



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.

A handwritten signature in black ink, appearing to read "Paul Wolfowitz", with a horizontal line extending to the right from the end of the signature.

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. XXXXXXXXXXXX
Chief Teller [as appropriate]
First National Bank
Anywhere, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXXXX

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. XXXXXXXXXXXX
President (as appropriate)
City National Bank and Trust Company
Anytown, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXXXXXXXX

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. XXXXXXXXXXXX
Manager
Army Federal Credit Union
Fort Anywhere, VA 00000-0000

Dear Mr./Mrs. XXXXXXXXXXXX

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.



[Federal Register](#) [Codification](#) [Executive Order](#) [Executive Orders](#)

CODIFICATION

[Print Page](#)

[E-mail Page](#)

[Bookmark Page](#)

[About the Codification](#)

[Alphabetical Index](#)

[Chapter Index](#)

[Numeric Index](#)

Search the Codification

[Go to the Executive Orders Main Page](#)

Executive Order 12333--United States intelligence activities

Source: The provisions of Executive Order 12333 of Dec. 4, 1981, appear at 46 FR CFR, 1981 Comp., p. 200, unless otherwise noted.

Table of Contents

Preamble

Part 1. Goals, Direction, Duties, and Responsibilities With Respect to the National 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 Department 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 of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by the authority vested in me by the Constitution and statutes of the United States of America, including the National Security Act of 1947, as amended, and as President of the United States of America, in order to provide for the effective conduct of United States intelligence 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 Intelligence

1.1 Goals. The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies 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 with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.

(c) Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons.

(d) To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive 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 Security Act of 1947.

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 Executive Branch entity that provides review of, guidance for and direction to the conduct of national foreign intelligence, counterintelligence, and special activities, and attend to such activities and programs.

(b) *Committees.* The NSC shall establish such committees as may be necessary to carry out its functions and responsibilities under this Order. The NSC, or a committee established by the NSC, shall consider and submit to the President a policy recommendation, including all recommendations, for each special activity and shall review proposals for other sensitive intelligence operations.

1.3 *National Foreign Intelligence Advisory Groups.*

(a) *Establishment and Duties.* The Director of Central Intelligence shall establish such 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 Intelligence.

(b) *Membership.* Advisory groups established pursuant to this section shall be chaired by the Director of Central Intelligence or his designated representative and shall consist of representatives from organizations within the Intelligence Community and from departments or agencies containing such organizations, as designated by the Director of Central Intelligence. Groups for consideration of substantive intelligence matters will include representatives of organizations involved in the collection, processing and analysis of intelligence. A senior representative of the Secretary of Commerce, the Attorney General, the Assistant to the President for National Security Affairs, and the Office of the Secretary of Defense shall be invited to participate in any group which deals with other than such intelligence matters.

1.4 *The Intelligence Community.* The agencies within the Intelligence Community shall conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States, including:

- (a) Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;
- (b) Production and dissemination of intelligence;
- (c) Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;
- (d) Special activities;

- (e) Administrative and support activities within the United States and abroad necessary for 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 responsibilities prescribed by law, the Director of Central Intelligence shall be responsible directly to the President and the NSC and shall:

- (a) Act as the primary adviser to the President and the NSC on national foreign intelligence 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 ensure the capabilities for responding to expected future needs for national foreign intelligence;
- (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 arrangements 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 for criminal narcotics intelligence activities abroad to ensure that these activities are coordinated with foreign intelligence programs;
- (g) Ensure the establishment by the Intelligence Community of common security standards for managing and handling foreign intelligence systems, information, and products;
- (h) Ensure that programs are developed which protect intelligence sources, methods, and analytical procedures;
- (i) Establish uniform criteria for the determination of relative priorities for the transmission of critical national foreign intelligence, and advise the Secretary of Defense concerning communications requirements of the Intelligence Community for the transmission of intelligence;
- (j) Establish appropriate staffs, committees, or other advisory groups to assist in the execution of the Director's responsibilities;
- (k) Have full responsibility for production and dissemination of national foreign intelligence and authority to levy analytic tasks on departmental intelligence production organizations, in consultation with those organizations, ensuring that appropriate mechanisms for coordination and analysis are developed so that diverse points of view are considered fully and different judgments within the Intelligence Community are brought to the attention of national policymakers;
- (l) Ensure the timely exploitation and dissemination of data gathered by national foreign intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government entities and military commands;
- (m) Establish mechanisms which translate national foreign intelligence objectives and priorities approved by the NSC into specific guidance for the Intelligence Community.

conflicts in tasking priority, provide to departments and agencies having informatic collection capabilities that are not part of the National Foreign Intelligence Program 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 agencies concerned, the consolidated National Foreign Intelligence Program budget, and present the President and the Congress;

(o) Review and approve all requests for reprogramming National Foreign Intelligence Program funds, in accordance with guidelines established by the Office of Management and Budget;

(p) Monitor National Foreign Intelligence Program implementation, and, as necessary, conduct program and performance audits and evaluations;

(q) Together with the Secretary of Defense, ensure that there is no unnecessary overlap between national foreign intelligence programs and Department of Defense intelligence programs consistent with the requirement to develop competitive analysis, and present and obtain from the Secretary of Defense all information necessary for this purpose;

(r) In accordance with law and relevant procedures approved by the Attorney General under this Order, give the heads of the departments and agencies access to all intelligence information developed by the CIA or the staff elements of the Director of Central Intelligence, consistent with the national intelligence needs of the departments and agencies; and

(s) Facilitate the use of national foreign intelligence products by Congress in a secure manner.

