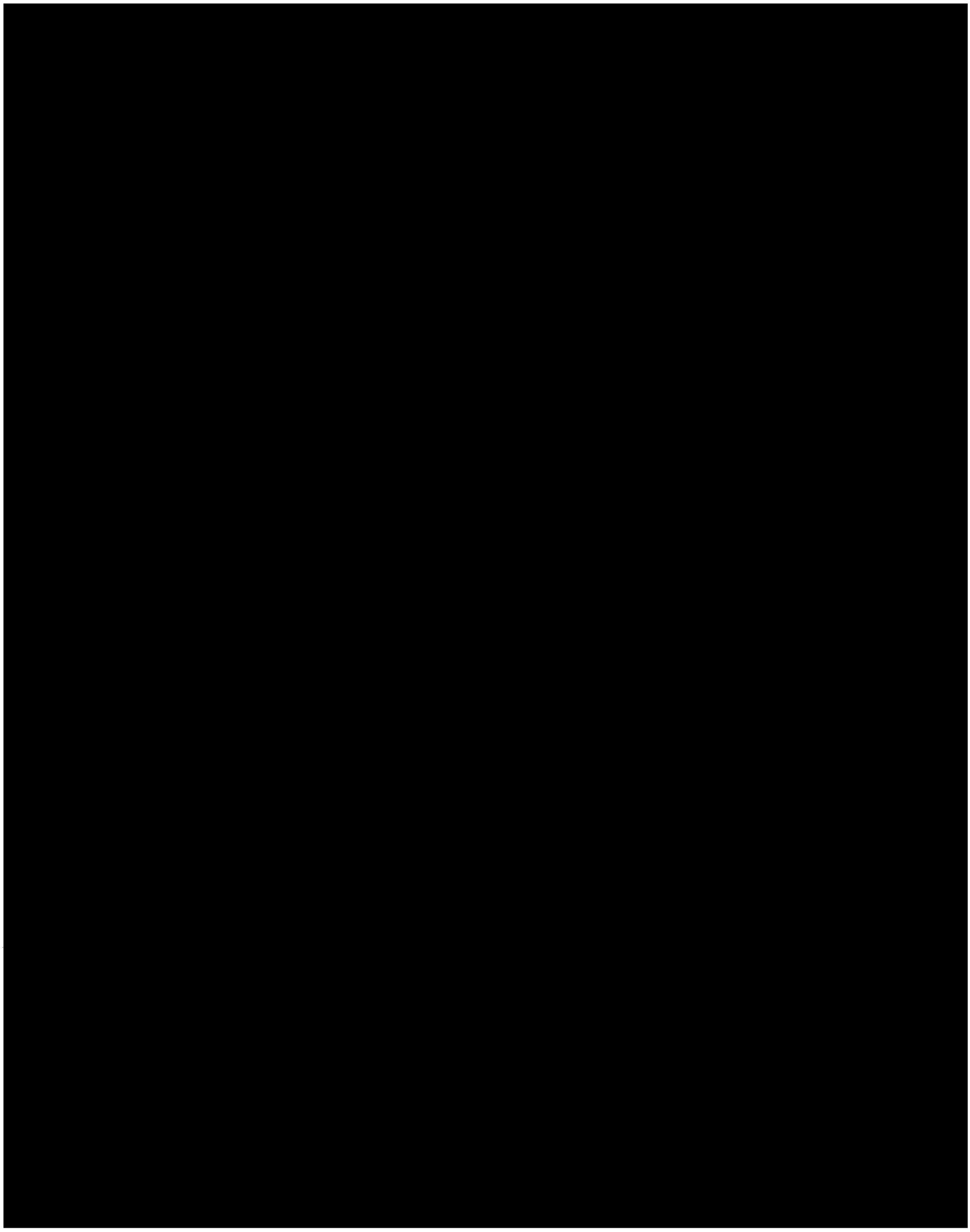
Classification: UNCLASSIFIED

[redacted]

[redacted]

Regards and thanks.

[redacted]



[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Thursday, January 18, 2007 7:20 AM
To: [redacted]
Cc:
Subject: FW: DRAFT Brief (U)

Attachments: NSLs.2.ppt

NSLs.2.ppt (21 KB)

Ref my previous e-mail -- here are the slides.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 17, 2007 7:43 PM
[redacted]
Subject: RE: DRAFT Brief (U)

[redacted]

[redacted]

Just my thoughts. Have a good night.

Cheers,

[redacted]

[redacted]

From: [redacted]
Sent: Wednesday, January 17, 2007 5:39 PM
To: [redacted]
Cc: [redacted]
Subject: DRAFT Brief (U)

Classification: UNCLASSIFIED

[redacted] per our discussion

[redacted] where I am just throwing stuff on a page.

[redacted]

From: [redacted]
Sent: Thursday, January 18, 2007 7:19 AM
To: [redacted]
Cc:
Subject: FW: DRAFT Brief (U)

Importance: High

[redacted] just to let you know this is coming our way. [redacted] is fighting this with [redacted] but I tappears that [redacted] will make the statement to the Hill that CIFA PM will take a look at NSL usage across the services - he is intent on making this happen!! I will send you a copy of the briefing slides separately.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 6:50 AM
To: [redacted]
Cc: [redacted]
Subject: FW: DRAFT Brief (U)

Here is [redacted] reply to our input. I don't know why he included [redacted] on his reply; didn't he depart sometime in Dec to work in the private sector?

Cheers,

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, January 18, 2007 6:19 AM
To: [redacted]
Cc: [redacted]
Subject: RE: DRAFT Brief (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Cheer and thanks.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 17, 2007 7:43 PM
[redacted]
Subject: RE: DRAFT Brief (U)

[redacted]

[redacted]

Just my thoughts. Have a good night.

Cheers,

[redacted]

[redacted]

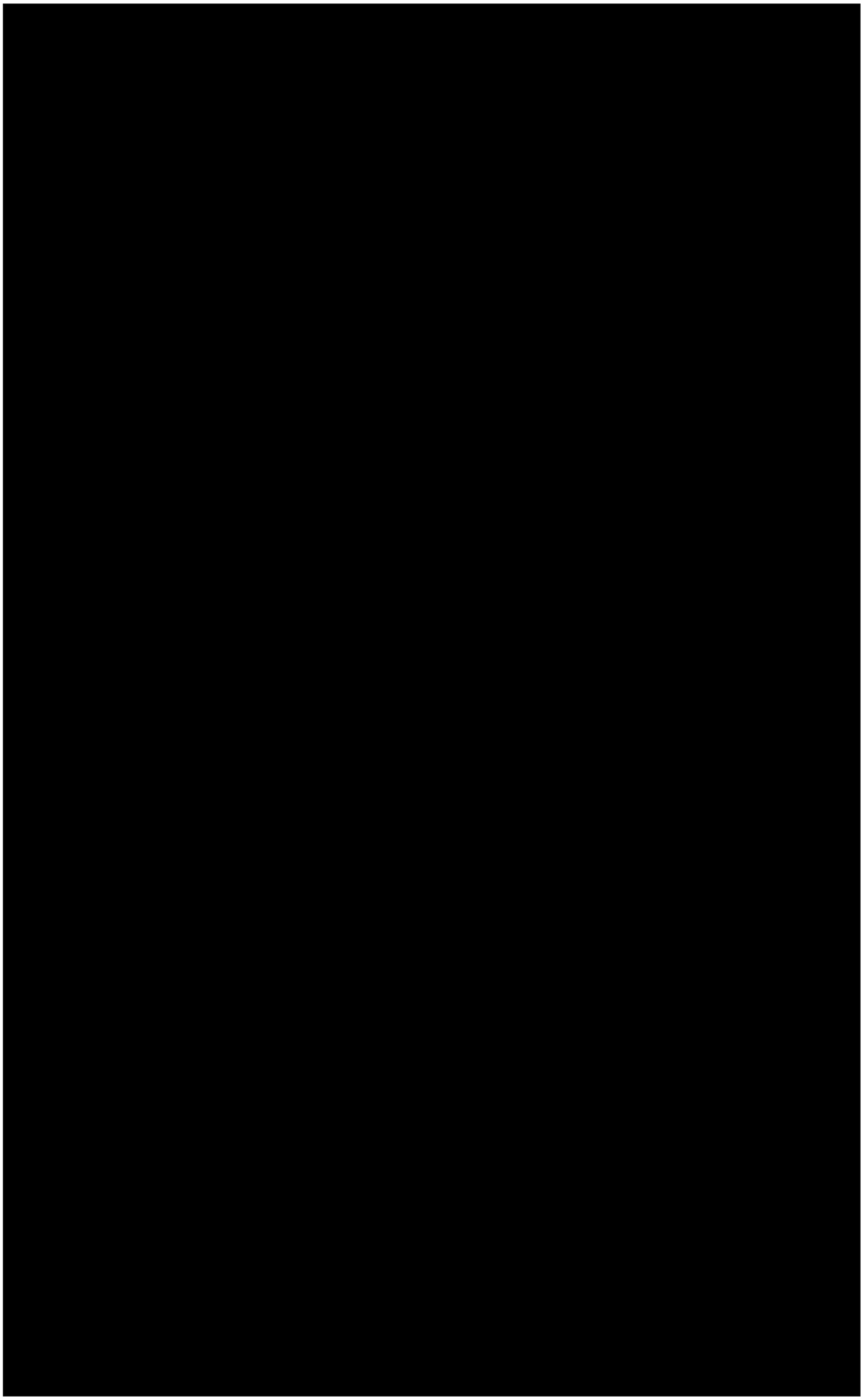
From: [redacted]
Sent: Wednesday, January 17, 2007 5:39 PM
To: [redacted]
Cc:
Subject: DRAFT Brief (U)

Classification: UNCLASSIFIED

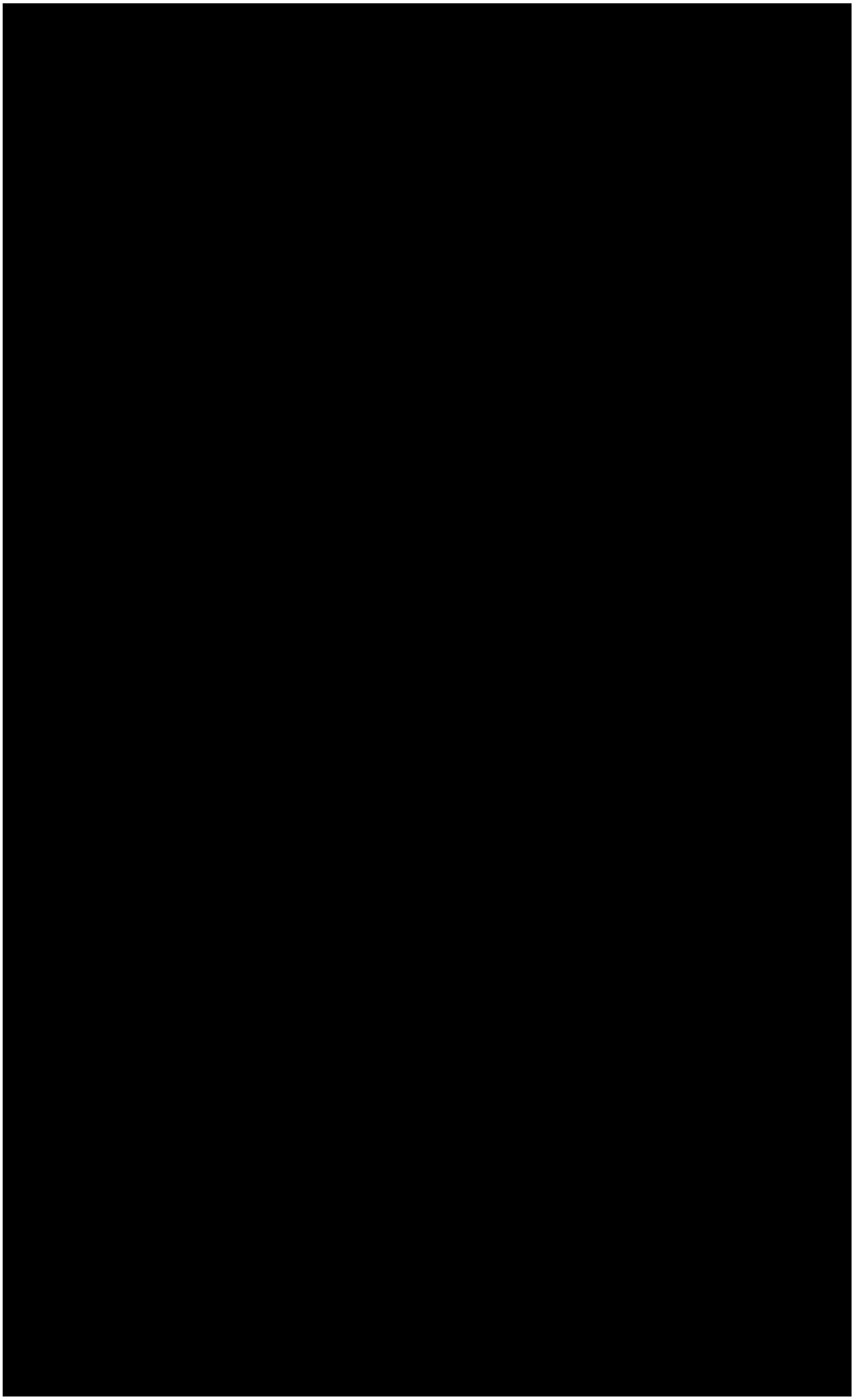
[redacted] per our discussion

[redacted] where I am just throwing stuff on a page.

[redacted]



[redacted]



(1)

[redacted]

From: [redacted]
Sent: Friday, January 19, 2007 12:38
To: [redacted]
Cc:
Subject: RE: Task#: 07-006**S: ASAP 26 Jan** SecDef INFO Memo re NSLs (U)

Attachments: 07-01-19 NSL Info Paper for SecDef (DRAFT) (2).doc

07-01-19 NSL Info Paper for Se...

~~FOR OFFICIAL USE ONLY~~

[redacted] changes made to memo.

-----Original Message-----
From: ODUSD(CI&S)
Sent: Friday, January 19, 2007 11:13 AM
To: [redacted]

Subject: Task#: 07-006**S: ASAP 26 Jan** SecDef INFO Memo re NSLs ~~(FOUO)~~

~~FOR OFFICIAL USE ONLY~~

I'm sorry about sending in this fashion but I have lost the bubble....

Lead: CI Directorate

CORD: ALL

[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

(2)

[redacted]

From: [redacted]
Sent: Monday, March 05, 2007 08:11
To: [redacted]
Cc:
Subject: FW: NSL--SASC Request (U)

Attachments: NSL SASC Reply DUSD Action Memo 070305.doc; SASC Financial Requests 1990-2007 070305.doc

~~FOR OFFICIAL USE ONLY~~

[redacted]

[redacted]

[redacted]

NSL SASC Reply DUSD Action Mem...
SASC Financial Requests 1990-2...

-----Original Message-----
From: [redacted]
Sent: Monday, March 05, 2007 7:48 AM
To: [redacted]
Subject: NSL--SASC Request ~~(FOUO)~~

~~FOR OFFICIAL USE ONLY~~

Draft report, with NCIS corrections, for your review.

V/R,

[redacted]
Deputy Director for
Counterintelligence Policy
USD(I)/CI&S/CI
[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

(3)

[redacted]

From: [redacted]
Sent: Monday, March 12, 2007 12:50
To: [redacted]
Subject: RE: National Security Letters

I'll look at the unclass

[redacted]
Principal Deputy General Counsel
[redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

-----Original Message-----
From: [redacted]
Sent: Monday, March 12, 2007 13:48
To: [redacted]
Subject: RE: National Security Letters

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, March 12, 2007 12:46
To: [redacted]
Cc: [redacted]
Subject: RE: National Security Letters

[redacted]
Principal Deputy General Counsel
[redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

-----Original Message-----
From: [redacted]
Sent: Monday, March 12, 2007 13:25
To: [redacted]
Subject: FW: National Security Letters

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Saturday, March 10, 2007 17:48
To: [redacted]
Subject: Re:

[redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: [redacted]
To: [redacted]
CC: [redacted]
Sent: Sat Mar 10 16:41:37 2007
Subject:

[redacted]

(4)

[redacted]

From: [redacted]
Sent: Saturday, March 10, 2007 17:53
To: [redacted]
Subject: Re:

Tnx

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: [redacted]
To: [redacted]
Sent: Sat Mar 10 17:48:18 2007
Subject: Re:

[redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From [redacted]
To:
CC:
[redacted]
Sent: Sat Mar 10 16:41:37 2007
Subject:

[redacted]

(5)

[redacted]

From: [redacted]
Sent: Wednesday, January 03, 2007 11:10
To: [redacted]
Cc: [redacted]

Subject: RE: USDI Staff Meeting (U)

Thanks, [redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 10:30 AM
To [redacted]
Cc [redacted]
Subject: RE: USDI Staff Meeting (U)

UNCLASSIFIED

Sirs,

[redacted]

V/R

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 8:26 AM
To: [redacted]
Cc: [redacted]
Subject: RE: USDI Staff Meeting (U)

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 8:11 AM
To: [redacted]
Cc: [redacted]
Subject: USDI Staff Meeting (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Thanks,

[redacted]

(6)

[redacted]

From: [redacted]
Sent: Monday, January 15, 2007 12:30
To: [redacted]
Subject: NSL Fact Sheet (v5-12Jan09-1400hrs)

Attachments: NSL Fact Sheet (v5-12Jan09-1400hrs).doc

NSL Fact Sheet
(v5-12Jan09-140...

[redacted]

[redacted]

From: [redacted]
Sent: Tuesday, January 16, 2007 09:54
To: [redacted]
Subject: OGC questions: *Draft* ~~(FOUO)~~
Attachments: DoD NSL Fact Sheet_OGC (16 Jan 07).doc

~~*FOR OFFICIAL USE ONLY*~~

<<DoD NSL Fact Sheet_OGC (16 Jan 07).doc>>

[redacted]
Associate Deputy General Counsel (Intelligence)
DoD OGC - OUSD(I)
[redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process, or other privileges. Information contained in this message may also be exempt from mandatory disclosure under the Freedom of Information Act (FOIA). Do not disseminate further without approval from the Office of the General Counsel, Department of Defense.

