1. PURPOSE: This instruction addresses the marking, handling, protection, and disposal of For Official Use Only information. It sets procedures to help insure that DLA and DOD sensitive information products are adequately safeguarded and appropriately used.

2. APPLICABILITY: This Process Chapter applies DLA-wide, including DLA contractors, grantees, and consultants.

3. POLICY:

   a. FOUO Criteria. Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public under one or more Freedom of Information Act (FOIA) exemptions 2 through 9 (see 32 CFR §286.12, http://www.access.gpo.gov/nara/cfr/cfr-table-search.html) will be considered as being "For Official Use Only" (FOUO). No other material shall be considered or marked as FOUO. Further, FOUO Markings will not be used to protect national security interests. Additional information on FOUO and other controlled, unclassified information may be found in DOD 5200.1-R, DOD Information Security Program Regulation (http://www.dtic.mil/whs/directives/corres/html/52001r.htm).

   b. Unauthorized Disclosure. DLA employees, military members, and DLA contractors, grantees, and consultants will not disclose FOUO material to unauthorized recipients or allow the improper use of FOUO data. Appropriate administrative remedies shall be taken to fix responsibility for unauthorized disclosure whenever feasible, and appropriate action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons.

   c. Prior FOUO Application. The prior application of FOUO markings is not a conclusive basis for withholding a record that is requested under the FOIA. When such a record is requested, it shall be evaluated to determine whether a FOIA exemption would apply.

   d. Historical Papers. Records such as notes, working papers, and drafts retained as historical evidence of DLA actions enjoy no special status apart from the exemptions under the FOIA.

   e. Time to Mark Records. The marking of records at the time of their creation provides notice of FOUO content and facilitates review when a record is requested under the FOIA.

References: Refer to Enclosure 1.
Records requested under the FOIA that do not bear such markings shall not be assumed to be releasable without examination for the presence of information that requires continued protection and qualifies as exempt from public release.


h. Removal of FOUO Material from the DLA Worksite. Where conditions warrant, individual supervisors may authorize removal of FOUO material from DLA worksites for use at home, at temporary duty locations, or at other locations.

i. Placement of FOUO Data on Public Web Sites. FOUO Data may not be placed on the World Wide Web or Internet web sites.

j. Use of Shared Drives and Internal (Intranet) Web Sites. FOUO information with dissemination restrictions, such as Privacy Act material, may not be placed on shared computer drives or internal (Intranet) web sites unless those drives and sites are password protected or otherwise restricted to individuals who have specific responsibilities for handling or using the data in the course of performing official duties.

k. Use of FOUO Data by Contractors or Grantees. Where a DLA contract requires that FOUO information be provided to a contractor or grantee, the contract or grant instrument will include a provision addressing the requirements for safeguarding the data according to Chapter 7-108, DOD 5220.22-R (http://www.dtic.mil/whs/directives/corres/html/522022r.htm). In addition, the contract or grant instrument will address disposal of the FOUO information upon termination or end of the instrument. Disposal may be by return to the Agency, destruction by the contractor, or other suitable method that ensures the data is protected from improper disclosures. The contract or grant instrument will also include a prohibition on secondary uses of any FOUO data by the contractor, grantee, or their employees, subcontractors, or affiliates.

l. Use of Encryption Techniques. When transmitting FOUO data via electronic mail (E-mail), the E-mail message will be encrypted and digitally signed using Common Access Card (CAC) based DOD public key (PK) certificates.

4. RESPONSIBILITIES: DES-S is responsible for establishing DLA “For Official Use Only” (FOUO) program and ensuring DLA compliance with DoD FOUO policy.

5. PROCEDURES: See Enclosure 2. Additional Information is located at Enclosure 3.

6. EFFECTIVE DATE: September 30, 2003

Director, DLA Enterprise Support
3 Enclosures
   Enclosure 1 – References
   Enclosure 2 – Procedures
   Enclosure 3 – Additional Information
Enclosure 1
References


14. DLA Instruction, Records Management
Enclosure 2
Procedures


(1) Marking Paper Records.