1.6 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies

(a) The heads of all Executive Branch departments and agencies shall, in accordance with law and relevant procedures approved by the Attorney General under this Order, give the Director of Central Intelligence access to all information relevant to the national intelligence needs of the United States, and shall give due consideration to the requests from the Director of Central Intelligence for appropriate support for the Intelligence Community.

(b) The heads of departments and agencies involved in the National Foreign Intelligence Program shall ensure timely development and submission to the Director of Central Intelligence by the program managers and heads of component activities of proposed 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 provided in a timely and responsive manner, all information necessary to perform the Director's program and budget responsibilities.

(c) The heads of departments and agencies involved in the National Foreign Intelligence Program may appeal to the President decisions by the Director of Central Intelligence regarding budget or reprogramming matters of the National Foreign Intelligence Program.

1.7 Senior Officials of the Intelligence Community. The heads of departments and agencies and with organizations in the Intelligence Community or the heads of such organizations, where appropriate, shall:

(a) Report to the Attorney General possible violations of federal criminal laws by employees and of specified federal criminal laws by any other person as provided in procedures

upon by the Attorney General and the head of the department or agency concerned in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(b) In any case involving serious or continuing breaches of security, recommend to the 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 applicable law and procedures approved by the Attorney General under this Order, the information required for the performance of their respective duties;

(d) Report to the Intelligence Oversight Board, and keep the Director of Central Intelligence appropriately informed, concerning any intelligence activities of their organizations which they have reason to believe may be unlawful or contrary to Executive order or Presidential directive;

(e) Protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the Director of Central Intelligence;

(f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the Director of Central Intelligence;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of intelligence resulting from criminal narcotic intelligence activities abroad if their departments, agencies, or organizations have intelligence responsibilities for foreign or domestic narcotics production and trafficking;

(h) Instruct their employees to cooperate fully with the Intelligence Oversight Board;

(i) Ensure that the Inspectors General and General Counsels for their organizations have 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 be limited to the intelligence functions set out below. As authorized by this Order; the National Security Act of 1947, as amended; the CIA Act of 1949, as amended; appropriate directives; and applicable law, the CIA shall:

(a) Collect, produce and disseminate foreign intelligence and counterintelligence, and information not otherwise obtainable. The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(b) Collect, produce and disseminate intelligence on foreign aspects of narcotics production and trafficking;

(c) Conduct counterintelligence activities outside the United States and, without performing any internal security functions, conduct counterintelligence activities within the United States in coordination with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(d) Coordinate counterintelligence activities and the collection of information not otherwise obtainable when conducted outside the United States by other departments and agencies;

(e) Conduct special activities approved by the President. No agency except the CIA or the Armed Forces of the United States in time of war declared by Congress or during a national emergency as covered by a report from the President to the Congress under the War Powers Resolution (50 U.S.C. 1541) may conduct any special activity unless the President determines that such activity is more likely to achieve a particular objective;

- (f) Conduct services of common concern for the Intelligence Community as directed by the National Security Council (NSC);
- (g) Carry out or contract for research, development and procurement of technical equipment and devices relating to authorized functions;
- (h) Protect the security of its installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the CIA as are necessary; and
- (i) Conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (a) through (h) 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 policy concerns required for the execution of the Secretary's responsibilities;
- (c) Disseminate, as appropriate, reports received from United States diplomatic posts and consulates;
- (d) Transmit reporting requirements of the Intelligence Community to the Chiefs of United States Missions abroad; and
- (e) Support Chiefs of Missions in discharging their statutory responsibilities for direct 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 foreign economic information;
- (c) Produce and disseminate foreign intelligence relating to United States economic interests required for the execution of the Secretary's responsibilities; and
- (d) Conduct, through the United States Secret Service, activities to determine the effectiveness and capability of surveillance equipment being used against the President of the United States, the Executive Office of the President, and, as authorized by the Secretary of the Treasury or the President, other Secret Service protectees and United States officials. Information shall be acquired intentionally through such activities except to protect the source of such surveillance, and those activities shall be conducted pursuant to procedures established 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 the Director of Central Intelligence;
- (b) Collect, produce and disseminate military and military-related foreign intelligence and 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 operations outside the United States in coordination with the CIA, and within the United States in coordination with the FBI pursuant to procedures agreed upon by the Secretary of Defense.

and the Attorney General;

- (e) Conduct, as the executive agent of the United States Government, signals intelligence and communications security activities, except as otherwise directed by the NSC;
- (f) Provide for the timely transmission of critical intelligence, as defined by the Director of Central Intelligence, within the United States Government;
- (g) Carry out or contract for research, development and procurement of technical intelligence 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 of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;
- (i) Establish and maintain military intelligence relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations, and ensure that such relationships and programs are in accordance with policies formulated by the Director of Central Intelligence;
- (j) Direct, operate, control and provide fiscal management for the National Security Agency and for defense and military intelligence and national reconnaissance entities; and
- (k) Conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (a) through (j).

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 perform the following:

- (a) *Defense Intelligence Agency*, whose responsibilities shall include:
 - (1) Collection, production, or, through tasking and coordination, provision of intelligence and military-related intelligence for the Secretary of Defense, the Joint Chiefs of Staff, other Defense components, and, as appropriate, non-Defense agencies;
 - (2) Collection and provision of military intelligence for national foreign intelligence and counterintelligence products;
 - (3) Coordination of all Department of Defense intelligence collection requirements;
 - (4) Management of the Defense Attache system; and
 - (5) Provision of foreign intelligence and counterintelligence staff support as required by the Joint Chiefs of Staff.
- (b) *National Security Agency*, whose responsibilities shall include:
 - (1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over communications operations that are conducted through other elements of the Intelligence Community. 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, including 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 intelligence purposes in accordance with guidance from the Director of Central Intelligence.