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

(8)

[redacted]

From: [redacted]
Sent: Wednesday, January 03, 2007 10:30
To:
Cc: [redacted]

Subject: RE: USDI Staff Meeting (U)

Attachments: NSL chart 50 usc - joint.doc

NSL chart 50 usc - joint.doc ...

UNCLASSIFIED

Sirs,

[redacted]

V/R

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 8:26 AM
To [redacted]
Cc [redacted]
Subject: RE: USDI Staff Meeting (U)

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 8:11 AM
To: [redacted]
Cc: [redacted]
Subject: USDI Staff Meeting (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

Thanks,

[redacted]

(9)

[redacted]

From: [redacted]
Sent: Tuesday, January 16, 2007 07:09
To: [redacted]
Cc:
Subject: RE:

Yes, sir...I'll call [redacted]

[redacted]

[redacted]
General Counsel
Counterintelligence Field Activity
[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, January 16, 2007 7:09 AM
To:
Cc: [redacted]
Subject: Re:

I spoke w [redacted] some. Pls catch up w him. Thanks. [redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: [redacted]
To: [redacted]

Sent: Tue Jan 16 06:58:18 2007
Subject: RE:

[redacted]

It's Tuesday morning and just read your note and listened to your voice message of yesterday....will call your office in a few minutes.

V/R [redacted]

[redacted]

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

From: [redacted]
Sent: Monday, January 15, 2007 11:42 AM
To: [redacted]
Cc:
Subject:

Call me about this right away, pls.

Military Expands Intelligence Role in U.S.
By ERIC LICHTBLAU and MARK MAZZETTI, The New York Times WASHINGTON, Jan. 13 - The Pentagon has been using a little-known power to obtain banking and credit records of hundreds of Americans and others suspected of terrorism or espionage inside the United States, part of an aggressive expansion by the military into domestic intelligence gathering.

The C.I.A. has also been issuing what are known as national security letters to gain access to financial records from American companies, though it has done so only rarely, intelligence officials say.

Banks, credit card companies and other financial institutions receiving the letters usually have turned over documents voluntarily, allowing investigators to examine the financial assets and transactions of American military personnel and civilians, officials say.

The F.B.I., the lead agency on domestic counterterrorism and espionage, has issued thousands of national security letters since the attacks of Sept. 11, 2001, provoking criticism and court challenges from civil liberties advocates who see them as unjustified intrusions into Americans' private lives.

But it was not previously known, even to some senior counterterrorism officials, that the Pentagon and the Central Intelligence Agency have been using their own "noncompulsory" versions of the letters. Congress has rejected several attempts by the two agencies since 2001 for authority to issue mandatory letters, in part because of concerns about the dangers of expanding their role in domestic spying.

The military and the C.I.A. have long been restricted in their domestic intelligence operations, and both are barred from conducting traditional domestic law enforcement work. The C.I.A.'s role within the United States has been largely limited to recruiting people to spy on foreign countries.

Carl Kropf, a spokesman for the director of national intelligence, said intelligence agencies like the C.I.A. used the letters on only a "limited basis."

Pentagon officials defended the letters as valuable tools and said they were part of a broader strategy since the Sept. 11 attacks to use more aggressive intelligence-gathering tactics - a priority of former Defense Secretary Donald H. Rumsfeld. The letters "provide tremendous leads to follow and often with which to corroborate other evidence in the context of counterespionage and counterterrorism," said Maj. Patrick Ryder, a Pentagon spokesman.

Government lawyers say the legal authority for the Pentagon and the C.I.A. to use national security letters in gathering domestic records dates back nearly three decades and, by their reading, was strengthened by the antiterrorism law known as the USA Patriot Act.

Pentagon officials said they used the letters to follow up on a variety of intelligence tips or leads. While they would not provide details about specific cases, military intelligence officials with knowledge of them said the military had issued the letters to collect financial records regarding a government contractor with unexplained wealth, for example, and a chaplain at Guantánamo Bay erroneously suspected of aiding prisoners at the facility.

Usually, the financial documents collected through the letters do not establish any links to espionage or terrorism and have seldom led to criminal charges, military officials say. Instead, the letters often help eliminate suspects.

"We may find out this person has unexplained wealth for reasons that have nothing to do with being a spy, in which case we're out of it," said Thomas A. Gandy, a senior Army counterintelligence official.

But even when the initial suspicions are unproven, the documents have intelligence value, military officials say. In the next year, they plan to incorporate the records into a database at the Counterintelligence Field Activity office at the Pentagon to track possible threats against the military, Pentagon officials said. Like others interviewed, they would speak only on the condition of anonymity.

Military intelligence officers have sent letters in up to 500 investigations over the last five years, two officials estimated. The number of letters is likely to be well into the thousands, the officials said, because a single case often generates letters to multiple financial institutions. For its part, the C.I.A. issues a handful of national security letters each year, agency officials said. Congressional officials said members of the House and Senate Intelligence Committees had been briefed on the use of the letters by the military and the C.I.A.

Some national security experts and civil liberties advocates are troubled by the C.I.A. and military taking on domestic intelligence activities, particularly in light of recent disclosures that the Counterintelligence Field Activity office had maintained files on Iraq war protesters in the United States in violation of the military's own guidelines. Some experts say the Pentagon has adopted an overly expansive view of its domestic role under the guise of "force protection," or efforts to guard military installations.

"There's a strong tradition of not using our military for domestic law enforcement," said Elizabeth Rindskopf Parker, a former general counsel at both the National Security Agency and the C.I.A. who is the dean at the McGeorge School of Law at the University of the Pacific. "They're moving into territory where historically they have not been authorized or presumed to be operating."

Similarly, John Radsan, an assistant general counsel at the C.I.A. from 2002 to 2004 and now a law professor at William Mitchell College of Law in St.
Paul, said, "The C.I.A. is not supposed to have any law enforcement powers, or internal security functions, so if they've been issuing their own national security letters, they better be able to explain how they don't cross the line."

The Pentagon's expanded intelligence-gathering role, in particular, has created occasional conflicts with other federal agencies. Pentagon efforts to post American military officers at embassies overseas to gather intelligence for counterterrorism operations or future war plans has rankled some State Department and C.I.A. officials, who see the military teams as duplicating and potentially interfering with the intelligence agency.

In the United States, the Federal Bureau of Investigation has complained about military officials dealing directly with local police - rather than through the bureau - for assistance in responding to possible terrorist threats against a military base. F.B.I. officials say the threats have often turned out to be uncorroborated and, at times, have stirred needless anxiety.

The military's frequent use of national security letters has sometimes caused concerns from the businesses receiving them, a counterterrorism official said. Lawyers at financial institutions, which routinely provide records to the F.B.I. in law enforcement investigations, have contacted bureau officials to say they were confused by the scope of the military's requests and whether they were obligated to turn the records over, the official said.

Companies are not eager to turn over sensitive financial data about customers to the government, the official said, "so the more this is done, and the more poorly it's done, the more pushback there is for the F.B.I."

The bureau has frequently relied on the letters in recent years to gather telephone and Internet logs, financial information and other records in terrorism investigations, serving more than 9,000 letters in 2005, according to a Justice Department tally. As an investigative tool, the letters present relatively few hurdles; they can be authorized by supervisors rather than a court. Passage of the Patriot Act in October 2001 lowered the standard for issuing the letters, requiring only that the documents sought be "relevant" to an investigation and allowing records requests for more peripheral figures, not just

targets of an inquiry.

Some Democrats have accused the F.B.I. of using the letters for fishing expeditions, and the American Civil Liberties Union won court challenges in two cases, one for library records in Connecticut and the other for Internet records in Manhattan. Concerned about possible abuses, Congress imposed new safeguards in extending the Patriot Act last year, in part by making clear that recipients of national security letters could contact a lawyer and seek court review. Congress also directed the Justice Department inspector general to study the F.B.I.'s use of the letters, a review that is continuing.

Unlike the F.B.I., the military and the C.I.A. do not have wide-ranging authority to seek records on Americans in intelligence investigations. But the expanded use of national security letters has allowed the Pentagon and the intelligence agency to collect records on their own. Sometimes, military or C.I.A. officials work with the F.B.I. to seek records, as occurred with an American translator who had worked for the military in Iraq and was suspected of having ties to insurgents.

After the Sept. 11 attacks, Mr. Rumsfeld directed military lawyers and intelligence officials to examine their legal authorities to collect intelligence both inside the United States and abroad. They concluded that the Pentagon had "way more" legal tools than it had been using, a senior Defense Department official said.

Military officials say the Right to Financial Privacy Act of 1978, which establishes procedures for government access to sensitive banking data, first authorized them to issue national security letters. The military had used the letters sporadically for years, officials say, but the pace accelerated in late 2001, when lawyers and intelligence officials concluded that the Patriot Act strengthened their ability to use the letters to seek financial records on a voluntary basis and to issue mandatory letters to obtain credit ratings, the officials said.

The Patriot Act does not specifically mention military intelligence or C.I.A. officials in connection with the national security letters.

Some F.B.I. officials said they were surprised by the Pentagon's interpretation of the law when military officials first informed them of it.
"It was a very broad reading of the law," a former counterterrorism official said.

While the letters typically have been used to trace the financial transactions of military personnel, they also have been used to investigate civilian contractors and people with no military ties who may pose a threat to the military, officials said. Military officials say they regard the letters as one of the least intrusive means to gather evidence. When a full investigation is opened, one official said, it has now become "standard practice" to issue such letters.

One prominent case in which letters were used to obtain financial records, according to two military officials, was that of a Muslim chaplain at Guantánamo Bay, Cuba, who was suspected in 2003 of aiding terror suspects imprisoned at the facility. The espionage case against the chaplain, James J. Yee, soon collapsed.

Eugene Fidell, a defense lawyer for the former chaplain and a military law expert, said he was unaware that military investigators may have used national security letters to obtain financial information about Mr. Yee, nor was he aware that the military had ever claimed the authority to issue the letters.

Mr. Fidell said he found the practice "disturbing," in part because the military does not have the same checks and balances when it comes to Americans' civil rights as does the F.B.I. "Where is the accountability?" he asked. "That's the evil of it - it doesn't leave fingerprints."

Even when a case is closed, military officials said they generally maintain the records for years because they may be relevant to future intelligence inquiries. Officials at the Pentagon's counterintelligence unit say they plan to incorporate those records into a database, called Portico, on intelligence leads. The financial documents will not be widely disseminated, but limited to investigators, an intelligence official said.

"You don't want to destroy something only to find out that the same guy comes up in another report and you don't know that he was investigated before," the official said.

The Counterintelligence Field Activity office, created in 2002 to better coordinate the military's efforts to combat foreign intelligence services, has drawn criticism for some domestic intelligence activities.

The agency houses an antiterrorist database of intelligence tips and threat reports, known as Talon, which had been collecting information on antiwar planning meetings at churches, libraries and other locations. The Defense Department has since tightened its procedures for what kind of information is allowed into the Talon database, and the counterintelligence office also purged more than 250 incident reports from the database that officials determined should never have been included because they centered on lawful political protests by people opposed to the war in Iraq.

FROM FOX NEWS SUNDAY YESTERDAY:

WALLACE: There's a report in the New York Times today that's been confirmed by administration officials that the Pentagon and the CIA have been obtaining financial records about hundreds of Americans suspected of involvement in either terrorism or espionage.

Why involve the CIA and the Pentagon in domestic intelligence- gathering?

CHENEY: Well, remember what these issues are. This is a question, as I understand it, of issuing national security letters that allow us to collect financial information, for example, on suspected -- or, on people we have reason to suspect.

The Defense Department gets involved because we've got hundreds of bases inside the United States that are potential terrorist targets. We've got hundreds of thousands of people, innocent Americans...

WALLACE: But why not let the FBI do that, sir?

CHENEY: Well, they can do a certain amount of it, and they do.

But the Department of Defense has legitimate authority in this area. This is an authority that goes back three or four decades. It was reaffirmed in the Patriot Act that was renewed here about a year or so ago.

It's a perfectly legitimate activity. There's nothing wrong with it or illegal. It doesn't violate people's civil rights. And if an institution that receives one of these national security letters disagrees with it, they're free to go to court to try to stop its execution.

So, you know, this is a dramatic story, but I think it's important for people to understand here this is a legitimate security effort that's been under way for a long time, and it does not represent a new departure from the standpoint of our efforts to protect ourselves against terrorist attacks.

(10)

[redacted]

From: [redacted]
Sent: Wednesday, January 03, 2007 13:19
To: [redacted]
Cc:

Subject: RE: USDI Staff Meeting (U)

Responding for CIFA OGC, I like this matrix more than the one we had in our files. Much easier to understand and captures all the relevant possibilities. Thanks [redacted]

[redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 10:30 AM
To: [redacted]
Cc: [redacted]
Subject: RE: USDI Staff Meeting (U)

UNCLASSIFIED

Sirs,

[redacted]

V/R

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 8:26 AM
To: [redacted]
Cc: [redacted]
Subject: RE: USDI Staff Meeting (U)

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 03, 2007 8:11 AM

To: [redacted]
Cc: [redacted]
[redacted]
Subject: USDI Staff Meeting (U)

Classification: UNCLASSIFIED

[redacted]

[redacted]

From: [redacted]
Sent: Friday, January 19, 2007 11:13
To: [redacted]
Cc:
Subject: Task#: 07-006**S: ASAP 26 Jan** SecDef INFO Memo re NSLs ~~(FOUO)~~
Attachments: Task#: 07-006**S: ASAP 26 Jan** SecDef INFO Memo re NSLs

~~*FOR OFFICIAL USE ONLY*~~

I'm sorry about sending in this fashion but I have lost the bubble….

Lead: CI Directorate

CORD: ALL

[redacted]

<<Task#: 07-006**S: ASAP 26 Jan** SecDef INFO Memo re NSLs>>

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

(14)

From: [redacted]
Sent: Tuesday, January 16, 2007 10:07 AM
To: [redacted]
Subject: Fw: OGC questions: *Draft* ~~(FOUO)~~

Attachments: DoD NSL Fact Sheet_OGC (16 Jan 07).doc

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: [redacted]
To: [redacted]
Sent: Tue Jan 16 09:53:39 2007
Subject: OGC questions: *Draft* ~~(FOUO)~~

~~FOR OFFICIAL USE ONLY~~

<<DoD NSL Fact Sheet_OGC (16 Jan 07).doc>>

[redacted]

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process, or other privileges. Information contained in this message may also be exempt from mandatory disclosure under the Freedom of Information Act (FOIA). Do not disseminate further without approval from the Office of the General Counsel, Department of Defense.

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

15

From: [redacted]
Sent: Monday, March 12, 2007 6:42 AM
To: [redacted]

Subject: EM Notes 3.12.07 ~~(FOUO)~~

Attachments: EM Notes 03.12.07.doc

~~FOR OFFICIAL USE ONLY~~

[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

(16)

From: [redacted]
Sent: Sunday, January 14, 2007 10:16 AM
To: [redacted]
Subject: Re: NYT Article

VP Cheney was asked about it by Chris Wallace on Fox News Sunday. VP response was in line with the fact sheet.
[redacted]

-----Original Message-----
From: [redacted]
To: [redacted]
Sent: Sat Jan 13 16:36:22 2007
Subject: Fw: NYT Article

All - NY Times has posted their article on the web. FYSA, Mr Whitman, DASD for Media Ops, has already received a query from the Washington Post and used the fact sheet to respond. Therefore, I'd also expect an article in the Post tomorrow.

V/R
[redacted]

-----Original Message-----
From: [redacted]
To: [redacted]
Sent: Sat Jan 13 14:59:50 2007
Subject: NYT Article

January 14, 2007

Military Expands Domestic Surveillance

By ERIC LICHTBLAU <http://topics.nytimes.com/top/reference/timestopics/people/l/eric_lichtblau/index.html?inline=nyt-per> and MARK MAZZETTI <http://topics.nytimes.com/top/reference/timestopics/people/m/mark_mazzetti/index.html?inline=nyt-per>

WASHINGTON, Jan. 13 — The Pentagon has been using a little-known power to obtain banking and credit records of hundreds of Americans and others suspected of terrorism or espionage inside the United States, part of an aggressive expansion by the military into domestic intelligence gathering.

The C.I.A. <http://topics.nytimes.com/top/reference/timestopics/organizations/c/central_intelligence_agency/index.html?inline=nyt-org> has also been issuing what are known as national security letters to gain access to financial records from American companies, though it has done so only rarely, intelligence officials say.

Banks, credit card companies and other financial institutions receiving the letters usually have turned over documents voluntarily, allowing investigators to examine the financial assets and transactions of American military personnel and civilians, officials say.

The F.B.I. <http://topics.nytimes.com/top/reference/timestopics/organizations/f/federal_bureau_of_investigation/index.html?inline=nyt-org> , the lead agency on domestic counterterrorism and espionage, has issued thousands of national security letters since the attacks of Sept. 11, 2001, provoking criticism and court challenges from civil liberties advocates who see them as unjustified intrusions into Americans' private lives.

But it was not previously known, even to some senior counterterrorism officials, that the Pentagon and the Central Intelligence Agency have been using their own "noncompulsory" versions of the letters. Congress has rejected several attempts by the two agencies since 2001 for authority to issue mandatory letters, in part because of concerns about the dangers of expanding their role in domestic spying.

The military and the C.I.A. have long been restricted in their domestic intelligence operations, and both are barred from conducting traditional domestic law enforcement work. The C.I.A.'s role within the United States has been largely limited to recruiting people to spy on foreign countries.

Carl Kropf, a spokesman for the director of national intelligence, said intelligence agencies like the C.I.A. used the letters on only a "limited basis."

Pentagon officials defended the letters as valuable tools and said they were part of a broader strategy since the Sept. 11 attacks to use more aggressive intelligence-gathering tactics — a priority of former Defense Secretary Donald H. Rumsfeld <http://topics.nytimes.com/top/reference/timestopics/people/r/donald_h_rumsfeld/index.html?inline=nyt-per> . The letters "provide tremendous leads to follow and often with which to corroborate other evidence in the context of counterespionage and counterterrorism," said Maj. Patrick Ryder, a Pentagon spokesman.

Government lawyers say the legal authority for the Pentagon and the C.I.A. to use national security letters in gathering domestic records dates back nearly three decades and, by their reading, was strengthened by the antiterrorism law known as the USA Patriot Act.

Pentagon officials said they used the letters to follow up on a variety of intelligence tips or leads. While they would not provide details about specific cases, military intelligence officials with knowledge of them said the military had issued the letters to collect financial records regarding a government contractor with unexplained wealth, for example, and a chaplain at Guantánamo Bay erroneously suspected of aiding prisoners at the facility.

Usually, the financial documents collected through the letters do not establish any links to espionage or terrorism and have seldom led to criminal charges, military officials say. Instead, the letters often help eliminate suspects.

"We may find out this person has unexplained wealth for reasons that have nothing to do with being a spy, in which case we're out of it," said Thomas A. Gandy, a senior Army counterintelligence official.

But even when the initial suspicions are unproven, the documents have intelligence value, military officials say. In the next year, they plan to incorporate the records into a database at the Counterintelligence Field Activity office at the Pentagon to track possible threats against the military, Pentagon officials said. Like others interviewed, they would speak only on the condition of anonymity.

Military intelligence officers have sent letters in up to 500 investigations over the last five years, two officials estimated. The number of letters is likely to be well into the thousands, the officials said, because a single case often generates letters to multiple financial institutions. For its part, the C.I.A. issues a handful of national security letters each year, agency officials said. Congressional officials said members of the House and Senate Intelligence Committees had been briefed on the use of the letters by the military and the C.I.A.

Some national security experts and civil liberties advocates are troubled by the C.I.A. and military taking on

domestic intelligence activities, particularly in light of recent disclosures that the Counterintelligence Field Activity office had maintained files on Iraq war protesters in the United States in violation of the military's own guidelines. Some experts say the Pentagon has adopted an overly expansive view of its domestic role under the guise of "force protection," or efforts to guard military installations.

"There's a strong tradition of not using our military for domestic law enforcement," said Elizabeth Rindskopf Parker, a former general counsel at both the National Security Agency <http://topics.nytimes.com/top/reference/timestopics/organizations/n/national_security_agency/index.html?inline=nyt-org> and the C.I.A. who is the dean at the McGeorge School of Law at the University of the Pacific. "They're moving into territory where historically they have not been authorized or presumed to be operating."

Similarly, John Radsan, an assistant general counsel at the C.I.A. from 2002 to 2004 and now a law professor at William Mitchell College of Law in St. Paul, said, "The C.I.A. is not supposed to have any law enforcement powers, or internal security functions, so if they've been issuing their own national security letters, they better be able to explain how they don't cross the line."

The Pentagon's expanded intelligence-gathering role, in particular, has created occasional conflicts with other federal agencies. Pentagon efforts to post American military officers at embassies overseas to gather intelligence for counterterrorism operations or future war plans has rankled some State Department and C.I.A. officials, who see the military teams as duplicating and potentially interfering with the intelligence agency.

In the United States, the Federal Bureau of Investigation has complained about military officials dealing directly with local police — rather than through the bureau — for assistance in responding to possible terrorist threats against a military base. F.B.I. officials say the threats have often turned out to be uncorroborated and, at times, have stirred needless anxiety.

The military's frequent use of national security letters has sometimes caused concerns from the businesses receiving them, a counterterrorism official said. Lawyers at financial institutions, which routinely provide records to the F.B.I. in law enforcement investigations, have contacted bureau officials to say they were confused by the scope of the military's requests and whether they were obligated to turn the records over, the official said.

Companies are not eager to turn over sensitive financial data about customers to the government, the official said, "so the more this is done, and the more poorly it's done, the more pushback there is for the F.B.I."

The bureau has frequently relied on the letters in recent years to gather telephone and Internet logs, financial information and other records in terrorism investigations, serving more than 9,000 letters in 2005, according to a Justice Department tally. As an investigative tool, the letters present relatively few hurdles; they can be authorized by supervisors rather than a court. Passage of the Patriot Act in October 2001 lowered the standard for issuing the letters, requiring only that the documents sought be "relevant" to an investigation and allowing records requests for more peripheral figures, not just targets of an inquiry.

Some Democrats <http://topics.nytimes.com/top/reference/timestopics/organizations/d/democratic_party/index.html?inline=nyt-org> have accused the F.B.I. of using the letters for fishing expeditions, and the American Civil Liberties Union <http://topics.nytimes.com/top/reference/timestopics/organizations/a/american_civil_liberties_union/index.html?inline=nyt-org> won court challenges in two cases, one for library records in Connecticut and the other for Internet records in Manhattan. Concerned about possible abuses, Congress imposed new safeguards in extending the Patriot Act last year, in part by making clear that recipients of national security letters could contact a lawyer and seek court review. Congress also directed the Justice Department inspector general to study the F.B.I.'s use of the letters, a review that is continuing.

Unlike the F.B.I., the military and the C.I.A. do not have wide-ranging authority to seek records on Americans in intelligence investigations. But the expanded use of national security letters has allowed the Pentagon and the intelligence agency to collect records on their own. Sometimes, military or C.I.A. officials work with the F.B.I. to seek records, as occurred with an American translator who had worked for the military in Iraq and was suspected of having ties to insurgents.

After the Sept. 11 attacks, Mr. Rumsfeld directed military lawyers and intelligence officials to examine their legal authorities to collect intelligence both inside the United States and abroad. They concluded that the Pentagon had "way more" legal tools than it had been using, a senior Defense Department official said.

Military officials say the Right to Financial Privacy Act of 1978, which establishes procedures for government access to sensitive banking data, first authorized them to issue national security letters. The military had used the letters sporadically for years, officials say, but the pace accelerated in late 2001, when lawyers and intelligence officials concluded that the Patriot Act strengthened their ability to use the letters to seek financial records on a voluntary basis and to issue mandatory letters to obtain credit ratings, the officials said.

The Patriot Act does not specifically mention military intelligence or C.I.A. officials in connection with the national security letters.

Some F.B.I. officials said they were surprised by the Pentagon's interpretation of the law when military officials first informed them of it. "It was a very broad reading of the law," a former counterterrorism official said.

While the letters typically have been used to trace the financial transactions of military personnel, they also have been used to investigate civilian contractors and people with no military ties who may pose a threat to the military, officials said. Military officials say they regard the letters as one of the least intrusive means to gather evidence. When a full investigation is opened, one official said, it has now become "standard practice" to issue such letters.

One prominent case in which letters were used to obtain financial records, according to two military officials, was that of a Muslim chaplain at Guantánamo Bay, Cuba, who was suspected in 2003 of aiding terror suspects imprisoned at the facility. The espionage case against the chaplain, James J. Yee, soon collapsed, and he was eventually convicted on lesser charges of adultery and downloading pornography.

Eugene Fidell, a defense lawyer for the former chaplain and a military law expert, said he was unaware that military investigators may have used national security letters to obtain financial information about Mr. Yee, nor was he aware that the military had ever claimed the authority to issue the letters.

Mr. Fidell said he found the practice "disturbing," in part because the military does not have the same checks and balances when it comes to Americans' civil rights as does the F.B.I. "Where is the accountability?" he asked. "That's the evil of it — it doesn't leave fingerprints."

Even when a case is closed, military officials said they generally maintain the records for years because they may be relevant to future intelligence inquiries. Officials at the Pentagon's counterintelligence unit say they plan to incorporate those records into a database, called Portico, on intelligence leads. The financial documents will not be widely disseminated, but limited to investigators, an intelligence official said.

"You don't want to destroy something only to find out that the same guy comes up in another report and you don't know that he was investigated before," the official said.

The Counterintelligence Field Activity office, created in 2002 to better coordinate the military's efforts to combat foreign intelligence services, has drawn criticism for some domestic intelligence activities.

The agency houses an antiterrorist database of intelligence tips and threat reports, known as Talon, which had been collecting information on antiwar planning meetings at churches, libraries and other locations. The Defense Department has since tightened its procedures for what kind of information is allowed into the Talon database, and the counterintelligence office also purged more than 250 incident reports from the database that officials determined should never have been included because they centered on lawful political protests by people opposed to the war in Iraq.

Copyright 2007 <http://www.nytimes.com/ref/membercenter/help/copyright.html> The New York Times Company <http://www.nytco.com/>

(17)

From: [redacted]
Sent: Wednesday, January 17, 2007 3:03 PM
To: [redacted]
Subject: FW: CIFA Memo (U)

Attachments: Post Article re TALON.doc; TALON-ACLU.pdf

UNCLASSIFIED

The original Post article is also attached.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 17, 2007 2:22 PM
To: [redacted]
[redacted]
Subject: CIFA Memo (U)

UNCLASSIFIED
FYI.
The memo referenced in the Pincus article.
V/R,
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, January 17, 2007 2:17 PM
To [redacted]
Cc [redacted]
Subject: RE: SSCI Request for NSL Briefing ~~(FOUO)~~

Sorry, here we go.

[redacted]
Director of Communications
Counterintelligence Field Activity
[redacted]

Washington Post
January 17, 2007
Pg. 8

Protesters Found In Database

ACLU Is Questioning Entries in Defense Dept. System

By Walter Pincus, Washington Post Staff Writer

A Defense Department database devoted to gathering information on potential threats to military facilities and personnel, known as Talon, had 13,000 entries as of a year ago -- including 2,821 reports involving American citizens, according to an internal Pentagon memo to be released today by the American Civil Liberties Union.

The Pentagon memo says an examination of the system led to the deletion of 1,131 reports involving Americans, 186 of which dealt with "anti-military protests or demonstrations in the U.S."

Titled "Review of the TALON Reporting System," the four-page memo produced in February 2006 summarizes some interim results from an inquiry ordered by then-Defense Secretary Donald H. Rumsfeld after disclosure in December 2005 that the system had collected and circulated data on anti-military protests and other peaceful demonstrations.

The released memo, one of a series of Talon documents made public over the past year by the ACLU under a Freedom of Information Act lawsuit, said that the deleted reports did not meet a 2003 Defense Department requirement that they have some foreign terrorist connection or relate to what was believed to be "a force protection threat."

The number of deleted reports far exceeds the estimate provided to The Washington Post just over a year ago by senior officials of Counterintelligence Field Activity (CIFA), the Defense Department agency that manages the Talon program. At that time, then-CIFA Director David A. Burtt II said the review had disclosed that only 1 percent of the then 12,500 Talon reports appeared to be problematic.

The ACLU said in its own report that past disclosures about Talon "cried out for congressional oversight yet Congress was silent." It said the new memo indicated there "may be even more disturbing" information to discover and declared "it is time for Congress to act."

The ACLU noted the memo showed that Talon reports had a much wider circulation than previously disclosed, with about 28 organizations and 3,589 individuals authorized to submit reports or have access to the database. The organizations with access include various military agencies as well as state, federal and local law enforcement officials.

In early 2006, Burtt also said CIFA had not devised a formal way to notify its users when it decided to delete a Talon report on American citizens. The newly released memo says that a software enhancement was being initiated to permit users to edit and delete entries from the database and that it was scheduled for completion in April 2006.

A Pentagon spokesman said there are 7,700 reports in the Talon database. Some involve U.S. citizens, but the spokesman declined to say how many. Over the past year the program has instituted multiple layers of review for screening which reports should go into the database, the spokesman said.

CIFA has begun a process for analysts to review materials to make sure they fit the program's criteria before being uploaded and made available to Talon users. CIFA was established in 2002 in the aftermath of the Sept. 11, 2001, terrorist attacks, originally to coordinate the counterterrorism and counterintelligence operations of the various branches and agencies of the Defense Department. It has grown rapidly over the past four years, but not without problems. Along with discovery of the Talon data collection, CIFA was linked to the lobbying and earmarking activities that led to the conviction of former congressman Randy "Duke" Cunningham (R-Calif.). Burtt and his top deputy retired in August 2006, and federal investigators are still looking at CIFA contracting activities.

Last week, the New York Times disclosed that CIFA had been using national security letters to gather financial data on U.S. citizens, but a Pentagon spokesman said yesterday that such information was for particular investigations and not made part of the Talon database.

Talon was started in May 2003 to capture raw, non-validated information about suspicious activity or potential terrorist threats to military personnel or facilities at home and abroad.

~~FOR OFFICIAL USE ONLY~~

[redacted]

From: [redacted]
Sent: Thursday, February 08, 2007 4:14 PM
To: [redacted]
Cc:
Subject: RE: Murderboard Prep for [redacted] testimony tomorrow ~~(FOUO)~~

Attachments: NSL.doc

~~*FOR OFFICIAL USE ONLY*~~

Minor edits. Apologize for the delay. Just saw it.

[redacted]

NSL.doc (28 KB)

From: [redacted]
Sent: Thursday, February 08, 2007 11:08 AM
To: [redacted]
Cc:
Subject: RE: Murderboard Prep for [redacted] testimony tomorrow ~~(FOUO)~~

~~*FOR OFFICIAL USE ONLY*~~

UNCLASSIFIED//~~FOUO~~

[redacted]

Can you give me a sanity check?

Thx, [redacted]

My Recommendations appear in Blue:

[redacted]

[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

[redacted]

RE Murderboard Prep for [redacted] testimony tomorrow ~~(FOUO)~~

From: [redacted]
Sent: Thursday, February 08, 2007 4:14 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Murderboard Prep for [redacted] testimony tomorrow ~~(FOUO)~~
~~FOR OFFICIAL USE ONLY~~

Minor edits. Apologize for the delay. Just saw it.

[redacted]

From: [redacted]
Sent: Thursday, February 08, 2007 11:08 AM
To: [redacted]
Cc: [redacted]
Subject: RE: Murderboard Prep for [redacted] testimony tomorrow ~~(FOUO)~~

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOUO~~

[redacted]

Can you give me a sanity check?

Thx, [redacted]

[redacted]

RE Murderboard Prep for [redacted] testimony tomorrow ~~(FOUO)~~
governing DoD use of the NSL.

** NSL Q&As from the Hill visits and statute info paper provided.

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

Department of Defense

DIRECTIVE

NUMBER 5400.12
December 2, 2004

DA&M

SUBJECT: Obtaining Information from Financial Institutions

References: (a) DoD Directive 5400.12, subject as above, February 6, 1980 (hereby canceled)
(b) Chapter 35 of title 12, United States Code, "Right to Financial Privacy Act of 1978"
(c) DoD Instruction 5400.15, "Guidance on Obtaining Information from Financial Institutions,"

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policies and responsibilities for obtaining access to financial records maintained by financial institutions.

1.2. Implements references (b) and (c) by providing guidance on the requirements and conditions for obtaining financial records.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Applies only to financial records maintained by financial institutions.

3. DEFINITIONS

Terms used in this Directive are defined in DoD Instruction 5400.aa (reference (c)).

4. POLICY

It is DoD policy that:

4.1. Authorization of the customer to whom the financial records pertain shall be sought unless doing so compromises or harmfully delays either a legitimate law enforcement inquiry or a lawful intelligence activity. If the person declines to consent to disclosure, the alternative means of obtaining the records authorized by reference (c) shall be utilized.

4.2. The provisions of reference (b) do not govern obtaining access to financial records maintained by military banking contractors located outside the United States, the District of Columbia, Guam, American Samoa, Puerto Rico, and the Virgin Islands. The guidance set forth in enclosure 16 of reference (c) may be used to obtain financial information from these contractor-operated facilities.

5. RESPONSIBILITIES

5.1. The Director of Administration and Management, Office of the Secretary of Defense, shall:

5.1.1. Exercise oversight to ensure compliance with this Directive.

5.1.2. Provide policy guidance to the affected DoD Components to implement this Directive.

5.2. The Secretaries of the Military Departments and the Heads of the affected DoD Components shall:

5.2.1. Implement policies and procedures to ensure implementation of this Directive and reference (b) when seeking access to financial records.

5.2.2. Adhere to the guidance and procedures contained in reference (c).

6. **EFFECTIVE DATE**

This Directive is effective immediately.

Paul Wolfowitz
Deputy Secretary of Defense

Department of Defense

INSTRUCTION

NUMBER 5400.15
December 2, 2004

DA&M

SUBJECT: Guidance on Obtaining Information from Financial Institutions

References: (a) DoD Directive 5400.12, "Obtaining Information From Financial Institutions," December 2, 2004
(b) Chapter 35 of title 12, United States Code, "Right to Financial Privacy Act of 1978"
(c) Chapter 16 of title 12, United States Code, "Federal Deposit Insurance Act"
(d) Chapter 29 of title 25, United States Code, "Indian Gaming Regulatory Act"
(e) through (m), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Implements policy and assigns responsibilities under reference (a).

1.2. Implements reference (b) and prescribes procedures for obtaining access to financial records maintained by financial institutions.

2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Applies only to financial records maintained by financial institutions.

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Authorization of the customer to whom the financial records pertain shall be sought unless doing so compromises or harmfully delays either a legitimate law enforcement inquiry or a lawful intelligence activity. If the person declines to consent to disclosure, the alternative means of obtaining the records authorized by this Instruction shall be utilized.

4.2. The provisions of reference (b) do not govern obtaining access to financial records maintained by military banking contractors located outside the United States, the District of Columbia, Guam, American Samoa, Puerto Rico, and the Virgin Islands. The guidance set forth in enclosure 16 may be used to obtain financial information from these contractor operated facilities.

5. RESPONSIBILITIES

5.1. The Director of Administration and Management, Office of the Secretary of Defense shall:

5.1.1. Exercise oversight to ensure compliance with this Instruction.

5.1.2. Provide policy guidance to affected DoD Components to implement this Instruction.

5.2. The Secretaries of the Military Departments and the Heads of the affected DoD Components shall implement policies and procedures to ensure implementation of this Instruction and references (a) and (b) when seeking access to financial records.

6. EFFECTIVE DATE

This Instruction is effective immediately.