- (4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;
- (5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military, in accordance with guidance from the Director of Central Intelligence;
- (6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;
- (7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national communications systems, these systems will be tasked within existing guidance from the Director of Central Intelligence;
- (8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;
- (9) Conduct of research and development to meet the needs of the United States for signals intelligence and communications security;
- (10) Protection of the security of its installations, activities, property, information, and personnel by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the agency as are necessary;
- (11) Prescribing, within its field of authorized operations, security regulations and operating practices, including the transmission, handling and distribution of intelligence and communications security material within and among the elements under control of the Director of the NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;
- (12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and
- (13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections 1 through 12 above, including procurement.

(c) *Offices for the collection of specialized intelligence through reconnaissance programs*, whose responsibilities shall include:

- (1) Carrying out consolidated reconnaissance programs for specialized intelligence;
- (2) Responding to tasking in accordance with procedures established by the Director of Central Intelligence; and
- (3) Delegating authority to the various departments and agencies for research, development, procurement, and operation of designated means of collection.

(d) *The foreign intelligence and counterintelligence elements of the Army, Navy, Air Force, 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 of narcotics production and trafficking. When collection is conducted in response to a specific intelligence requirement, the collection shall be conducted in accordance with the guidance of the Director of Central Intelligence.

national foreign intelligence requirements, it will be conducted in accordance with the guidance from the Director of Central Intelligence. Collection of national foreign intelligence, not otherwise obtainable, outside the United States shall be coordinated with the CIA, and such collection within the United States shall be coordinated with the FBI;

(2) Conduct of counterintelligence activities outside the United States in coordination with the CIA, and within the United States in coordination with the FBI; and

(3) Monitoring of the development, procurement and management of tactical intelligence systems and equipment and conducting related research, development 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 offices are used for intelligence purposes, the provisions of Part 2 of this Order shall apply to those 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 respect to foreign energy matters;

(b) Produce and disseminate foreign intelligence necessary for the Secretary's responsibilities;

(c) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(d) Provide expert technical, analytical and research capability to other agencies within the Intelligence Community.

1.14 *The Federal Bureau of Investigation.* Under the supervision of the Attorney General pursuant to such regulations as the Attorney General may establish, the Director of the FBI shall:

(a) Within the United States conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community. When a counterintelligence activity of the FBI involves military or civilian personnel of the Department of Defense, the FBI shall coordinate with the Department of Defense;

(b) Conduct counterintelligence activities outside the United States in coordination with the CIA as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(c) Conduct within the United States, when requested by officials of the Intelligence Community designated by the President, activities undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the Intelligence Community, or, when requested by the Director of the National Security Agency 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 equipment and devices relating to the functions authorized above.

Part 2

Conduct of Intelligence Activities

2.1Need. Accurate and timely information about the capabilities, intentions and actions of 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 and responsible manner that is consistent with the Constitution and applicable law and of the principles upon which the United States was founded.

2.2Purpose. This Order is intended to enhance human and technical collection techniques especially those undertaken abroad, and the acquisition of significant foreign intelligence well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Set forth below are certain general principles that, in part and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. No part of this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3Collection of Information. Agencies within the Intelligence Community are authorized to 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 Order. Those procedures shall permit collection, retention and dissemination of the following information:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection of information concerning United States persons of foreign intelligence not otherwise obtainable shall be undertaken only if, or when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agency may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
- (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;
- (d) Information needed to protect the safety of any persons or organizations, including those 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 may collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for such employment or contracting;
- (f) Information concerning persons who are reasonably believed to be potential sources of information for the purpose of determining their suitability or credibility;
- (g) Information arising out of a lawful personnel, physical or communications security investigation;

investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United persons;

(i) Incidentally obtained information that may indicate involvement in activities that violate federal, state, local or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, agencies within the Intelligence Community may disseminate information that is more than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

2.4 Collection Techniques. Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, monitoring devices unless they are in accordance with procedures established by the agency concerned and approved by the Attorney General. Such procedures shall respect constitutional and other legal rights and limit use of such information to lawful government purposes. These procedures shall not authorize:

(a) The CIA to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic signals;

(b) Unconsented physical searches in the United States by agencies other than the CIA, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes authorized by a military commander empowered to approve physical search for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in possession.

(c) Physical surveillance of a United States person in the United States by agencies other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a nonintelligence agency or a military service.

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that such information is relevant to the national security.

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 be conducted in accordance with that Act, as well as this Order.

2.6 Assistance to Law Enforcement Authorities. Agencies within the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting employees, information, property and facilities of any agency within the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement 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 personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in advance by the General Counsel of the providing agency; and

(d) Render any other assistance and cooperation to law enforcement authorities not otherwise precluded by applicable law.

2.7 Contracting. Agencies within the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with private companies or 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 authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of agencies within the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any agency within the Intelligence Community without disclosing his intelligence affiliation to appropriate officials of the organization in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such participation shall be authorized only if it is necessary to achieving lawful purposes as determined by the agency head or designee. No such 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 United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 Human Experimentation. No agency within the Intelligence Community shall enter into a contract for or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 *Prohibition on Assassination.* No person employed by or acting on behalf of the States Government shall engage in, or conspire to engage in, assassination.