Raymond F. DuBois
Director,
Washington Headquarters Services

Enclosures – 16

E1. References, continued
E2. Definitions
E3. Obtaining Basic Identifying Account Information
E4. Obtaining Customer Authorization
E5. Obtaining Access by Administrative or Judicial Subpoena or by a Formal Written Request
E6. Obtaining Access by Search Warrant
E7. Obtaining Access for Foreign Intelligence, Foreign Counterintelligence, and International Terrorist Activities or Investigations
E8. Obtaining Emergency Access
E9. Releasing Information Obtained from Financial Institutions
E10. Procedures for Delay of Notice
E11. Format for Obtaining Basic Identifying Account Information
E12. Format for Customer Authorization
E13. Format for a Formal Written Request
E14. Format for Customer Notice for Administrative or Judicial Subpoena or for Formal Written Request
E15. Format for Certificate of Compliance with the Right to Financial Privacy Act of 1978
E16. Obtaining Access to Financial Records Overseas

E1. ENCLOSURE 1

REFERENCES, continued

(e) Chapter 1 of title 7, United States Code, "Commodity Exchange Act"
(f) DoD Directive 5400.11, "DoD Privacy Program," December 13, 1999
(g) Appendix 3 of title 5, United States Code, Inspector General Act of 1978"
(h) Rule 41 of the Federal Rules of Criminal Procedure
(i) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988
(j) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(k) Manual for Courts-Martial, United States, 2002
(l) Chapter 47 of title 10, United States Code, "Uniform Code of Military Justice"
(m) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1992

E2. ENCLOSURE 2

DEFINITIONS

E2.1. TERMS

Terms used in reference (a) and this Instruction are defined as follows:

E2.1.1. Administrative Summons or Subpoena. A statutory writ issued by a Government Authority.

E2.1.2. Customer. Any person or authorized representative of that person who used or is using any service of a financial institution or for whom a financial institution is acting or has acted as fiduciary for an account maintained in the name of that person.

E2.1.3. Financial Institution (for intelligence activity purposes only).

E2.1.3.1. An insured bank (includes a foreign bank having an insured branch) whose deposits are insured under the Federal Deposit Insurance Act (reference (c)).

E2.1.3.2. A commercial bank or trust company.

E2.1.3.3. A private banker.

E2.1.3.4. An agency or branch of a foreign bank in the United States.

E2.1.3.5. Any credit union.

E2.1.3.6. A thrift institution.

E2.1.3.7. A broker or dealer registered with the Securities and Exchange Commission.

E2.1.3.8. A broker or dealer in securities or commodities.

E2.1.3.9. An investment banker or investment company.

E2.1.3.10. A currency exchange.

E2.1.3.11. An issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments.

E2.1.3.12. An operator of a credit card system.

E2.1.3.13. An insurance company.

E2.1.3.14. A dealer in precious metals, stones, or jewels.

E2.1.3.15. A pawnbroker.

E2.1.3.16. A loan or finance company.

E2.1.3.17. A travel agency.

E2.1.3.18. A licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.

E2.1.3.19. A telegraph company.

E2.1.3.20. A business engaged in vehicle sales, including automobile, airplane, and boat sales.

E2.1.3.21 Persons involved in real estate closings and settlements.

E2.1.3.22. The United States Postal Service.

E2.1.3.23. An agency of the United States Government or of a State or local government performing a duty or power of a business described in this definition.

E2.1.3.24. A casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which is licensed as a casino, gambling casino, or gaming establishment under the laws of a State or locality or is an Indian gaming operation conducted pursuant to, and as authorized by, the Indian Gaming Regulatory Act (reference (d)).

E2.1.3.25. Any business or agency that engages in any activity which the Secretary of the Treasury, by regulation determines to be an activity in which any business described in this definition is authorized to engage; or any other business designated by the Secretary of the Treasury whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

E2.1.3.26. Any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act (reference (e)) that is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.

E2.1.4. Financial Institution (other than for intelligence activity purposes). Any office of a bank, savings bank, credit card issuer, industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit

union, or consumer finance institution that is located in any state or territory of the United States, or in the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.

E2.1.5. Financial Record. An original, its copy, or information known to have been derived from the original record held by a financial institution that pertains to a customer's relationship with the financial institution.

E2.1.6. Government Authority. Any agency or Department of the United States, or any officer, employee, or agent thereof, to include DoD law enforcement offices, personnel security elements, and/or intelligence organizations.

E2.1.7. Intelligence Activities. The collection, production, and dissemination of foreign intelligence and counterintelligence, to include investigation or analyses related to international terrorism, by DoD intelligence organizations.

E2.1.8. Intelligence Organizations. Any element of a DoD Component authorized by the Secretary of Defense to conduct intelligence activities.

E2.1.9. Law Enforcement Inquiry. A lawful investigation or official proceeding that inquires into a violation of or failure to comply with a criminal or civil statute, or any rule, regulation, or order issued pursuant thereto.

E2.1.10. Law Enforcement Office. Any element of a DoD Component authorized by the Head of the DoD Component conducting law enforcement inquiries.

E2.1.11. Person. An individual or a partnership consisting of five or fewer individuals.

E2.1.12. Personnel Security Element. Any element of a DoD Component authorized by the Secretary of Defense conducting personnel security investigations.

E2.1.13. Personnel Security Investigation. An investigation required for determining a person's eligibility for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. Personnel security investigations include investigations conducted for the purpose of making personnel security determinations. They also include investigations of allegations that may arise subsequent to favorable adjudicative action and require resolution to determine a person's current eligibility for access to classified information or assignment or retention in a sensitive position.

E3. ENCLOSURE 3

OBTAINING BASIC IDENTIFYING ACCOUNT INFORMATION

E3.1.1. A DoD law enforcement office may issue a formal written request for basic identifying account information to a financial institution relevant to a legitimate law enforcement inquiry. A request may be issued to a financial institution for any or all of the following identifying data:

E3.1.1.1. Name.

E3.1.1.2. Address.

E3.1.1.3. Account number.

E3.1.1.4. Type of account of any customer or ascertainable group of customers associated with a financial transaction or class of financial transactions.

E3.1.2. The notice (paragraph E5.1.2., below), challenge (paragraph E5.1.4., below), and transfer (paragraph E9.1.2., below) requirements of this Instruction shall not apply when a Government authority is seeking only the above specified basic identifying information concerning a customer's account.

E3.1.3. A format for obtaining basic identifying account information is set forth in enclosure 11.

E4. ENCLOSURE 4

OBTAINING CUSTOMER AUTHORIZATION

E4.1.1. A DoD law enforcement office or personal security element seeking access to a person's financial records shall, when feasible, obtain the customer's consent.

E4.1.2. Any authorization obtained under paragraph E4.1.1., above, shall:

E4.1.2.1. Be in writing, signed, and dated.

E4.1.2.2. Identify the particular financial records that are being disclosed.

E4.1.2.3. State that the customer may revoke the authorization at any time before disclosure.

E4.1.2.4. Specify the purposes for disclosure and to which Governmental authority the records may be disclosed.

E4.1.2.5. Authorize the disclosure for a period not in excess of 3 months.

E4.1.2.6. Contain a "Statement of Customer Rights" as required by reference (b) (see enclosure 12).

E4.1.2.7. Contain a Privacy Act Statement as required by DoD Directive 5400.11 (reference (f)) for a personnel security investigation.

E4.1.3. Any customer's authorization not containing all of the elements listed in paragraph E4.1.2., above, shall be void. A customer authorization form, in a format set forth in enclosure 12, shall be used for this purpose.

E4.1.4. A copy of the customer's authorization shall be made a part of the law enforcement or personnel security file where the financial records are maintained.

E4.1.5. A certificate of compliance stating that the applicable requirements of reference (b) have been met (enclosure 15), along with the customer's authorization, shall be provided to the financial institution as a prerequisite to obtaining access to financial records.

E5. ENCLOSURE 5

OBTAINING ACCESS BY ADMINISTRATIVE OR JUDICIAL SUBPOENA OR BY FORMAL WRITTEN REQUEST

E5.1.1. Access to information contained in financial records from a financial institution may be obtained by Government authority when the nature of the records is reasonably described and the records are acquired by:

E5.1.1.1. Administrative Summons or Subpoena

E5.1.1.1.1. Within the Department of Defense, the Inspector General, DoD, has the authority under the Inspector General Act (reference (g)) to issue administrative subpoenas for access to financial records. No other DoD Component official may issue summons or subpoenas for access to these records.

E5.1.1.1.2. The Inspector General, DoD shall issue administrative subpoenas for access to financial records in accordance with established procedures but subject to the procedural requirements of this enclosure.

E5.1.1.2. Judicial Subpoena.

E5.1.1.3. Formal Written Request.

E5.1.1.3.1. Formal requests may only be used if an administrative summons or subpoena is not reasonably available to obtain the financial records.

E5.1.1.3.2. A formal written request shall be in a format set forth in enclosure 13 and shall:

E5.1.1.3.2.1. State that the request is issued under reference (b) and the DoD Component's implementation of this Instruction.

E5.1.1.3.2.2. Describe the specific records to be examined.

E5.1.1.3.2.3. State that access is sought in connection with a legitimate law enforcement inquiry.

E5.1.1.3.2.4. Describe the nature of the inquiry.

E5.1.1.3.2.5. Be signed by the head of the law enforcement office or a designee.

E5.1.2. A copy of the administrative or judicial subpoena or formal request, along with a notice specifying the nature of the law enforcement inquiry, shall be served on the person or

mailed to the person's last known mailing address on or before the subpoena is served on the financial institution unless a delay of notice has been obtained under enclosure 10.

E5.1.3. The notice to the customer shall be in a format similar to enclosure 14 and shall be personally served at least 10 days or mailed at least 14 days prior to the date on which access is sought.

E5.1.4. The customer shall have 10 days to challenge a notice request when personal service is made and 14 days when service is by mail.

E5.1.5. No access to financial records shall be attempted before the expiration of the pertinent time period while awaiting receipt of a potential customer challenge, or prior to the adjudication of any challenge made.

E5.1.6. The official who signs the customer notice shall be designated to receive any challenge from the customer.

E5.1.7. When a customer fails to file a challenge to access to financial records within the above pertinent time periods, or after a challenge is adjudicated in favor of the law enforcement office, the head of the office, or a designee, shall certify in writing to the financial institution that such office has complied with the requirements of reference (b). No access to any financial records shall be made before such certification (enclosure 15) is provided the financial institution.

E6. ENCLOSURE 6

OBTAINING ACCESS BY SEARCH WARRANT

E6.1.1. A Government authority may obtain financial records by using a search warrant obtained under Rule 41 of the Federal Rules of Criminal Procedure (reference (h)).

E6.1.2. Unless a delay of notice has been obtained under provisions of enclosure 10, the law enforcement office shall, no later than 90 days after serving the search warrant, mail to the customer's last known address a copy of the search warrant together with the following notice:

"Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this [DoD office or activity] on [date] for the following purpose: [state purpose]. You may have rights under the Right to Financial Privacy Act of 1978."

E6.1.3. In any state or territory of the United States, or in the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands, search authorizations signed by installation commanders, military judges, or magistrates shall not be used to gain access to financial records.

E7. ENCLOSURE 7

REQUESTS FOR FINANCIAL RECORDS IN CONNECTION WITH FOREIGN INTELLIGENCE AND FOREIGN COUNTERINTELLIGENCE ACTIVITIES

E7.1.1. Financial records may be obtained from a financial institution (as identified at paragraph E2.1.3.) by an intelligence organization, as identified in DoD 5240.1 (reference (i)), authorized to conduct intelligence activities, to include investigation or analyses related to international terrorism, pursuant to references (i) and Executive Order 12333 (reference (j)).

E7.1.2. The provisions of this Instruction do not apply to the production and disclosure of financial records when requests are submitted by intelligence organizations except as may be required by this enclosure.

E7.1.3. When a request for financial records is made under paragraph E7.1.1., above, a Component official designated by the Secretary of Defense, the Secretary of a Military Department, or the Head of the DoD Component authorized to conduct foreign intelligence or foreign counterintelligence activities shall certify to the financial institution that the requesting Component has complied with the provisions of reference (b). Such certification in a format similar to enclosure 15 shall be made before obtaining any records.

E7.1.4. An intelligence organization requesting financial records under paragraph E7.1.1., above, may notify the financial institution from which records are sought that section 3414(3) of reference (b) prohibits disclosure to any person by the institution, its agents, or employees that financial records have been sought or obtained.

E7.1.5. An intelligence organization requesting financial records under paragraph E7.1.1., above, shall maintain an annual tabulation of the occasions in which this access procedure was used.

E8. ENCLOSURE 8

OBTAINING EMERGENCY ACCESS

E8.1.1. Except as provided in paragraphs E8.1.2. and E8.1.3., below, nothing in this Instruction shall apply to a request for financial records from a financial institution when a determination is made that a delay in obtaining access to such records would create an imminent danger of:

E8.1.1.1. Physical injury to any person.

E8.1.1.2. Serious property damage.

E8.1.1.3. Flight to avoid prosecution.

E8.1.2. When access is made to financial records under paragraph E8.1.1., above, a Component official designated by the Secretary of Defense or the Secretary of a Military Department shall:

E8.1.2.1. Certify in writing, in a format set forth in enclosure 15, to the financial institution that the Component has complied with the provisions of reference (b), as a prerequisite to obtaining access.

E8.1.2.2. Submit for filing with the appropriate court a signed sworn statement setting forth the grounds for the emergency access within 5 days of obtaining access to financial records.

E8.1.3. When access to financial records are obtained under paragraph E8.1.1., above, a copy of the request, along with the following notice, shall be served on the person or mailed to the person's last known mailing address as soon as practicable after the records have been obtained unless a delay of notice has been obtained under enclosure 10.

"Records concerning your transactions held by the financial institution named in the attached request were obtained by
[Agency or Department] under the Right to Financial Privacy
Act of 1978 on [date] for the following purpose: [state with reasonable specificity the nature of the law enforcement inquiry]. Emergency access to such records was obtained on the grounds that [state grounds]."

Mailings under this paragraph shall be by certified or registered mail.

E9. ENCLOSURE 9

RELEASING INFORMATION OBTAINED FROM FINANCIAL INSTITUTIONS

E9.1.1. Financial records obtained under reference (b) shall be marked: "This record was obtained pursuant to the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et. seq., and may not be transferred to another Federal Agency or Department without prior compliance with the transferring requirements of 12 U.S.C. 3412."

E9.1.2. Financial records obtained under this Instruction shall not be transferred to another Agency or Department outside the Department of Defense unless the head of the transferring law enforcement office, personnel security element, or intelligence organization, or designee, certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity (to include investigation or analyses related to international terrorism) within the jurisdiction of the receiving Agency or Department. Such certificates shall be maintained with the DoD Component along with a copy of the released records.

E9.1.3. Subject to paragraph E9.1.4., below, and unless a delay of customer notice has been obtained under enclosure 10, the law enforcement office or personnel security element shall, within 14 days, personally serve or mail to the customer, at his or her last known address, a copy of the certificate required by section E9.1.2., above, along with the following notice:

> "Copies of or information contained in your financial records lawfully in possession of [name of Component] have been furnished to [name of Agency or Department] pursuant to the Right to Financial Privacy Act of 1978 for the following purposes: [state the nature of the law enforcement inquiry with reasonable specificity]. If you believe that this transfer has not been made to further a legitimate law enforcement inquiry, you may have legal rights under the Financial Privacy Act of 1978 or the Privacy Act of 1974."

E9.1.4. If a request for release of information is from a Federal Agency, as identified in reference (j), authorized to conduct foreign intelligence or foreign counterintelligence activities), the transferring DoD Component shall release the information without notifying the customer, unless permission to provide notification is given in writing by the requesting Agency.

E9.1.5. Whenever financial data obtained under this Instruction is incorporated into a report of investigation or other correspondence; precautions must be taken to ensure that:

E9.1.5.1. The reports or correspondence are not distributed outside the Department of Defense except in compliance with paragraph E9.1.2., above; and

E9.1.5.2. The report or other correspondence contains an appropriate warning restriction on the first page or cover.
Such a warning could read as follows:

"Some of the information contained herein (cite specific paragraph) is financial record information which was obtained pursuant to the Right to Privacy Act of 1978, 12 U.S.C. 3401 et seq. This information may not be released to another Federal Agency or Department outside the Department of Defense except for those purposes expressly authorized by Act."

E10. ENCLOSURE 10

PROCEDURES FOR DELAY OF NOTICE

E10.1.1. The customer notice required when seeking an administrative subpoena or summons (paragraph E5.1.2.), obtaining a search warrant (paragraph E6.1.2.), seeking a judicial subpoena (paragraph E5.1.2.), making a formal written request (paragraph E5.1.2.), obtaining emergency access (paragraph E8.1.3.), or transferring information (paragraph E9.1.3.) may be delayed for an initial period of 90 days and successive periods of 90 days. The notice required when obtaining a search warrant (paragraph E6.2.) may be delayed for a period of 180 days and successive periods of 90 days. A delay of notice may only be made by an order of an appropriate court if the presiding judge or magistrate finds that:

E10.1.1.1. The investigation is within the lawful jurisdiction of the Government authority seeking the records.

E10.1.1.2. There is reason to believe the records being sought are relevant to a law enforcement inquiry.

E10.1.1.3. There is reason to believe that serving the notice will result in:

E10.1.1.3.1. Endangering the life or physical safety of any person.

E10.1.1.3.2. Flight from prosecution.

E10.1.1.3.3. Destruction of or tampering with evidence.

E10.1.1.3.4. Intimidation of potential witnesses.

E10.1.1.3.5. Otherwise seriously jeopardizing an investigation or official proceeding or unduly delaying a trial or ongoing official proceeding to the same degree as the circumstances in subparagraphs E8.1.1.3.1. through E8.1.1.3.4., above.

E10.1.2. When a delay of notice is appropriate, legal counsel shall be consulted to obtain such a delay. Application for delays of notice shall be made with reasonable specificity.

E10.1.3. Upon the expiration of a delay of notification obtained under paragraph E10.1.1. for a search warrant, the law enforcement office obtaining such records shall mail to the customer a copy of the search warrant, along with the following notice:

> "Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this [agency or department] on [date].

Notification was delayed beyond the statutory 180-day delay period pursuant to a determination by the court that such notice would seriously jeopardize an investigation concerning [state with reasonable specificity]. You may have rights under the Right to Financial Privacy Act of 1978."

E10.1.4. Upon the expiration of all other delays of notification obtained under paragraph E10.1.1., the customer shall be served with or mailed a copy of the legal process or formal request, together with the following notice which shall state with reasonable specificity the nature of the law enforcement inquiry.

"Records or information concerning your transactions which are held by the financial institution named in the attached process or request were supplied to or requested by the Government authority named in the process or request on (date). Notification was withheld pursuant to a determination by the (title of the court ordering the delay) under the Right to Financial Privacy Act of 1978 that such notice might (state the reason). The purpose of the investigation or official proceeding was (state the purpose)."

E11. ENCLOSURE 11

FORMAT FOR OBTAINING BASIC IDENTIFYING ACCOUNT INFORMATION

[Official Letterhead]

[Date]

Mr./Mrs. XXXXXXXXXX
Chief Teller [as appropriate]
First National Bank
Anywhere, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXX

In connection with a legitimate law enforcement inquiry and pursuant to section 3413(g) of the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et. seq., you are requested to provide the following account information:

[Name, address, account number, and type of account of any customer or ascertainable group of customers associated with a financial transaction or class of financial transactions.

I hereby certify, pursuant to section 3403(b) of the Right of Financial Privacy Act of 1978, that the provisions of the Act have been complied with as to this request for account information.

Under section 3417(c) of the Act, good faith reliance upon this certification relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of the requested financial records.

[Official Signature Block]

E12. ENCLOSURE 12

FORMAT FOR CUSTOMER AUTHORIZATION

Pursuant to section 3404(a) of the Right to Financial Privacy Act of 1978, I, [Name of customer], having read the explanation of my rights on the reverse side, hereby authorize the [Name and address of financial institution] to disclosure these financial records: [List the particular financial records] to [DoD Component] for the following purpose(s): [Specify the purpose(s)].

I understand that the authorization may be revoked by me in writing at any time before my records, as described above, are disclosed, and that this authorization is valid for no more than three months from the date of my signature.

Signature:_____ Date:_____

[Typed name]
[Mailing address of customer]

STATEMENT OF CUSTOMER RIGHTS UNDER THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

Federal law protects the privacy of your financial records. Before banks, savings and loan associations, credit unions, credit card issuers, or other financial institutions may give financial information about you to a Federal Agency, certain procedures must be followed.

AUTHORIZATION TO ACCESS FINANCIAL RECORDS

You may be asked to authorize the financial institution to make your financial records available to the Government. You may withhold your authorization, and your authorization is not required as a condition of doing business with any financial institution. If you provide authorization, it can be revoked in writing at any time before your records are disclosed. Furthermore, any authorization you provide is effective for only three months, and your financial institution must keep a record of the instances in which it discloses your financial information.

WITHOUT YOUR AUTHORIZATION

Without your authorization, a Federal Agency that wants to see your financial records may do so ordinarily only by means of a lawful administrative subpoena or summons, search warrant, judicial subpoena, or formal written request for that purpose. Generally, the Federal Agency must give you advance notice of its request for your records explaining why the information is being sought and telling you how to object in court.

The Federal Agency must also send you copies of court documents to be prepared by you with instructions for filling them out. While these procedures will be kept as simple as possible, you may want to consult an attorney before making a challenge to a Federal Agency's request.

EXCEPTIONS

In some circumstances, a Federal Agency may obtain financial information about you without advance notice or your authorization. In most of these cases, the Federal Agency will be required to go to court for permission to obtain your records without giving you notice beforehand. In these instances, the court will make the Government show that its investigation and request for your records are proper. When the reason for the delay of notice no longer exists, you will be notified that your records were obtained.

TRANSFER OF INFORMATION

Generally, a Federal Agency that obtains your financial records is prohibited from transferring them to another Federal Agency unless it certifies in writing that the transfer is proper and sends a notice to you that your records have been sent to another Agency.

PENALTIES

If the Federal Agency or financial institution violates the Right to Financial Privacy Act, you may sue for damages or seek compliance with the law. If you win, you may be repaid your attorney's fee and costs.

ADDITIONAL INFORMATION

If you have any questions about your rights under this law, or about how to consent to release your financial records, please call the official whose name and telephone number appears below:

_____

(Last Name, First Name, Middle Initial) Title
(Area Code) (Telephone number)

_____

(Component activity, Local Mailing Address)

E13. ENCLOSURE 13

FORMAT FOR FORMAL WRITTEN REQUEST

[Official Letterhead]

[Date]

Mr./Mrs. XXXXXXXXXX
President (as appropriate)
City National Bank and Trust Company
Anytown, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXXXXX

In connection with a legitimate law enforcement inquiry and pursuant to section 3402(5) and section 3408 of the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et. seq., and [cite Component's implementation of this Instruction], you are requested to provide the following account information pertaining to the subject:

[Describe the specific records to be examined]

The [DoD Component] is without authority to issue an administrative summons or subpoena for access to these financial records which are required for [Describe the nature or purpose of the inquiry].

A copy of this request was [personally served upon or mailed to the subject on [date] who has [10 or 14] days in which to challenge this request by filing an application in an appropriate United States District Court if the subject desires to do so.

Upon the expiration of the above mentioned time period and absent any filing or challenge by the subject, you will be furnished a certification certifying in writing that the applicable provisions of the Act have been complied with prior to obtaining the requested records. Upon your receipt of a Certificate of Compliance with the Right to Financial Privacy Act of 1978, you will be relieved of any possible liability to the subject in connection with the disclosure of the requested financial records.

[Official Signature Block]

E14. ENCLOSURE 14

FORMAT FOR CUSTOMER NOTICE FOR ADMINISTRATIVE OR JUDICIAL SUBPOENA OR FOR A FORMAL WRITTEN REQUEST

[Official Letterhead]

[Date]

Mr./Ms. XXXXX X. XXXX
1500 N. Main Street
Anytown, VA 00000-0000

Dear Mr./Ms. XXXX:

Information or records concerning your transactions held by the financial institution named in the attached [administrative subpoena or summons] [judicial subpoena] [request] are being sought by the [Agency/Department] in accordance with the Right to Financial Privacy Act of 1978, Title 12, United States Code, Section 3401 et. seq., and [Component's implementing document], for the following purpose(s):

[List the purpose(s)]

If you desire that such records or information not be made available, you must:

1. Fill out the accompanying motion paper and sworn statement or write one of your own, stating that you are the customer whose records are being requested by the Government and either giving the reasons you believe that the records are not relevant to the legitimate law enforcement inquiry stated in this notice or any other legal basis for objecting to the release of the records.

2. File the motion and statement by mailing or delivering them to the clerk of any one of the following United States District Courts:

[List applicable courts]

3. Serve the Government authority requesting the records by mailing or delivering a copy of your motion and statement to: [Give title and address].

4. Be prepared to come to court and present your position in further detail.

5. You do not need to have a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of 10 days from the date of personal service or 14 days from the date of mailing of this notice, the records or information requested therein may be made available. These records may be transferred to other Government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer.

[Signature]
[Name and title of official]
[DoD Component]
[Telephone]

Attachments - 3
1. Copy of request
2. Motion papers
3. Sworn statement

E15. ENCLOSURE 15

FORMAT FOR CERTIFICATE OF COMPLIANCE WITH THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

[Official Letterhead]

[Date]

Mr./Mrs. XXXXXXXXXX
Manager
Army Federal Credit Union
Fort Anywhere, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXX

I certify, pursuant to section 3403(b) of the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et. seq., that the applicable provisions of that statute have been complied with as to the [Customer's authorization, administrative subpoena or summons, search warrant, judicial subpoena, formal written request, emergency access, as applicable] presented on [date], for the following financial records of [customer's name]:

[Describe the specific records]

Pursuant to section 3417(c) of the Right to Financial Privacy Act of 1978, good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records.

[Official Signature Block]

E16. ENCLOSURE 16

OBTAINING ACCESS TO FINANCIAL RECORDS OVERSEAS

E16.1.1. The provisions of reference (b) do not govern obtaining access to financial records maintained by military banking contractors overseas or other financial institutions in offices located on DoD installations outside the United States, the District of Columbia, Guam, American Samoa, Puerto Rico, or the Virgin Islands.

E16.1.2. Access to financial records held by such contractors or institutions is preferably obtained by customer authorization. However, in those cases where it would not be appropriate to obtain this authorization or where such authorization is refused and the financial institution is not otherwise willing to provide access to its records:

E16.1.2.1. A law enforcement activity may seek access by the use of a search authorization issued pursuant to established Component procedures; Rule 315, Military Rules of Evidence (Part III, Manual for Courts-Martial (reference (k)); and Article 46 of the Uniform Code of Military Justice (reference (l)).

E16.1.2.2. An intelligence organization may seek access pursuant to Procedure 7, DoD 5240.1-R (reference (m)).

E16.1.3. Information obtained under this Enclosure shall be properly identified as financial information and transferred only where an official need-to-know exists. Failure to identify or limit access in accordance with this paragraph does not render the information inadmissible in courts-martial or other proceedings.

E16.1.4. Access to financial records maintained by all other financial institutions overseas by law enforcement activities shall be in accordance with the local foreign statutes or procedures governing such access.

Executive Order 12333--United States intelligence activities

Source: The provisions of Executive Order 12333 of Dec. 4, 1981, appear at 46 FI CFR, 1981 Comp., p. 200, unless otherwise noted.

Table of Contents

Preamble

Part 1. *Goals, Direction, Duties, and Responsibilities With Respect to the National I Effort*

1.1 Goals
1.2 The National Security Council
1.3 National Foreign Intelligence Advisory Groups
1.4 The Intelligence Community
1.5 Director of Central Intelligence
1.6 Duties and Responsibilities of the Heads of Executive Branch Departmen Agencies
1.7 Senior Officials of the Intelligence Community
1.8 The Central Intelligence Agency
1.9 The Department of State
1.10 The Department of the Treasury
1.11 The Department of Defense
1.12 Intelligence Components Utilized by the Secretary of Defense
1.13 The Department of Energy
1.14 The Federal Bureau of Investigation

Part 2. *Conduct of Intelligence Activities*

2.1 Need
2.2 Purpose
2.3 Collection of Information
2.4 Collection Techniques
2.5 Attorney General Approval
2.6 Assistance to Law Enforcement Authorities
2.7 Contracting
2.8 Consistency With Other Laws

2.9 Undisclosed Participation in Organizations Within the United States
2.10 Human Experimentation
2.11 Prohibition on Assassination
2.12 Indirect Participation
Part 3.*General Provisions*
3.1 Congressional Oversight
3.2 Implementation
3.3 Procedures
3.4 Definitions
3.5 Purpose and Effect
3.6 Revocation

Timely and accurate information about the activities, capabilities, plans, and intent foreign powers, organizations, and persons and their agents, is essential to the na security of the United States. All reasonable and lawful means must be used to en the United States will receive the best intelligence available. For that purpose, by v the authority vested in me by the Constitution and statutes of the United States of including the National Security Act of 1947, as amended, and as President of the L States of America, in order to provide for the effective conduct of United States int activities and the protection of constitutional rights, it is hereby ordered as follows

Part 1

Goals, Direction, Duties and Responsibilities With Respect to the National Intelliger

1.1*Goals.* The United States intelligence effort shall provide the President and the I Security Council with the necessary information on which to base decisions concer conduct and development of foreign, defense and economic policy, and the protect United States national interests from foreign security threats. All departments and shall cooperate fully to fulfill this goal.
(a) Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.
(b) All means, consistent with applicable United States law and this Order, and wit consideration of the rights of United States persons, shall be used to develop intell information for the President and the National Security Council. A balanced approa between technical collection efforts and other means should be maintained and en
(c) Special emphasis should be given to detecting and countering espionage and o threats and activities directed by foreign intelligence services against the United St Government, or United States corporations, establishments, or persons.
(d) To the greatest extent possible consistent with applicable United States law an Order, and with full consideration of the rights of United States persons, all agenci departments should seek to ensure full and free exchange of information in order t maximum benefit from the United States intelligence effort.

1.2*The National Security Council.*
(a) *Purpose.* The National Security Council (NSC) was established by the National S

Act of 1947 to advise the President with respect to the integration of domestic, for military policies relating to the national security. The NSC shall act as the highest I Branch entity that provides review of, guidance for and direction to the conduct of national foreign intelligence, counterintelligence, and special activities, and attend and programs.

(b) *Committees.* The NSC shall establish such committees as may be necessary to its functions and responsibilities under this Order. The NSC, or a committee establ shall consider and submit to the President a policy recommendation, including all c each special activity and shall review proposals for other sensitive intelligence ope

1.3*National Foreign Intelligence Advisory Groups.*

(a) *Establishment and Duties.* The Director of Central Intelligence shall establish s councils, or groups as required for the purpose of obtaining advice from within the Intelligence Community concerning:

(1) Production, review and coordination of national foreign intelligence;

(2) Priorities for the National Foreign Intelligence Program budget;

(3) Interagency exchanges of foreign intelligence information;

(4) Arrangements with foreign governments on intelligence matters;

(5) Protection of intelligence sources and methods;

(6) Activities of common concern; and

(7) Such other matters as may be referred by the Director of Central Intelli

(b) *Membership.* Advisory groups established pursuant to this section shall be chai Director of Central Intelligence or his designated representative and shall consist o representatives from organizations within the Intelligence Community and from de or agencies containing such organizations, as designated by the Director of Centra Intelligence. Groups for consideration of substantive intelligence matters will inclu representatives of organizations involved in the collection, processing and analysis intelligence. A senior representative of the Secretary of Commerce, the Attorney G Assistant to the President for National Security Affairs, and the Office of the Secret Defense shall be invited to participate in any group which deals with other than su intelligence matters.

1.4*The Intelligence Community.* The agencies within the Intelligence Community s accordance with applicable United States law and with the other provisions of this conduct intelligence activities necessary for the conduct of foreign relations and th protection of the national security of the United States, including:

(a) Collection of information needed by the President, the National Security Counci Secretaries of State and Defense, and other Executive Branch officials for the perf their duties and responsibilities;

(b) Production and dissemination of intelligence;

(c) Collection of information concerning, and the conduct of activities to protect ag intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the U States by foreign powers, organizations, persons, and their agents;

(d) Special activities;

(e) Administrative and support activities within the United States and abroad nece: the performance of authorized activities; and
(f) Such other intelligence activities as the President may direct from time to time.

1.5*Director of Central Intelligence.* In order to discharge the duties and responsibil prescribed by law, the Director of Central Intelligence shall be responsible directly President and the NSC and shall:
(a) Act as the primary adviser to the President and the NSC on national foreign int and provide the President and other officials in the Executive Branch with national intelligence;
(b) Develop such objectives and guidance for the Intelligence Community as will e capabilities for responding to expected future needs for national foreign intelligenc
(c) Promote the development and maintenance of services of common concern by intelligence organizations on behalf of the Intelligence Community;
(d) Ensure implementation of special activities;
(e) Formulate policies concerning foreign intelligence and counterintelligence arran with foreign governments, coordinate foreign intelligence and counterintelligence relationships between agencies of the Intelligence Community and the intelligence security services of foreign governments, and establish procedures governing the liaison by any department or agency with such services on narcotics activities;
(f) Participate in the development of procedures approved by the Attorney General criminal narcotics intelligence activities abroad to ensure that these activities are c with foreign intelligence programs;
(g) Ensure the establishment by the Intelligence Community of common security a standards for managing and handling foreign intelligence systems, information, an products;
(h) Ensure that programs are developed which protect intelligence sources, metho analytical procedures;
(i) Establish uniform criteria for the determination of relative priorities for the tran critical national foreign intelligence, and advise the Secretary of Defense concernin communications requirements of the Intelligence Community for the transmission intelligence;
(j) Establish appropriate staffs, committees, or other advisory groups to assist in t execution of the Director's responsibilities;
(k) Have full responsibility for production and dissemination of national foreign inte and authority to levy analytic tasks on departmental intelligence production organi consultation with those organizations, ensuring that appropriate mechanisms for c analysis are developed so that diverse points of view are considered fully and diffe judgment within the Intelligence Community are brought to the attention of nation policymakers;
(*l*) Ensure the timely exploitation and dissemination of data gathered by national f intelligence collection means, and ensure that the resulting intelligence is dissemin immediately to appropriate government entities and military commands;
(m) Establish mechanisms which translate national foreign intelligence objectives a priorities approved by the NSC into specific guidance for the Intelligence Communi

conflicts in tasking priority, provide to departments and agencies having informatic collection capabilities that are not part of the National Foreign Intelligence Progran tasking concerning collection of national foreign intelligence, and provide for the development of plans and arrangements for transfer of required collection tasking to the Secretary of Defense when directed by the President;
(n) Develop, with the advice of the program managers and departments and agen concerned, the consolidated National Foreign Intelligence Program budget, and pre the President and the Congress;
(o) Review and approve all requests for reprogramming National Foreign Intelligen Program funds, in accordance with guidelines established by the Office of Manager Budget;
(p) Monitor National Foreign Intelligence Program implementation, and, as necessa conduct program and performance audits and evaluations;
(q) Together with the Secretary of Defense, ensure that there is no unnecessary o between national foreign intelligence programs and Department of Defense intellig programs consistent with the requirement to develop competitive analysis, and pr and obtain from the Secretary of Defense all information necessary for this purpos
(r) In accordance with law and relevant procedures approved by the Attorney Gen this Order, give the heads of the departments and agencies access to all intelligen developed by the CIA or the staff elements of the Director of Central Intelligence, the national intelligence needs of the departments and agencies; and
(s) Facilitate the use of national foreign intelligence products by Congress in a sec manner.