2.12 *Indirect Participation.* No agency of the Intelligence Community shall participate in, or 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 Central Intelligence and the heads of other departments, agencies, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibility for oversight of intelligence activities shall be as provided in title 50, United States Code 413. The requirements of section 662 of the Foreign Assistance Act of 1961, as amended (50 U.S.C. 2422), and section 501 of the National Security Act of 1947, as amended (50 U.S.C. 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 the Director of Central Intelligence shall issue such appropriate directives and procedures necessary to implement this Order. Heads of agencies within the Intelligence Community shall issue appropriate supplementary directives and procedures consistent with this Order. The Attorney General shall provide a statement of reasons for not approving any procedure 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 and the Attorney General are unable to reach agreement on other than constitutional or 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 accordance with existing procedures or requirements established under Executive Order No. 12036. Procedures required by this Order shall be established as expeditiously as possible. Existing procedures promulgated pursuant to this Order shall be made available to the congressional 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 protect against espionage, other intelligence activities, sabotage, or assassinations conducted on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

(b) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, or 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 finding equipment solely to determine the location of a transmitter.

(c) *Employee* means a person employed by, assigned to or acting for an agency with

Intelligence Community.

(d) *Foreign intelligence* means information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

(e) *Intelligence activities* means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to this Order.

(f) *Intelligence Community and agencies within the Intelligence Community* refer to the 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 special 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 Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the 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, the composition shall be subject to review by the National Security Council and modified by the President:

- (1) The programs of the CIA;
- (2) The Consolidated Cryptologic Program, the General Defense Intelligence Program and the programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance, except such as the Director of Central Intelligence and the Secretary of Defense agree shall be excluded;
- (3) Other programs of agencies within the Intelligence Community designated by the Director of Central Intelligence and the head of the department or by the 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 conducting of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program.

(h) *Special activities* means activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of intelligence 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 or production of intelligence or related support functions.

(i) *United States person* means a United States citizen, an alien known by the intelligence 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 and 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 provided 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, entitled "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

--	--	--	--

CRS-5

NSL Statute	18 U.S.C. 2709	12 U.S.C. 3414	15 U.S.C. 1681a	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/ 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

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: [REDACTED]
- Percentage: [REDACTED]

❖ **AF Office of Special Investigations (OSI) (FY 2000-Present):**

- Total No. of Investigations: [REDACTED]
- Total No. Using NSLs: [REDACTED]
- Percentage: [REDACTED]

❖ **Naval Criminal Investigative Service (NCIS) (FY 2000-Present):**

- Total No. of Investigations: [REDACTED]
- Total No. Using NSLs: [REDACTED]
- Percentage: [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]

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: [REDACTED]

❖ **AF OSI [See Footnotes 4 & 5]:**

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

❖ **NCIS:⁶**

- Total: [REDACTED]
- 15 USC § 1681v [REDACTED]
- 12 USC § 3414: [REDACTED]
- 50 USC § 436: [REDACTED]

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.

THIS PAGE IS UNCLASSIFIED WHEN SEPARATED FROM TAB D

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

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

Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

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 LAW 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

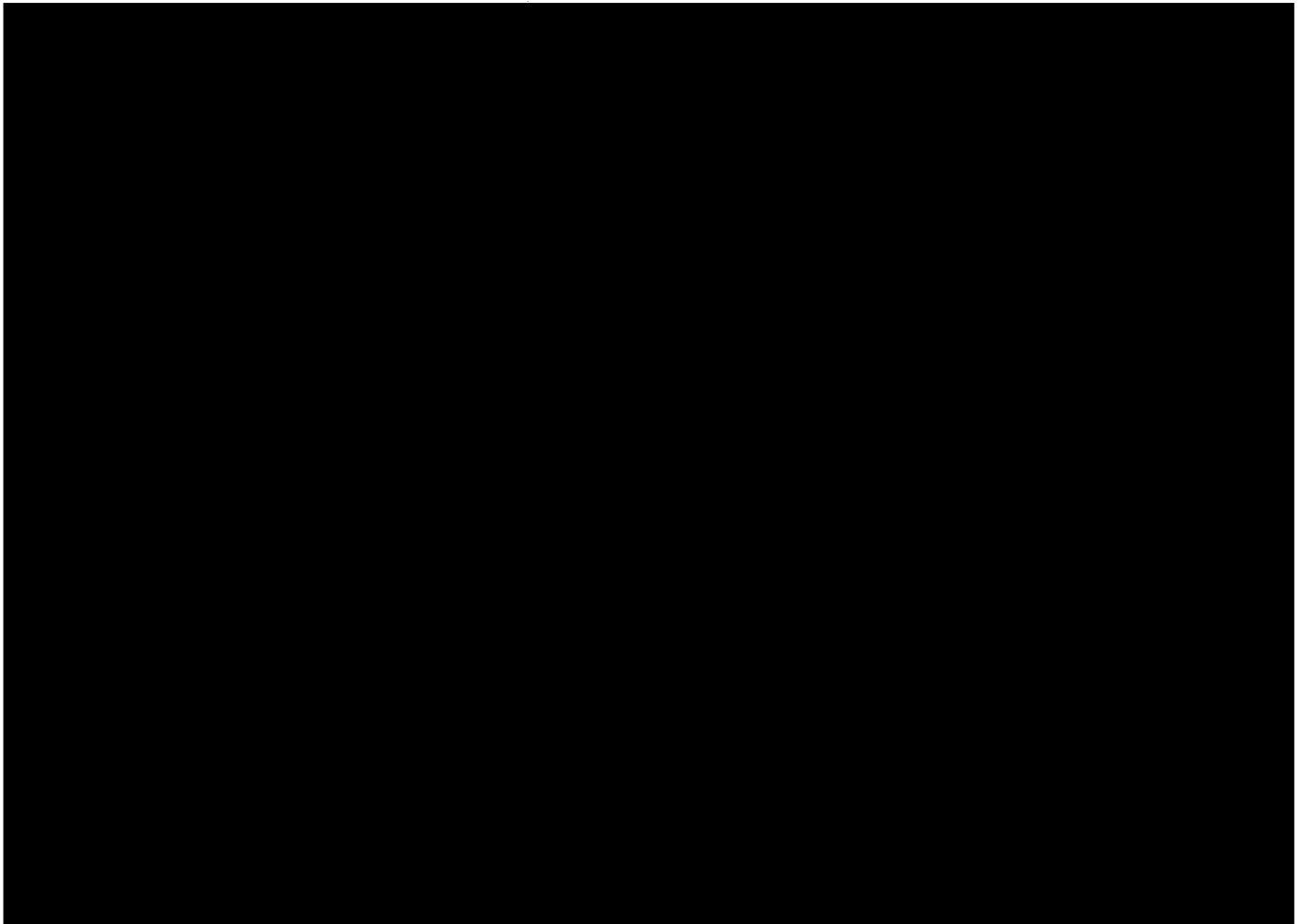
Army CI Investigative Handbook (final draft)
Financial Checks Exerpt