1.6*Duties and Responsibilities of the Heads of Executive Branch Departments and* .
(a) The heads of all Executive Branch departments and agencies shall, in accordan law and relevant procedures approved by the Attorney General under this Order, g Director of Central Intelligence access to all information relevant to the national in needs of the United States, and shall give due consideration to the requests from t Director of Central Intelligence for appropriate support for Intelligence Community
(b) The heads of departments and agencies involved in the National Foreign Intelli Program shall ensure timely development and submission to the Director of Centra Intelligence by the program managers and heads of component activities of propo national programs and budgets in the format designated by the Director of Central Intelligence, and shall also ensure that the Director of Central Intelligence is provi timely and responsive manner, all information necessary to perform the Director's and budget responsibilities.
(c) The heads of departments and agencies involved in the National Foreign Intelli Program may appeal to the President decisions by the Director of Central Intelliger budget or reprogramming matters of the National Foreign Intelligence Program.

1.7*Senior Officials of the Intelligence Community.* The heads of departments and a with organizations in the Intelligence Community or the heads of such organizatior appropriate, shall:
(a) Report to the Attorney General possible violations of federal criminal laws by e and of specified federal criminal laws by any other person as provided in procedur

upon by the Attorney General and the head of the department or agency concerne
manner consistent with the protection of intelligence sources and methods, as spe
those procedures;
(b) In any case involving serious or continuing breaches of security, recommend tc
Attorney General that the case be referred to the FBI for further investigation;
(c) Furnish the Director of Central Intelligence and the NSC, in accordance with ap
law and procedures approved by the Attorney General under this Order, the inform
required for the performance of their respective duties;
(d) Report to the Intelligence Oversight Board, and keep the Director of Central In
appropriately informed, concerning any intelligence activities of their organizations
have reason to believe may be unlawful or contrary to Executive order or Presiden
directive;
(e) Protect intelligence and intelligence sources and methods from unauthorized di
consistent with guidance from the Director of Central Intelligence;
(f) Disseminate intelligence to cooperating foreign governments under arrangemer
established or agreed to by the Director of Central Intelligence;
(g) Participate in the development of procedures approved by the Attorney Genera
governing production and dissemination of intelligence resulting from criminal narc
intelligence activities abroad if their departments, agencies, or organizations have
intelligence responsibilities for foreign or domestic narcotics production and traffick
(h) Instruct their employees to cooperate fully with the Intelligence Oversight Boai
(i) Ensure that the Inspectors General and General Counsels for their organizations
access to any information necessary to perform their duties assigned by this Order

1.8*The Central Intelligence Agency.* All duties and responsibilities of the CIA shall l
to the intelligence functions set out below. As authorized by this Order; the Nation
Act of 1947, as amended; the CIA Act of 1949, as amended; appropriate directives
applicable law, the CIA shall:
(a) Collect, produce and disseminate foreign intelligence and counterintelligence, ii
information not otherwise obtainable. The collection of foreign intelligence or
counterintelligence within the United States shall be coordinated with the FBI as re
procedures agreed upon by the Director of Central Intelligence and the Attorney G
(b) Collect, produce and disseminate intelligence on foreign aspects of narcotics pr
and trafficking;
(c) Conduct counterintelligence activities outside the United States and, without as
performing any internal security functions, conduct counterintelligence activities w
United States in coordination with the FBI as required by procedures agreed upon
Director of Central Intelligence and the Attorney General;
(d) Coordinate counterintelligence activities and the collection of information not o
obtainable when conducted outside the United States by other departments and ag
(e) Conduct special activities approved by the President. No agency except the CIA
Armed Forces of the United States in time of war declared by Congress or during a
covered by a report from the President to the Congress under the War Powers Res
Stat. 855)[1]) may conduct any special activity unless the President determines that
agency is more likely to achieve a particular objective;

(f) Conduct services of common concern for the Intelligence Community as directe NSC;
(g) Carry out or contract for research, development and procurement of technical : and devices relating to authorized functions;
(h) Protect the security of its installations, activities, information, property, and en by appropriate means, including such investigations of applicants, employees, cont and other persons with similar associations with the CIA as are necessary; and
(i) Conduct such administrative and technical support activities within and outside States as are necessary to perform the functions described in sections (a) through including procurement and essential cover and proprietary arrangements.

1.9*The Department of State.* The Secretary of State shall:
(a) Overtly collect information relevant to United States foreign policy concerns;
(b) Produce and disseminate foreign intelligence relating to United States foreign p required for the execution of the Secretary's responsibilities;
(c) Disseminate, as appropriate, reports received from United States diplomatic an posts;
(d) Transmit reporting requirements of the Intelligence Community to the Chiefs o States Missions abroad; and
(e) Support Chiefs of Missions in discharging their statutory responsibilities for dire coordination of mission activities.

1.10*The Department of the Treasury.* The Secretary of the Treasury shall:
(a) Overtly collect foreign financial and monetary information;
(b) Participate with the Department of State in the overt collection of general forei economic information;
(c) Produce and disseminate foreign intelligence relating to United States economi required for the execution of the Secretary's responsibilities; and
(d) Conduct, through the United States Secret Service, activities to determine the and capability of surveillance equipment being used against the President of the Ui States, the Executive Office of the President, and, as authorized by the Secretary (Treasury or the President, other Secret Service protectees and United States offici information shall be acquired intentionally through such activities except to protect such surveillance, and those activities shall be conducted pursuant to procedures a upon by the Secretary of the Treasury and the Attorney General.

1.11*The Department of Defense.* The Secretary of Defense shall:
(a) Collect national foreign intelligence and be responsive to collection tasking by t Director of Central Intelligence;
(b) Collect, produce and disseminate military and military-related foreign intelliger counterintelligence as required for execution of the Secretary's responsibilities;
(c) Conduct programs and missions necessary to fulfill national, departmental and foreign intelligence requirements;
(d) Conduct counterintelligence activities in support of Department of Defense corr outside the United States in coordination with the CIA, and within the United State coordination with the FBI pursuant to procedures agreed upon by the Secretary of

and the Attorney General;
(e) Conduct, as the executive agent of the United States Government, signals inte and communications security activities, except as otherwise directed by the NSC;
(f) Provide for the timely transmission of critical intelligence, as defined by the Dir Central Intelligence, within the United States Government;
(g) Carry out or contract for research, development and procurement of technical and devices relating to authorized intelligence functions;
(h) Protect the security of Department of Defense installations, activities, property information, and employees by appropriate means, including such investigations o applicants, employees, contractors, and other persons with similar associations wit Department of Defense as are necessary;
(i) Establish and maintain military intelligence relationships and military intelligenc exchange programs with selected cooperative foreign defense establishments and international organizations, and ensure that such relationships and programs are i accordance with policies formulated by the Director of Central Intelligence;
(j) Direct, operate, control and provide fiscal management for the National Securit and for defense and military intelligence and national reconnaissance entities; and
(k) Conduct such administrative and technical support activities within and outside States as are necessary to perform the functions described in sections (a) through

1.12*Intelligence Components Utilized by the Secretary of Defense.* In carrying out responsibilities assigned in section 1.11, the Secretary of Defense is authorized to following:

(a) *Defense Intelligence Agency,* whose responsibilities shall include;

(1) Collection, production, or, through tasking and coordination, provision o and military-related intelligence for the Secretary of Defense, the Joint Chie other Defense components, and, as appropriate, non-Defense agencies;

(2) Collection and provision of military intelligence for national foreign intelli counterintelligence products;

(3) Coordination of all Department of Defense intelligence collection require

(4) Management of the Defense Attache system; and

(5) Provision of foreign intelligence and counterintelligence staff support as the Joint Chiefs of Staff.

(b) *National Security Agency,* whose responsibilities shall include:

(1) Establishment and operation of an effective unified organization for sign intelligence activities, except for the delegation of operational control over c operations that are conducted through other elements of the Intelligence Cc No other department or agency may engage in signals intelligence activities pursuant to a delegation by the Secretary of Defense;

(2) Control of signals intelligence collection and processing activities, includi assignment of resources to an appropriate agent for such periods and tasks required for the direct support of military commanders;

(3) Collection of signals intelligence information for national foreign intellige purposes in accordance with guidance from the Director of Central Intelliger

(4) Processing of signals intelligence data for national foreign intelligence pu
accordance with guidance from the Director of Central Intelligence;

(5) Dissemination of signals intelligence information for national foreign inte
purposes to authorized elements of the Government, including the military s
accordance with guidance from the Director of Central Intelligence;

(6) Collection, processing and dissemination of signals intelligence informati
counterintelligence purposes;

(7) Provision of signals intelligence support for the conduct of military opera
accordance with tasking, priorities, and standards of timeliness assigned by
Secretary of Defense. If provision of such support requires use of national c
systems, these systems will be tasked within existing guidance from the Dir
Central Intelligence;

(8) Executing the responsibilities of the Secretary of Defense as executive a
the communications security of the United States Government;

(9) Conduct of research and development to meet the needs of the United S
signals intelligence and communications security;

(10) Protection of the security of its installations, activities, property, inform
employees by appropriate means, including such investigations of applicants
employees, contractors, and other persons with similar associations with the
are necessary;

(11) Prescribing, within its field of authorized operations, security regulation
operating practices, including the transmission, handling and distribution of
intelligence and communications security material within and among the ele
under control of the Director of the NSA, and exercising the necessary supe
control to ensure compliance with the regulations;

(12) Conduct of foreign cryptologic liaison relationships, with liaison for inte
purposes conducted in accordance with policies formulated by the Director c
Intelligence; and

(13) Conduct of such administrative and technical support activities within a
the United States as are necessary to perform the functions described in sec
through (12) above, including procurement.

(c) *Offices for the collection of specialized intelligence through reconnaissance pro*
whose responsibilities shall include:

(1) Carrying out consolidated reconnaissance programs for specialized intell

(2) Responding to tasking in accordance with procedures established by the
Central Intelligence; and

(3) Delegating authority to the various departments and agencies for resear
development, procurement, and operation of designated means of collectior

(d) *The foreign intelligence and counterintelligence elements of the Army, Navy, A*
and Marine Corps, whose responsibilities shall include:

(1) Collection, production and dissemination of military and military-related
intelligence and counterintelligence, and information on the foreign aspects
narcotics production and trafficking. When collection is conducted in respons

national foreign intelligence requirements, it will be conducted in accordance guidance from the Director of Central Intelligence. Collection of national fore intelligence, not otherwise obtainable, outside the United States shall be coc with the CIA, and such collection within the United States shall be coordinat FBI;

(2) Conduct of counterintelligence activities outside the United States in coo with the CIA, and within the United States in coordination with the FBI; and

(3) Monitoring of the development, procurement and management of tactica intelligence systems and equipment and conducting related research, develc and test and evaluation activities.

(e) *Other offices within the Department of Defense appropriate for conduct of the missions and responsibilities assigned to the Secretary of Defense.* If such other of used for intelligence purposes, the provisions of Part 2 of this Order shall apply to offices when used for those purposes.

1.13*The Department of Energy.* The Secretary of Energy shall:

(a) Participate with the Department of State in overtly collecting information with foreign energy matters;

(b) Produce and disseminate foreign intelligence necessary for the Secretary's responsibilities;

(c) Participate in formulating intelligence collection and analysis requirements whe special expert capability of the Department can contribute; and

(d) Provide expert technical, analytical and research capability to other agencies w Intelligence Community.

1.14*The Federal Bureau of Investigation.* Under the supervision of the Attorney Ge pursuant to such regulations as the Attorney General may establish, the Director o shall:

(a) Within the United States conduct counterintelligence and coordinate counterint activities of other agencies within the Intelligence Community. When a counterinte activity of the FBI involves military or civilian personnel of the Department of Defe FBI shall coordinate with the Department of Defense;

(b) Conduct counterintelligence activities outside the United States in coordination CIA as required by procedures agreed upon by the Director of Central Intelligence Attorney General;

(c) Conduct within the United States, when requested by officials of the Intelligenc Community designated by the President, activities undertaken to collect foreign int or support foreign intelligence collection requirements of other agencies within the Intelligence Community, or, when requested by the Director of the National Securi to support the communications security activities of the United States Government

(d) Produce and disseminate foreign intelligence and counterintelligence; and

(e) Carry out or contract for research, development and procurement of technical and devices relating to the functions authorized above.

Part 2

Conduct of Intelligence Activities

2.1*Need.* Accurate and timely information about the capabilities, intentions and ac foreign powers, organizations, or persons and their agents is essential to informed decisionmaking in the areas of national defense and foreign relations. Collection of information is a priority objective and will be pursued in a vigorous, innovative anc responsible manner that is consistent with the Constitution and applicable law and of the principles upon which the United States was founded.

2.2*Purpose.* This Order is intended to enhance human and technical collection tech especially those undertaken abroad, and the acquisition of significant foreign intell well as the detection and countering of international terrorist activities and espiona conducted by foreign powers. Set forth below are certain general principles that, ir to and consistent with applicable laws, are intended to achieve the proper balance the acquisition of essential information and protection of individual interests. Nothi Order shall be construed to apply to or interfere with any authorized civil or crimin enforcement responsibility of any department or agency.

2.3*Collection of Information.* Agencies within the Intelligence Community are auth collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and by the Attorney General, consistent with the authorities provided by Part 1 of this Those procedures shall permit collection, retention and dissemination of the follow of information:

(a) Information that is publicly available or collected with the consent of the perso concerned;

(b) Information constituting foreign intelligence or counterintelligence, including su information concerning corporations or other commercial organizations. Collection United States of foreign intelligence not otherwise obtainable shall be undertaken l or, when significant foreign intelligence is sought, by other authorized agencies of Intelligence Community, provided that no foreign intelligence collection by such ag may be undertaken for the purpose of acquiring information concerning the domes activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintell international narcotics or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, inclu who are targets, victims or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence source methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community n collect such information concerning present or former employees, present or forme intelligence agency contractors or their present or former employees, or applicants such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential so contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical or communications secu

investigation;
(h) Information acquired by overhead reconnaissance not directed at specific Unite persons;
(i) Incidentally obtained information that may indicate involvement in activities tha violate federal, state, local or foreign laws; and
(j) Information necessary for administrative purposes.
In addition, agencies within the Intelligence Community may disseminate informat than information derived from signals intelligence, to each appropriate agency witl Intelligence Community for purposes of allowing the recipient agency to determine the information is relevant to its responsibilities and can be retained by it.

2.4*Collection Techniques.* Agencies within the Intelligence Community shall use th intrusive collection techniques feasible within the United States or directed against States persons abroad. Agencies are not authorized to use such techniques as elec surveillance, unconsented physical search, mail surveillance, physical surveillance, monitoring devices unless they are in accordance with procedures established by t the agency concerned and approved by the Attorney General. Such procedures sha constitutional and other legal rights and limit use of such information to lawful gov purposes. These procedures shall not authorize:
(a) The CIA to engage in electronic surveillance within the United States except fo purpose of training, testing, or conducting countermeasures to hostile electronic su
(b) Unconsented physical searches in the United States by agencies other than the except for:
(1) Searches by counterintelligence elements of the military services directe military personnel within the United States or abroad for intelligence purpos authorized by a military commander empowered to approve physical search enforcement purposes, based upon a finding of probable cause to believe th persons are acting as agents of foreign powers; and
(2) Searches by CIA of personal property of non-United States persons lawf possession.
(c) Physical surveillance of a United States person in the United States by agencies than the FBI, except for:
(1) Physical surveillance of present or former employees, present or former intelligence agency contractors or their present of former employees, or app any such employment or contracting; and
(2) Physical surveillance of a military person employed by a nonintelligence a military service.
(d) Physical surveillance of a United States person abroad to collect foreign intellig except to obtain significant information that cannot reasonably be acquired by oth

2.5*Attorney General Approval.* The Attorney General hereby is delegated the powe approve the use for intelligence purposes, within the United States or against a Un person abroad, of any technique for which a warrant would be required if undertak enforcement purposes, provided that such techniques shall not be undertaken unle Attorney General has determined in each case that there is probable cause to belie

the technique is directed against a foreign power or an agent of a foreign power. E surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall b conducted in accordance with that Act, as well as this Order.

2.6*Assistance to Law Enforcement Authorities.* Agencies within the Intelligence Co are authorized to:
(a) Cooperate with appropriate law enforcement agencies for the purpose of prote employees, information, property and facilities of any agency within the Intelligenc Community;
(b) Unless otherwise precluded by law or this Order, participate in law enforcemen to investigate or prevent clandestine intelligence activities by foreign powers, or in terrorist or narcotics activities;
(c) Provide specialized equipment, technical knowledge, or assistance of expert pe use by any department or agency, or, when lives are endangered, to support local enforcement agencies. Provision of assistance by expert personnel shall be approv case by the General Counsel of the providing agency; and
(d) Render any other assistance and cooperation to law enforcement authorities n precluded by applicable law.

2.7*Contracting.* Agencies within the Intelligence Community are authorized to ente contracts or arrangements for the provision of goods or services with private comp institutions in the United States and need not reveal the sponsorship of such contr arrangements for authorized intelligence purposes. Contracts or arrangements wit institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8*Consistency With Other Laws.* Nothing in this Order shall be construed to autho activity in violation of the Constitution or statutes of the United States.

2.9*Undisclosed Participation in Organizations Within the United States.* No one acti behalf of agencies within the Intelligence Community may join or otherwise partici organization in the United States on behalf of any agency within the Intelligence C without disclosing his intelligence affiliation to appropriate officials of the organizat in accordance with procedures established by the head of the agency concerned ar approved by the Attorney General. Such participation shall be authorized only if it to achieving lawful purposes as determined by the agency head or designee. No su participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:
(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or
(b) The organization concerned is composed primarily of individuals who are not U States persons and is reasonably believed to be acting on behalf of a foreign powe

2.10*Human Experimentation.* No agency within the Intelligence Community shall s contract for or conduct research on human subjects except in accordance with guic issued by the Department of Health and Human Services. The subject's informed c shall be documented as required by those guidelines.

2.11*Prohibition on Assassination.* No person employed by or acting on behalf of th States Government shall engage in, or conspire to engage in, assassination.

2.12*Indirect Participation.* No agency of the Intelligence Community shall participa request any person to undertake activities forbidden by this Order.

Part 3

General Provisions

3.1*Congressional Oversight.* The duties and responsibilities of the Director of Centr Intelligence and the heads of other departments, agencies, and entities engaged ir intelligence activities to cooperate with the Congress in the conduct of its responsil oversight of intelligence activities shall be as provided in title 50, United States Co 413. The requirements of section 662 of the Foreign Assistance Act of 1961, as arr U.S.C. 2422), and section 501 of the National Security Act of 1947, as amended (5 413), shall apply to all special activities as defined in this Order.

3.2*Implementation.* The NSC, the Secretary of Defense, the Attorney General, and Director of Central Intelligence shall issue such appropriate directives and procedu necessary to implement this Order. Heads of agencies within the Intelligence Comr shall issue appropriate supplementary directives and procedures consistent with th The Attorney General shall provide a statement of reasons for not approving any p established by the head of an agency in the Intelligence Community other than the National Security Council may establish procedures in instances where the agency the Attorney General are unable to reach agreement on other than constitutional c legal grounds.

3.3*Procedures.* Until the procedures required by this Order have been established, activities herein authorized which require procedures shall be conducted in accorda existing procedures or requirements established under Executive Order No. 12036 Procedures required by this Order shall be established as expeditiously as possible procedures promulgated pursuant to this Order shall be made available to the con intelligence committees.

3.4*Definitions.* For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to pr against espionage, other intelligence activities, sabotage, or assassinations conduc on behalf of foreign powers, organizations or persons, or international terrorist act not including personnel, physical, document or communications security programs

(b) *Electronic surveillance* means acquisition of a nonpublic communication by elec means without the consent of a person who is a party to an electronic communicat the case of a nonelectronic communication, without the consent of a person who is present at the place of communication, but not including the use of radio direction equipment solely to determine the location of a transmitter.

(c) *Employee* means a person employed by, assigned to or acting for an agency wi

Intelligence Community.

(d) *Foreign intelligence* means information relating to the capabilities, intentions a activities of foreign powers, organizations or persons, but not including counterinte except for information on international terrorist activities.

(e) *Intelligence activities* means all activities that agencies within the Intelligence (are authorized to conduct pursuant to this Order.

(f) *Intelligence Community and agencies within the Intelligence Community* refer t following agencies or organizations:

(1) The Central Intelligence Agency (CIA);

(2) The National Security Agency (NSA);

(3) The Defense Intelligence Agency (DIA);

(4) The offices within the Department of Defense for the collection of specia national foreign intelligence through reconnaissance programs;

(5) The Bureau of Intelligence and Research of the Department of State;

(6) The intelligence elements of the Army, Navy, Air Force, and Marine Corp Federal Bureau of Investigation (FBI), the Department of the Treasury, and Department of Energy; and

(7) The staff elements of the Director of Central Intelligence.

(g) *The National Foreign Intelligence Program* includes the programs listed below, composition shall be subject to review by the National Security Council and modifi the President:

(1) The programs of the CIA;

(2) The Consolidated Cryptologic Program, the General Defense Intelligence and the programs of the offices within the Department of Defense for the co specialized national foreign intelligence through reconnaissance, except suc as the Director of Central Intelligence and the Secretary of Defense agree sl excluded;

(3) Other programs of agencies within the Intelligence Community designat by the Director of Central Intelligence and the head of the department or by President as national foreign intelligence or counterintelligence activities;

(4) Activities of the staff elements of the Director of Central Intelligence;

(5) Activities to acquire the intelligence required for the planning and condu tactical operations by the United States military forces are not included in th Foreign Intelligence Program.

(h) *Special activities* means activities conducted in support of national foreign polic objectives abroad which are planned and executed so that the role of the United S Government is not apparent or acknowledged publicly, and functions in support of activities, but which are not intended to influence United States political processes opinion, policies, or media and do not include diplomatic activities or the collection production of intelligence or related support functions.

(i) *United States person* means a United States citizen, an alien known by the inte agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a

corporation incorporated in the United States, except for a corporation directed an controlled by a foreign government or governments.

3.5*Purpose and Effect.* This Order is intended to control and provide direction and to the Intelligence Community. Nothing contained herein or in any procedures pro hereunder is intended to confer any substantive or procedural right or privilege on person or organization.

3.6*Revocation.* Executive Order No. 12036 of January 24, 1978, as amended, entit "United States Intelligence Activities," is revoked.

---

[1] **Editorial note:** The correct citation is (87 Stat. 555).

Archives.gov Home Contact Us Privacy Policy Accessibility Freedom of Information Act No FEAR Act

The U.S. National Archives and Records Administration
8601 Adelphi Road, College Park, MD 20740-6001
Telephone: 1-86-NARA-NARA or 1-866-272-6272

NSL Statute	18 U.S.C. 2709	12 U.S.C. 3414	15 U.S.C. 1681u	15 U.S.C. 1681v	50 U.S.C. 436
Addressee	communications providers	financial institutions	consumer credit agencies	consumer credit agencies	financial institutions, consumer credit agencies, travel agencies
Certifying officials	senior FBI officials and SACs	senior FBI officials and SACs	senior FBI officials and SACs	supervisory official of an agency investigating, conducting intelligence activities relating to or analyzing int'l terrorism	senior officials no lower than Ass't Secretary or Ass't Director of agency w/ employees w/ access to classified material
Information covered	identified customer's name, address, length of service, and billing info	identified customer financial records	identified consumer's name, address, former address, place and former place of employment; name and address of consumer's banks	all information relating to an identified consumer	all financial information relating to consenting, identified employee
Standard/ purpose	relevant to an investigation to protect against int'l terrorism or espionage	sought for foreign counter-intelligence purposes to protect against int'l terrorism or espionage	sought for an investigation to protect against int'l terrorism or espionage	necessary for the agency's investigation, activities, or analysis	necessary to conduct a law enforcement investigation, counter-intelligence inquiry or security determination
Dissemination	only per Att'y Gen. guidelines	only per Att'y Gen. guidelines	w/i FBI, to secure approval for intell. investigation, to military investigators when inform. relates to military member	no provision	only to agency of employee under investigation, DOJ for law enforcement or intell. purposes, or fed. agency when clearly relevant to mission
Immunity/fees	no provisions	no provisions	fees; immunity for good faith compliance with a NSL	immunity for good faith compliance with a NSL	reimbursement; immunity for good faith compliance with a NSL

~~SECRET~~

Department of Defense Response
to the Senate Select Committee on Intelligence and
the House Appropriations Committee – Defense
Following January 2007 Briefings on
National Security Letters (NSLs)

Q1: What is the percentage, by Service, of the total investigations that use NSLs?[1]

- **Army CI (FY 2000-Present):**
  - Total No. of Investigations: [redacted]
  - Total No. Using NSLs:
  - Percentage:
- **AF Office of Special Investigations (OSI) (FY 2000-Present):**
  - Total No. of Investigations: [redacted]
  - Total No. Using NSLs:
  - Percentage:
- **Naval Criminal Investigative Service (NCIS) (FY 2000-Present):**
  - Total No. of Investigations: [redacted]
  - Total No. Using NSLs:
  - Percentage:

[1] Congress has defined the term "National Security Letter" in section 119(g) of the PATRIOT Improvement and Reauthorization Act of 2006, and specifically did not include in the NSL definition requests made by authorized government agencies, such as the Department of Defense (DoD), under the Right to Financial Privacy Act (RFPA), 12 USC § 3414 (a)(1)-(4). As such, DoD requests made pursuant to the RFPA are not included in the above Service totals.

[2] For completeness, of the total number of investigations, Army CI records indicate that [redacted] investigations used a request made pursuant to the RFPA.

[3] For completeness, of the total number of investigations, Army CI investigations that used a request made pursuant to the RFPA was [redacted] of total number of investigations.

[4] For completeness, of the total number of investigations, AFOSI records indicate that [redacted] investigations used a request made pursuant to the RFPA.

[5] For completeness, of the total number of investigations, AFOSI investigations that used a request made pursuant to the RFPA was [redacted] of total number of investigations.

THIS PAGE IS UNCLASSIFIED WHEN SEPARATED FROM TAB D

Prepared by: [redacted] CI Directorate, OUSD(I)/CI&S, [redacted]

Q2: What is the breakout of statutes used for each NSL or request made pursuant to the RFPA (see note 1)?

- **Army CI: [See Footnotes 1 & 2]**
  - Total: [redacted]
  - 12 USC § 3414:
- **AF OSI [See Footnotes 4 & 5]:**
  - Total: [redacted]
  - 12 USC § 3414:
  - 50 USC § 436:
- **NCIS:**[6]
  - Total: [redacted]
  - 15 USC § 1681v
  - 12 USC § 3414:
  - 50 USC § 436:

Q3: What is the number of NSLs that DoD has asked FBI to issue in conjunction with a DoD investigation?

- DoD does not ask FBI to issue NSLs in conjunction with a DoD investigation. For DoD investigations, the military service organizations authorized to conduct counterintelligence investigations determine whether, in a particular investigation, use of NSLs is appropriate. If so, the request for information is made by the DOD organization.
- As the representatives from the Army CI and AFOSI stated during the January 2007 briefings, some investigations are conducted jointly with the FBI. During these joint investigations, it is not uncommon for the investigators to divide investigative tasks between agencies. However, this division of workload is not considered by the Department or the Military Services to be a DoD "request" for FBI to issue NSLs. Moreover, the Military Services do not maintain records of the number of FBI-issued NSLs in joint investigations.

---

[6] NCIS totals did not specify how many investigations used a request made pursuant to the RFPA, but the percentage of RFPA requests is [redacted] of the total number of investigations.

Q4: What are the relevant DoD Directives governing use of NSLs?

- ❖ DoD Directive 5200.12, "Obtaining Information from Financial Institutions," December 2, 2004 (TAB A-1)
- ❖ DoD Instruction 5200.15, "Guidance on Obtaining Information from Financial Institutions", December 2, 2004 (TAB A-2)

Q5: Please provide a copy of each Service's procedures for issuing NSL-type requests.

- ❖ Army CI Investigation Handbook – Financial Checks Excerpt (TAB B-1)
- ❖ AF OSI Manual 71-119 (Approved draft, dtd 11Feb 02) (TAB B-2)
- ❖ NCIS General Administrative document excerpt (TAB B-3)

Q6: Please provide examples of an NSL from each Service.

- ❖ Department of the Army Example (TAB C-1)
- ❖ Department of the Navy Examples (TAB C-2)
- ❖ Department of the Air Force Examples (TAB C-3)

Q7: Please provide a copy of the 1979 MOA with the FBI and the 1996 amendment.

- ❖ April 5, 1979 Memorandum of Understanding: Coordination of Counterintelligence Matters Between FBI & DoD (TAB D-1) – **Marked CONFIDENTIAL**
- ❖ 1996 Supplement to 1979 FBI/DoD Memorandum of Understanding: Coordination of Counterintelligence Matters Between FBI & DoD (TAB D-2) – **Marked SECRET**

THIS PAGE IS UNCLASSIFIED WHEN SEPARATED FROM TAB D

Prepared by: [redacted] CI Directorate, OUSD(I)/CI&S, [redacted]

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

15-10 Financial Checks

a. Legal and Regulatory Framework. The right to privacy extends to the financial aspects of a person's life. Because the U.S. financial system is complex and consists of several different types of institutions each covered by different laws and regulations; it will come as no surprise that there are also several portions of the USC that government's ability to access those records. In the following paragraphs the major relevant portions of the USC are identified and discussed with an emphasis on the authorities, exceptions and procedures that allow CI agents to access them.

(1) Fair Credit Reporting Act (15 USC 1681). The Fair Credit Reporting Act was passed to ensure the privacy, as well as the fair and accurate reporting of consumer credit information for a multitude of purposes including employment and credit worthiness. The act significantly restricts the ability of the government to perform un-consented checks of consumer reporting agency records (AKA credit reporting services). Generally, these records can be obtained only with consent or by a warrant, judicial or administrative subpoena or other court order.

(a) Exception for Identifying Data. A general exemption (15 USC 1681f) allows all governmental agencies (including Army CI) access to limited identification information. Upon the presentation of a formal written request, consumer reporting agencies will provide, name and address, former addresses, places of employment and former places of employment for named consumers. This limited authority can be used for all authorized investigative and operational purposes. (LINK to template of Request)

(b) FBI CI Exception. The original act provided the FBI a specific exception for disclosures for CI purposes (15 USC 1681u). A similar general exception for military CI services does not exist. However, the FBI exception specifically authorized the FBI to disseminate results of their checks to appropriate investigative authorities within the military as may be necessary for the conduct of a joint foreign CI investigation. Additionally, it authorizes the FBI to provide information to the military for SUBJECTs who fall under the UCMJ.

(c) Exception for International Terrorism. The PATRIOT Act added a broader exception for international terrorism (15 USC 1681v), which allows **any government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism** to conduct un-consented checks of these records. Army CI may utilize this exception. A formal written request certifying compliance with the code is required. (LINK to Consumer Reporting Services Template)

(2) Right to Financial Privacy Act of 1978 (12 USC 3401-3422). The Right to Financial Privacy Act is the primary source of financial privacy rights and governs a broad spectrum of records across a wide variety of financial institutions. Government access to records

of financial institutions may be obtained through consent, search warrant, administrative or judicial subpoena, court order or formal written request.

(a) FCI and Terrorism Exceptions. Specific exceptions exist for FCI and international terrorism (15 USC 3414(a)(1)(a) and (c) respectively). These exceptions apply to any government authority authorized to conduct foreign counterintelligence, positive intelligence or international terrorism activities. They allow un-consented checks of financial institution records upon presentation of an appropriately signed formal written request certifying compliance with the act. (LINK to template)

(b) Definition of Financial Institution. The definition of financial institution for the purposes of the exceptions outline above is broader than for the rest of the act (see 15 USC 3414(d)). The following are defined as financial institutions IAW 31 USC 5312(a)(2) and (c)(1).

(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813 (h)));
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) any credit union;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones, or jewels;
(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and settlements;
(V) the United States Postal Service;
(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which—
(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or

(II) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

(c) Army Implementation Guidance. AR 190-6, Obtaining Information from Financial Institutions, dated 15 January 1982, implements DODD 2400.12 and the Right to Financial Privacy Act of 1978 (12 USC 3401 *et seq*). It provides additional guidance on obtaining information from financial institutions by consent, search warrant, judicial subpoena, and formal written request. Generic sample templates for each type of request are provided. A specific exception for Foreign Intelligence and Foreign Counterintelligence may be found at para 2-10. This paragraph also delegates signature authority for certificates of compliance with 12 USC 3414(a)(3) to Military Intelligence Group Commanders, investigative control office, CG (or DCG) INSCOM.

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

[redacted]

c. Financial Crimes Information Network (FINCEN) Checks. FINCEN checks are considered a NAC, therefore ACCO will coordinate all FINCEN checks. This is the only authorized channel for FINCEN queries. The following information must be provided to ACCO for each request: ACCO CCN; Full name, any/all AKA, relationship in case (subject/witness); Address and phone number; DPOB; SSAN; Race/ethnicity; Sex; Height/weight; Color of eyes and hair; Other identifying data if available, such as passport number; Financial institution(s) known to be utilized; If joint/bilateral case, list other agencies involved. Specify what type of product you desire from FINCEN e.g. analytical reports and/or data base extracts.

DEPARTMENT OF THE AIR FORCE
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

[redacted]

Air Force Office of Special Investigations
1535 Command Drive, Suite C301
Andrews AFB, MD 20762-7002

Dear [redacted]

The Air Force Office of Special Investigations (AFOSI) is a Federal agency authorized to conduct foreign counterintelligence activities by Executive Order 12333 and Department of Defense Directive 5240.2. Pursuant to Title 12, United States Code, Section 3414(a) you are requested to provide the following account information pertaining to the below-named person:

All personal account information including, but not limited to, account transactions, individuals authorized to use the accounts and their personal information, account deposits, withdrawals, credits and account reports. Transaction information should include the date, business, locations, and the amount of charges

[redacted]

Please forward the requested documents via US Postal Service to:

[redacted]
Air Force Office of Special Investigations
Unit 5695
APO, AE 09470-5695

Regardless of whether you provide this information, please be advised that Section 3414(a)(3) of Title 12 prohibits your institution or its officers, agents, or employees from disclosing to any person that these financial records have been sought or obtained.

A certification pursuant to Section 3403(b) indicating that AFOSI has complied with all requirements of the Right to Financial Privacy Act in making this request is attached. Under Section 3417(c) of Title 12, good faith reliance upon this certification relieves your institution and its employees or agents of any liability to your customer in connection with the disclosure of the requested financial records.

[redacted]

Attachment
Certification of Compliance

DEPARTMENT OF THE AIR FORCE
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

Special Agent
Air Force Office of Special Investigations
Headquarters

Dear [redacted]

I certify, pursuant to Title 12, United States Code, Section 3403(b), that the Special Procedures Provisions of the Right to Financial Privacy Act (codified in Section 3414 of Title 12) have been followed with regard to this request for the financial records of [redacted]

Regardless of whether you provide this information, please be advised that Section 3414(a)(3) of Title 12 prohibits your institution or its officers, agents, or employees from disclosing to any person that these financial records have been sought or that may have obtained.

Under Section 3417(c) of Title 12, good faith reliance upon this certifiention relieves your institution and its employees or agents of any liability to your customer in connection with the disclosure of the requested financial records.

[redacted]
Special Agent, USAF

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
HEADQUARTERS, 902D MILITARY INTELLIGENCE GROUP
FORT GEORGE G. MEADE, MARYLAND 20755-5910

[redacted]

To Whom It May Concern,

Under the provisions of the Right to Financial Privacy Act of 1978 (hereinafter the ACT), Title 12. U.S.C. 3401 *et seq*., the Department of the Army requests that your institution provide financial and credit information, to include any record information, concerning the individual identified below.

[redacted]
Account Number: [redacted]

This letter certifies that the Department of the Army has complied with the applicable provisions of the Act. Title 12. U.S.C. 3417 (c) specifies that good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records. The authorization to endorse this certificate has been delegated to me by the Secretary of the Army, contained in paragraph 2-10b(1), U.S. Army Regulation 190-6, Obtaining Information From Financial Institutions.

Title 12. U.S.C. 3414 (a) (3) prohibits your institution, employees, or agents of your institution from disclosing to any person that we have sought or obtained access to a customer's financial records.