(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);

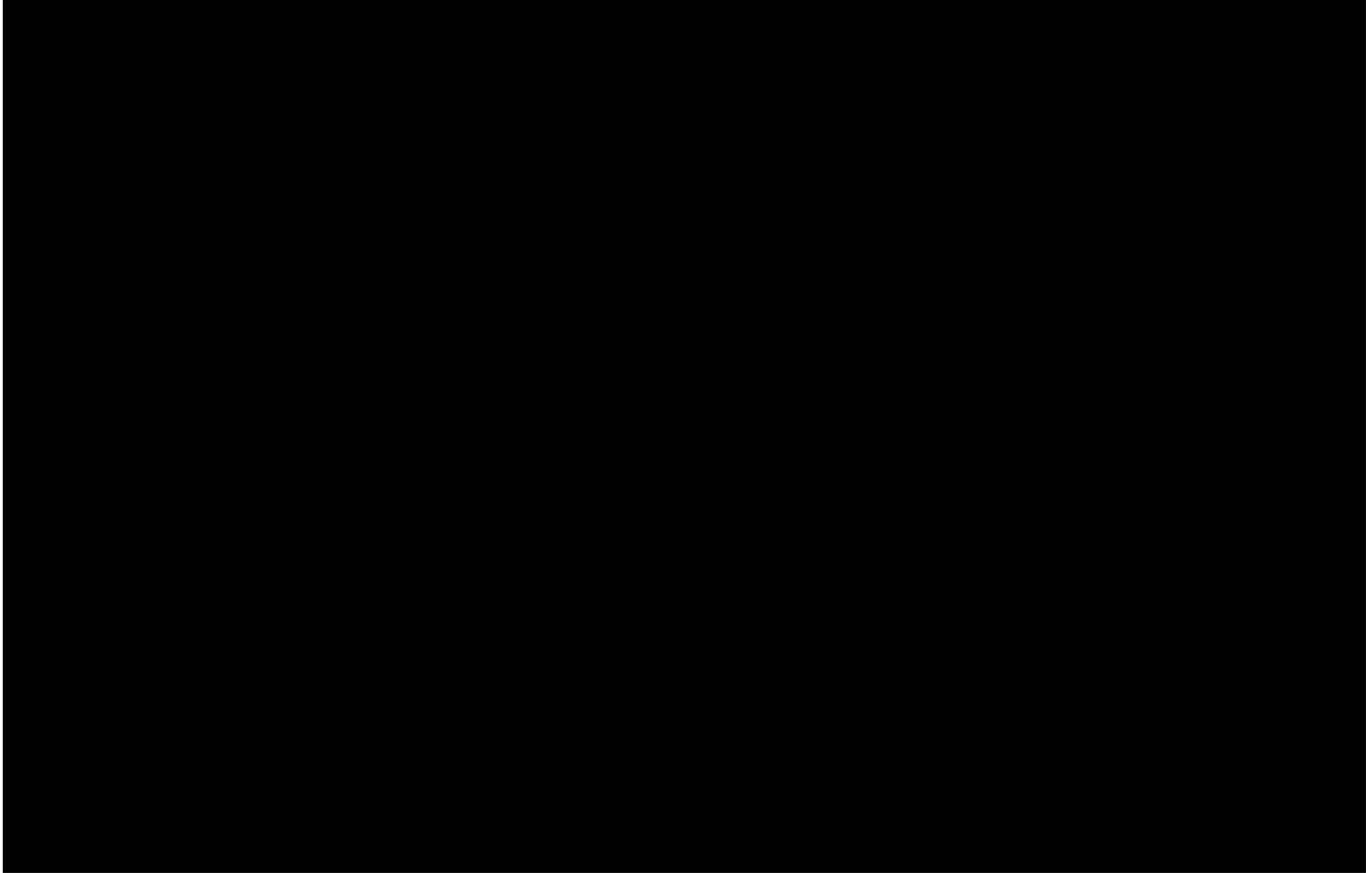
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or

(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.