In accordance with Title 12. U.S.C. 3415, we will reimburse your institution for such costs as are reasonably necessary and which have been directly incurred in searching for, reproducing, or transporting books, papers, records, or other data required or requested to be reproduced.

Thank you for your cooperation and assistance given to the Department of the Army, this command, and the Special Agent who presented this certificate.

Sincerely,

[redacted]
Colonel, U.S. Army
Commanding

[redacted]

Dear Custodian of Records:

Pursuant to Executive Order 12333 and the Right to Financial Privacy Act (Act), 12 United States Code §§3401, et seq., you are requested to provide the Naval Criminal Investigative Service with the name, address and financial records pertaining to the customer or accounts listed below:

Customer Name: if available

Address: if available

Date of birth: if available

Social Security: if available

Account numbers: if available

Requested period: if applicable (you may be required to pay for the records/search)

Pursuant to Section 3403(b) of the Act, I certify that NCIS has complied with the Special Procedures Provision contained in Section 3414. In accordance with Section 3417(c), your good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these records.

Please note that disclosing this request to the customer or others without a need to know in order to process this request may result in danger to the national security of the United States and interference with a counterterrorism or counterintelligence investigation. Accordingly, your company or its officers, employees, or agents are prohibited from disclosing to the customer that these records have been sought or obtained.

As a result of the sensitive nature of this request, please contact NCIS Special Agent _____ at (xxx) xxx-xxxx to make arrangements to provide the records. Thank you for your cooperation in this matter.

Sincerely,

Director, DD, AD for CI, AD for CT, or DAD for CI, or DAD for CT

Ser XX/U00XX
19Dec06

[redacted]

Dear [redacted]

I am a supervisory official designated by the General Counsel of the Department of the Navy to make the certification necessary under 15 U.S.C. § 1681v to compel disclosure of requested information and provide your agency with safe harbor.

In accordance with 15 U.S.C. § 1681v, I hereby certify that the information herein requested is necessary for an investigation of and/or analysis related to international terrorism.

Therefore, pursuant to Executive Order 12333 and Title 15 U.S.C. § 1681v of the Fair Credit Reporting Act you are directed to provide the Naval Criminal Investigative Service (NCIS) with a consumer report and all other information you possess in your files for the below listed consumers:

Consumer Name:

Date of Birth:

Social Security Number:

Address:

Please note that disclosing this request to the customer or others without a need to know in order to process this request may result in danger to the national security of the United States and interference with a counterterrorism or counterintelligence investigation. Accordingly, your company or its officers, employees, or agents are prohibited from disclosing to the customer that these records have been sought or obtained.

DEPARTMENT OF THE AIR FORCE
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

16 January 2007

MEMORANDUM FOR DUSD (CI&S)

FROM: HQ AFOSI

SUBJECT: National Security Letters (NSL) Calendar Year (CY) 2000 - present

1. Reference your email request, dtd 14 Jan 07, the following information is provided to answer the questions posed in reference -

A. NSLs (Total - [redacted]

[redacted]

Note 1 – AFOSI was transitioning from legacy system case management (CACTIS) to I2MS/CI2MS from 2000 to 2002. We are conducting checks at our file repository for NSLs in 2000 – 2002.

~~For Official Use Only~~

B. Prior to 2005, HQ AFOSI advised the field to leverage the FBI to submit NSLs for financial institutions. The justification for this is that we (DoD Investigative Components) cannot compel a financial institution to provide us with the records; however, NSL from the FBI require financial institutes to respond.

[redacted]

D. The signature authority for NSL sent from HQ AFOSI is the Commander (CC); however, the NSLs submitted in 2004 were signed by the Vice Commander (CV).

E. My point of contact in this matter is [redacted], HQ AFOSI/XOQ and he can be reached at [redacted]

/S/

[redacted]

[redacted]

[redacted]

[redacted]

~~From:~~ [redacted]
Sent: Monday, January 15, 2007 10:22 AM
To: [redacted]
Subject: FW: NSL (~~FOUO~~)

~~FOR OFFICIAL USE ONLY~~

[redacted]
Acting Director
Counterintelligence
DUSD (CI&S)
[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, January 15, 2007 9:22 AM
To: [redacted]

Subject: Re: NSL (~~FOUO~~)

Another NYT article this morning...

New York TimesJanuary 15, 2007
Cheney Defends Efforts To Obtain Financial Records By Mark Mazzetti Vice President Dick Cheney yesterday defended efforts by the Pentagon and the Central Intelligence Agency to obtain financial records of Americans suspected of terrorism or espionage, calling the practice a "perfectly legitimate activity" used partly to protect troops stationed on military bases in the United States.
But the chairman of the House Intelligence Committee expressed concern over the expansion of the military's domestic intelligence collection efforts and said his committee would investigate how the Pentagon was using its authority.
Appearing on "Fox News Sunday," Mr. Cheney said "national security letters" issued to banks and credit agencies were an essential tool for investigating terrorism cases in the United States.
He said the Pentagon had crossed no legal boundaries in issuing the letters independent of the Federal Bureau of Investigation.
"There's nothing wrong with it or illegal," Mr. Cheney said. "It doesn't violate people's civil rights. And if an institution that receives one of these national security letters disagrees with it, they're free to go to court to try to stop its execution."
Representative Silvestre Reyes, a Texas Democrat who is the new chairman of the House Intelligence Committee, said his panel would examine the matter. Mr. Reyes also indicated that he might renew efforts to pass a law requiring various agencies to get court approval before issuing national security letters.
"Any expansion by the department into intelligence collection, particularly on U.S. soil, is something our committee will thoroughly review," he said in a statement issued to the news media.
Since the Sept. 11 attacks, the Pentagon has issued hundreds of letters to American banks and other financial institutions seeking information about suspects in counterterrorism or counterespionage investigations.

Banks are not required to hand over the information, but Pentagon officials said that financial institutions usually complied.

The C.I.A. also uses the letters as an investigative tool, but issues them far less frequently than does the Pentagon, intelligence officials said.

The use of the national security letters by the Pentagon and the C.I.A. was first reported in The New York Times yesterday.

By law, the Pentagon and the C.I.A. are barred from any domestic law enforcement activities. But government officials said that their authority to issue the letters dated back several decades and was strengthened by the USA Patriot Act, an antiterrorism law passed in 2001.

Mr. Cheney said yesterday that the letters were valuable for protecting American forces stationed at hundreds of bases in the United States.

Since Sept. 11, the Pentagon has increased its domestic intelligence collection efforts to help ensure that American bases are protected from potential terrorist attacks.

The efforts have been criticized by civil liberties organizations, who say the Pentagon is using "force protection" to spy on Americans and collect information on groups like war protesters.

The American Civil Liberties Union said yesterday that it had "serious concerns" about the use of the letters by the Pentagon and the C.I.A., and it called for a Congressional investigation to examine the frequency and legal basis for the records demands, along with civil liberties safeguards in place.

"This country has a long tradition of rejecting the use of the C.I.A. and the Pentagon to spy on Americans, and rightfully so," said Caroline Fredrickson, director of the A.C.L.U.'s Washington office. "Today's published report that the Pentagon and C.I.A. have been relying on 'national security letters' to collect the financial records of Americans without judicial supervision or Congressional oversight raises a host of questions that need to be answered."

Pentagon officials said the financial documents obtained through the national security letters usually did not establish an individual's links to terrorism or espionage and had rarely led to criminal charges.

But officials said the records still had intelligence value, and the Pentagon plans within the next year to incorporate the records into a database at its Counterintelligence Field Activity office.

With the Democrats now in charge of both houses of Congress, the House and the Senate Intelligence Committees are planning hearings on various intelligence programs conducted by the Bush administration since Sept. 11, 2001.

At the top of the agenda are hearings on the National Security Agency's domestic surveillance program and the C.I.A.'s detention and interrogation of terrorism suspects.

Mr. Reyes indicated yesterday that the military's domestic collection efforts could also be a priority for his committee.

"We want our intelligence professionals to have strong tools that will enable them to interrupt the planning process of our enemies and to stop attacks against our country," his statement said.

"But in doing so, we also want those tools to comply fully with the law and the Constitution."

[redacted]
Office of the Under Secretary of Defense
(Intelligence)
[redacted]

-----Original Message-----
From: [redacted]
To: [redacted]

[redacted]

[redacted]
Sent: Sun Jan 14 16:17:11 2007
Subject: RE: NSL ~~(FOUO)~~

[redacted]

I am in the office on Sunday responding to your inquiry. Unfortunately, and as expected, I don't have all the answers. I am providing as much as I can in that I will be out of the office until Friday. We will provide additional information next week, but as you requested, I am providing the info I have now, rather than wait to compile it all. Prior to the USA PATRIOT Act, most, if not all, NSLs were requested through the FBI, even though we had the authority under the RTFP.

CI
2007 (as of 12 Jan 07) - [redacted]
2006 - [redacted]
2005 -
2004 -
2003 -
2002-
2001 - to be provided later
2000 - to be provided later

CT
2006 [redacted]
2005
2001-2004 - to be provided later; Prior to 9/11 CT was handled by the CI directorate

NSLs issued pursuant to 12 USC 3414 and 15 USC 1681v may be signed by the Director, Deputy Directors, Executive Assistant Director (EAD) for CI, EAD for CT, Deputy Assistant Director (DAD) for CI, or DAD for CT.
The DADs are GS-15s and the others with authority to sign are SES. A request issued under 50 USC 436 may be signed by the Director, DD, EAD for CI, or EAD for CT, as delegated by the OGC of DoN. All letters require a legal review to ensure compliance with the statue prior to signature:

As far as I know, the credit agencies have complied with all of our requests. Initially, we had to explain who NCIS is and how we fall within the statute, but once we provided those answers, they have complied. Only two financial institutions that I can recall did not provide records in response to our requests.

Letters have been issued in cases involving AD, civilians, and contractors. All cases involving civilians and contractors are coordinated with FBI. We will need additional time to identify the break down of the individual subjects.

Please advise if you need to discuss further. NCIS will provide additional information next week.

V/r
[redacted]

[redacted]
National Security Law Unit
Naval Criminal Investigative Service
[redacted]

-----Original Message-----
From: [redacted]
Sent: Sunday, January 14, 2007 12:20
To: [redacted]

[redacted]

Subject: NSL ~~(FOUO)~~

~~FOR OFFICIAL USE ONLY~~
Happy Sunday to everyone,

Probably by now you are aware of the NY Times Article. In response to the article, the Acting USD(I) [redacted] has asked for information by Tuesday 1200. In discussion with the Acting DUSD, [redacted] this office will take the lead on gathering the information requested by [redacted] Please provide information 1000 hrs Tuesday 16 Jan. Send to myself and [redacted]

A. [redacted] has requested:

I must have an initial point paper by 1200 Tuesday, 16 Jan that addresses the following questions:

* How many of these letters has been sent out?
  * From 2000 to present
  * Number per year
  * CI or CT
    *. For Army: For CI/CT Understand your challenge of researching each case.

If you can't make suspense, let us know the soonest you can.

* How much of an increase has there been over time?
* What are the processes that governs how the letters are sent?
* What regulations outline these processes? When were the regs last reviewed? Who reviewed?
* Who must sign off on the letters before they go out? Does CIFA control these? Or can individual Services or components send them out?

Please do not wait until "all" the information is in hand--if we do, we'll wait forever. I know that, with time, we can build a more complete picture--this will be an iterative process. But I need some facts now.

I emphasize: Make it short. Make it quick. Make it factual. Do not waste your time and mine with arguments about justification, value to investigations, or finger-pointing.

Let me have soonest what is on hand. Then we can dig back to look at trends.

B. In response to the NY Times article please provide the following by 1200 Wednesday 17 Jan. Or let us know when you can get us this information.

* How many letters were turned down/information not provided.

* Were the letters issued on Uniformed personnel/government civilian/contractors/Foreign Nationals. Break down per year back to 2000.

* Army: Were letters Used in the [redacted] case?

<<DoD NSL Fact Sheet (13 Jan 07).doc>> <<NYT Article>>

v/r

[redacted]

[redacted]
Acting Director
Counterintelligence
DUSD (CI&S)
[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

~~FOR OFFICIAL USE ONLY~~

[redacted]

From: [redacted]
Sent: Friday, January 19, 2007 5:00 PM
To: [redacted]
Subject: NSL briefs ~~(FOUO)~~

~~FOR OFFICIAL USE ONLY~~
[redacted]

Just aheads up. For future Hill briefs, there is a possibility that a NCIS agent type will be asked to be the NCIS rep. We can chat why on Monday.

[redacted]
Acting Director
Counterintelligence
DUSD (CI&S)
[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

[redacted]

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

NCIS General Administrative Message J-0002, subject: USA PATRIOT Act dated 26 Feb 2003

1. The USA PATRIOT Act expands certain National Security Letter (NSL) authorities to the Director, Naval Criminal Investigative Service or his designee. Previously only the Director or Deputy Director of the Federal Bureau of Investigation (FBI) could issue NSLs.

2. The authority to issue an NSL is found in three statutes: The Right to Financial Privacy Act (RTFPA), The Fair Credit Reporting Act (FCRA), and the Electronic Communications Privacy Act (ECPA). All three statutes contain a provision that prohibits disclosing the request for records to anyone except those with a need to know to process the request. The NSLs are useful because they may establish patterns of a target, identify acquaintances or relationships of a target, identify unexplainable wealth, or develop further leads.

3. Under the RTFPA (12 USC 3414), an NSL may be submitted to any financial institution in the United States or its territories. Financial institutions include banks, savings banks, card issuers, loan companies, savings associations, credit unions, and consumer finance institutions. An NSL may be issued in all cases where the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, to include espionage. The customer whose records are sought need not be the target of the investigation. In other words, if the target of a terrorism investigation is Mohammed Atta, an NSL may be issued for the records of Atta, as well as others, if those records are relevant to the investigation of Atta. The responsive records are all records the financial institution maintains about that customer, to include IRS records. For example, a mortgage company may have IRS records, tax returns, employer information, payment history, past credit reports, and information on cosigners. The records from a financial institution may show the flow of money into and out of accounts. The records obtained may also establish relationships between targets.

4. The FBI or NCIS may issue an NSL pursuant to the RTFPA. Specifically, within the FBI, the Director, his designee not lower than Deputy Assistant Director (DAD) at FBI Headquarters (HQTRS), or a Special Agent in Charge (SAC) at a field office (FO) may request and compel disclosure of records from a financial institution. Within NCIS, the Director, Deputy Director, Assistant Director for Counterintelligence, Assistant Director for Counterterrorism, Deputy Assistant Director for Counterintelligence and Deputy Assistant Director for Counterterrorism may request the disclosure. Whereas the FBI may compel disclosure of the records, NCIS may only request the disclosure.

5. Two sections of the FCRA (15 USC 1681) provide for the issuance of NSLs. Both sections, Disclosure to FBI for counterintelligence purposes (15 USC 1681u) and Disclosures to governmental agencies for counterterrorism purposes (15 USC 1681v) apply to credit reporting agencies, such as TRW and Equifax. Both sections require the credit reporting agency, upon receipt of an NSL, to provide their records containing names and addresses of all financial institutions at which a consumer maintains or has maintained an account, present and former addresses of the consumer, and names and addresses of present and former employers of the consumer. These records may be useful to identify subsequent financial institutions to which an

NSL under the RTFPA should be issued and to identify past addresses of a target. The consumer need not be the target of the investigation.

6. Pursuant to 15 USC 1681v, the Secretary of the Navy, the General Counsel of the Department of the Navy (GC), or a designated supervisory official may issue an NSL when the records sought are necessary for an investigation or analysis related to international terrorism, and not clandestine intelligence activity. On December 18, 2002, the GC designated the NCIS Director, Deputy Director, Assistant Director for Counterintelligence, Assistant Director for Counterterrorism, Deputy Assistant Director for Counterintelligence and Deputy Assistant Director for Counterterrorism as supervisory officials able to issue an NSL pursuant to 15 USC 1681v.

7. Pursuant to 15 USC 1681u, when the information sought is for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, only the Director, FBI, his designee not lower than DAD at FBI HQTRS, or a SAC at a FBI FO can issue an NSL. NCIS does not have the authority under 15 USC 1681u to issue an NSL.

8. ECPA also contains a section for issuing NSLs. The section titled, Counterintelligence access to telephone toll and transactional records (18 USC 2709), provides for the Director, FBI, his designee not lower than DAD at FBI HQTRS, or a SAC at a FBI FO to issue an NSL to a wire communications provider, such as a telephone company, or an electronic communications provider, such as an Internet service provider (ISP). In response to an NSL, the provider shall provide subscriber information to include the name and address on the account, length of the account, and local and long distance records. This section applies when the records sought are relevant to an authorized investigation of international terrorism or clandestine intelligence activities. The subscriber need not be the target of the investigation. Only the FBI has the authority to issue an NSL under ECPA.

9. Another valuable tool, although not an NSL, is governed by Requests by authorized investigative agencies, 50 USC 436. This section authorizes NCIS to request from financial agencies, financial institutions, consumer reporting agencies, and commercial entities with records pertaining to travel outside the U.S., all financial records and information and records pertaining to travel outside the U.S. The request must contain a written certification signed by the NCIS Director, Deputy Director, Assistant Director for Counterintelligence, or Assistant Director for Counterterrorism. The certification must state that the person concerned is or was an employee of the Executive Branch, which includes persons on active duty and DoD civilians; the person signed a consent form for such records; and the person has or had access to classified material within the last three years. The request may be pursued only if reasonable grounds exist to believe that the person is or may be disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power; the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information; or the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or agent of a foreign power.

10. Although NCIS has the authority to issue an NSL in many cases, we should do so only in those cases in which NCIS exercises primary jurisdiction or the FBI has deferred jurisdiction. Case agents must submit a draft NSL and the supporting documentation to the desk officer when requesting NCIS to issue an NSL. The desk officer will provide the draft NSL to an attorney in the National Security Law Unit (NSLU) for a legal review before submitting the NSL for signature. The case agent must contact the anticipated recipient of the NSL before the NSL is issued.