Army CI Investigative Handbook (final draft)
Financial Checks Exerpt



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]
[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.

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 those 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]
Special Agent, USAF



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
HEADQUARTERS, 902D MILITARY INTELLIGENCE GROUP
FORT GEORGE G. MEADE, MARYLAND 20755-6910

[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



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

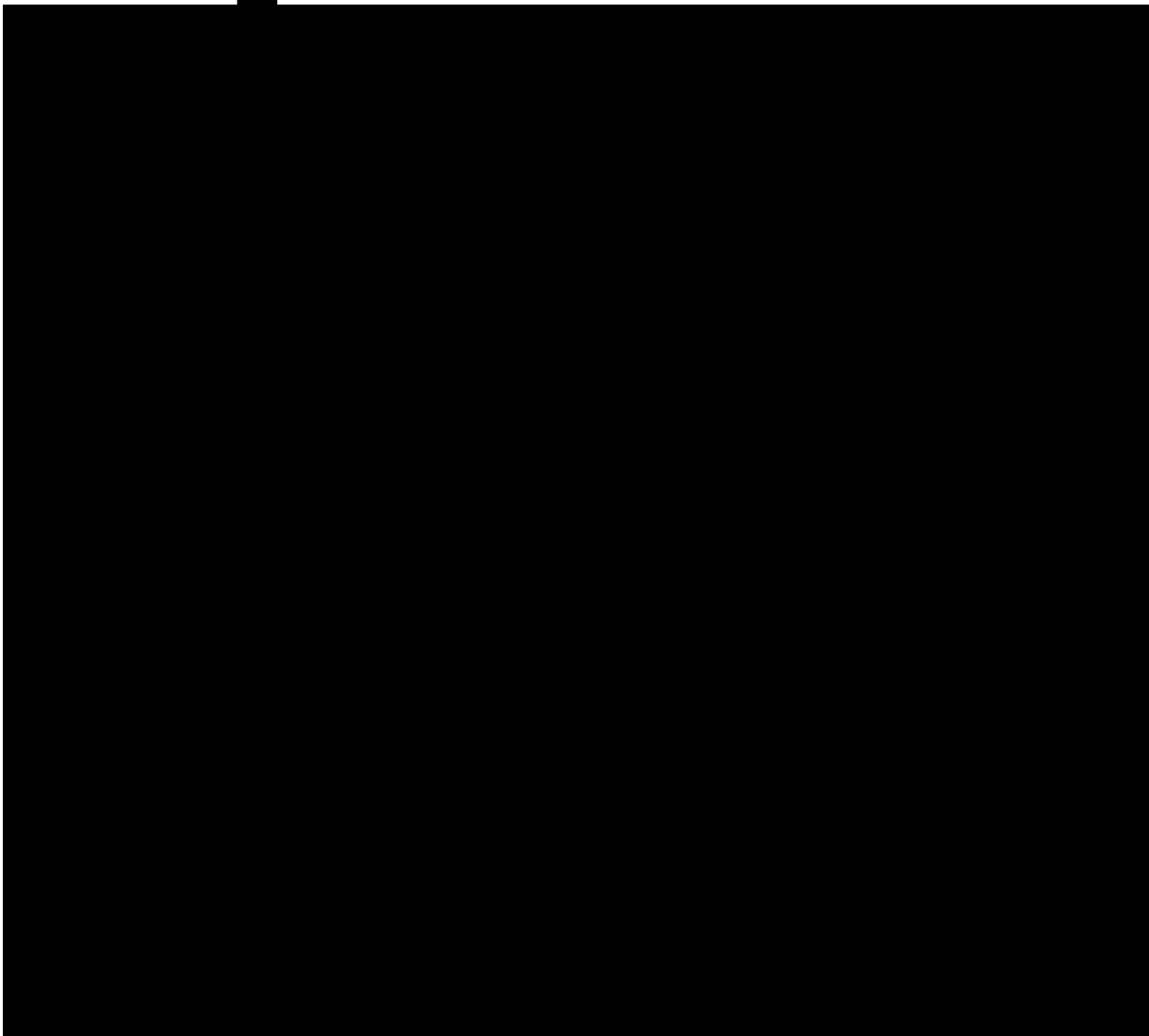
MEMORANDUM FOR DUSD (CI&S)

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 -

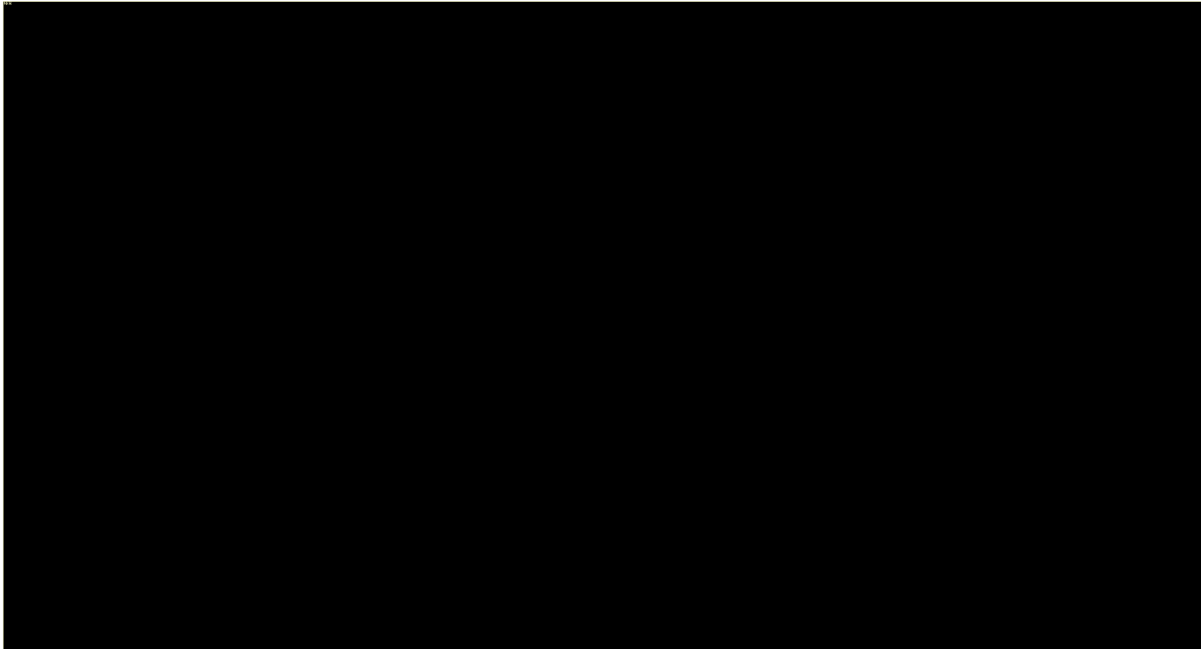
A. NSLs (Total - [REDACTED])



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~~

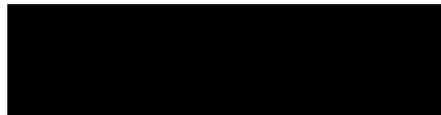
B. Prior to 2005, HQ AFOSI advised the field to leverage the FBI to submit NSLs for financial institutions. The justification for this is that we (DoD Investigative Components) cannot compel a financial institution to provide us with the records; however, NSL from the FBI require financial institutes to respond.

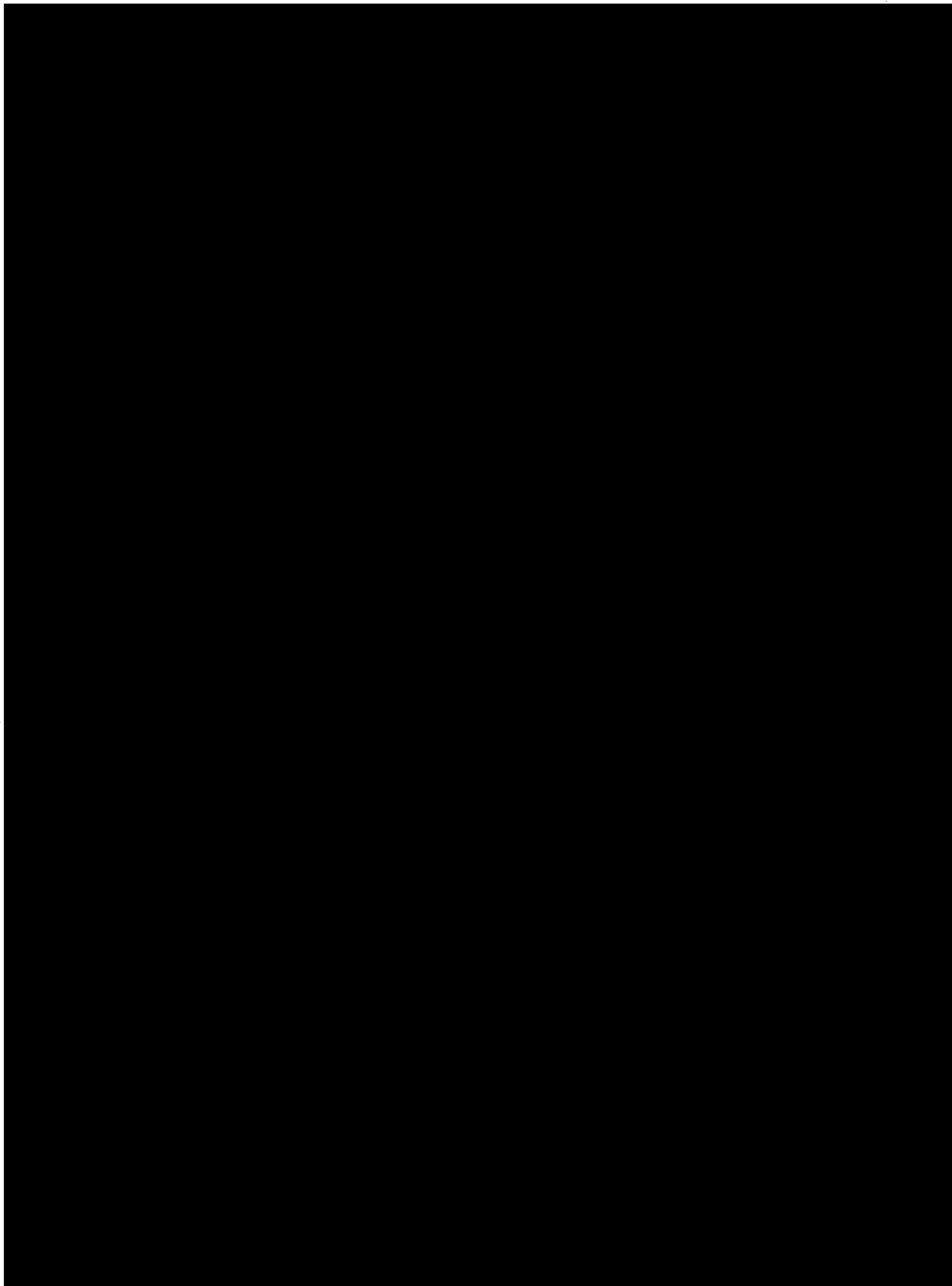


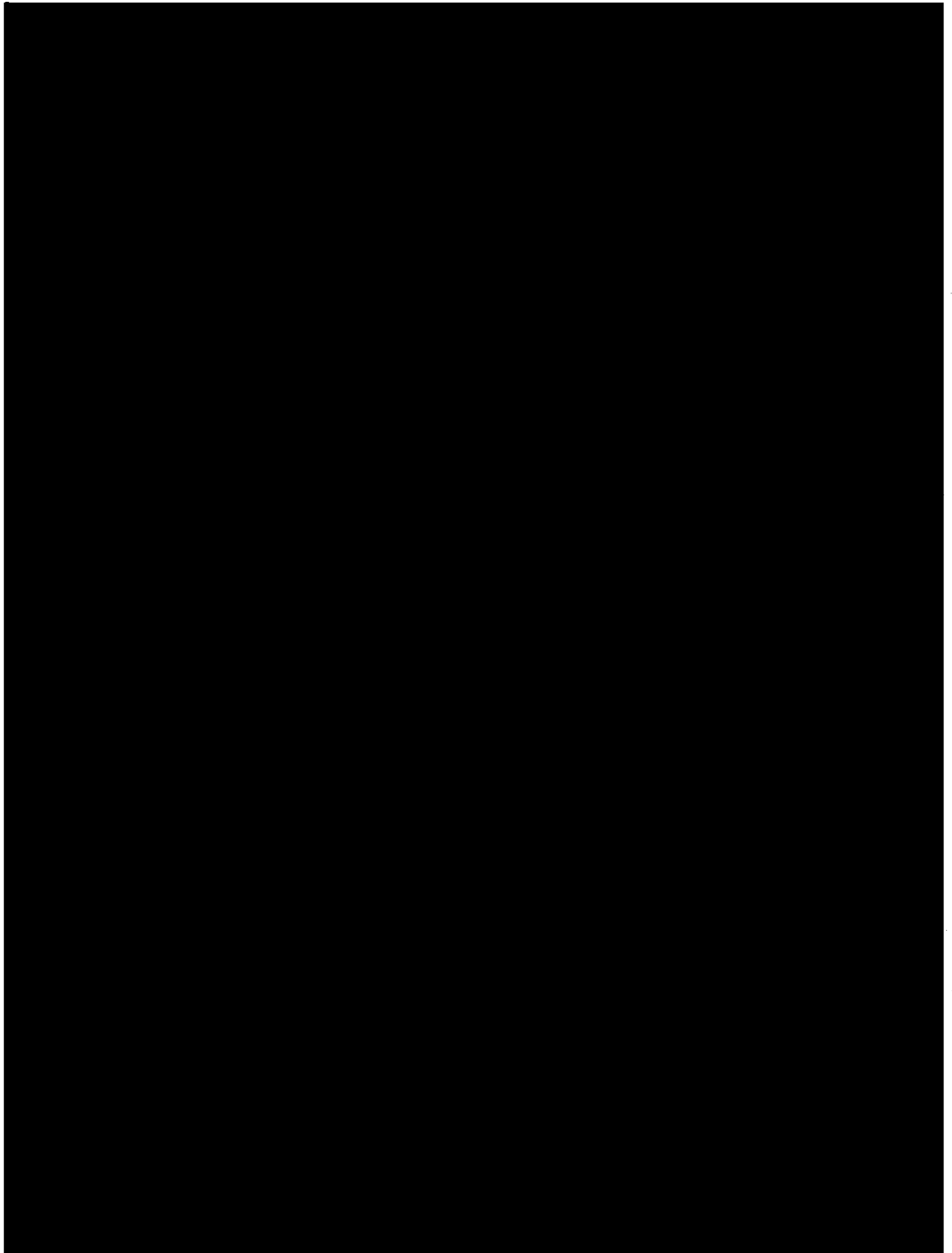
D. The signature authority for NSL sent from HQ AFOSI is the Commander (CC); however, the NSLs submitted in 2004 were signed by the Vice Commander (CV).

E. My point of contact in this matter is [REDACTED] HQ AFOSI/XOQ and he can be reached at [REDACTED]

/S/







~~FOR OFFICIAL USE ONLY~~

[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 Times January 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.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

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."

Office of the Under Secretary of Defense
(Intelligence)

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

From:
To:

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

Sent: Sun Jan 14 16:17:11 2007
Subject: RE: NSL (~~FOUO~~)

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 - [REDACTED]
2004 - [REDACTED]
2003 - [REDACTED]
2002- [REDACTED]
2001 - to be provided later
2000 - to be provided later

CT

2006 [REDACTED]
2005 [REDACTED]

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 statute 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]

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

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]

[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?

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

<<DoD NSL Fact Sheet (13 Jan 07).doc>> <<NYT Article>>

v/r

[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~~

~~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).

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~



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

~~FOR OFFICIAL USE ONLY~~

**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.

~~For Official Use Only~~

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.

~~For Official Use Only~~