(2) An unclassified document containing FOUO information shall be marked "For Official Use Only" at the bottom on the outside of the front cover (if any), on the title page (if used), on each page containing FOUO information, and on the outside of the back cover (if any). Each paragraph containing FOUO information shall be marked as such.

(3) Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page according to DOD 5200.1-R (http://www.dtic.mil/whs/directives/corres/html/52001r.htm). Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate.

(4) Within a classified document, an individual page that contains FOUO information but no classified information shall be marked "For Official Use Only" at the top and bottom of the page, as well as each paragraph that contains FOUO information.

(5) Unclassified transmittal letters shall be marked to call attention to any FOUO material attached.

(6) File folders containing data subject to the Privacy Act will be labeled using DLA Form 1461, Pressure Sensitive Privacy Act Label. The form will be placed on the folder tab to call attention to the sensitive nature of the folder contents. No other uses will be made of DLA Form 1461.

b. Marking Electronic Records. For electronic records, the provisions in Paragraph 4.a.1. will be applied to the extent practicable.

c. FOUO Displayed on Terminal Screens: Where electronic information products contain FOUO data, the opening screen will be marked with the FOUO handling legend. Where possible, each paragraph, column, row, or portion of an electronic record that contains FOUO material will be so marked. The marking may appear in the opening screen, as a footnote, or a remark; e.g., "Data in columns a, c, and f of this database are to be handled as FOUO."

d. Printouts or Reports Containing FOUO Data. Each page of a printout or report generated from databases containing FOUO data will display a pre-programmed header and footer containing the FOUO handling legend. Where practical, the legend may be rubber stamped on the document.

e. Unclassified Electronic Mail (E-Mail) Messages Containing FOUO Data. The opening line of an E-mail message is to call attention to the fact that it contains FOUO data, e.g., "This message is to be handled as For Official Use Only." Similarly, if a FOUO document has been
attached to the E-Mail, the opening line of the message is to state that fact; e.g., "The attachment to this E-Mail message is to be handled as For Official Use Only." Within the body of the message, each part containing FOUO information will be marked at the beginning with the FOUO legend in parentheses.

f. Facsimile Cover Sheets. Where FOUO data is sent via facsimile message, the facsimile cover sheet is to call attention to the fact that the attachment is to be handled as FOUO.

g. Marking Other Types of Housing Devices. Compact Disks, diskettes, canisters, cartridges, tapes, cassettes, and similar housing devices used to permanently store FOUO data will be marked "For Official Use Only" or "FOUO" in a manner that ensures that a recipient or viewer is aware of the status of the information therein. DLA Label 1804, For Official Use Only Pressure Sensitive Label, may be used for this purpose. If the data is also subject to the Privacy Act, DLA Form 1462, Pressure Sensitive Privacy Act Label may be used to mark housing devices in lieu of DLA Label 1804.

h. Transmitting FOUO Material. Paper and electronic records containing FOUO information shall be transmitted in a manner that prevents disclosure of the contents.

(1) Hand-Carried Documents. DLA Form 22, For Official Use Only Cover Sheet, may be used to shield the contents of documents during transport.

(2) Use of U.S. Mails. When not commingled with classified information, paper records containing FOUO information may be sent via first-class mail or parcel post. FOUO material is to be placed in opaque, sealable envelopes and addressed to an authorized recipient. Where conditions warrant, the material may be double wrapped. Where double wrapping is used, the inner envelope may contain the FOUO legend. However, the outer envelope will contain no marking to indicate the sensitivity of the envelope contents. Bulky shipments of FOUO material that otherwise qualify under postal regulations may be sent by fourth-class mail.

(3) Use of Internal Mail Distribution Systems. A paper record containing FOUO data sent using internal mail systems is to be placed in an opaque, sealable envelope and addressed to an individual authorized access to the data. The use of Optional Form 65-B (U. S. Government Messenger Envelope) or similar devices are not authorized to transport FOUO data.

(4) Electronic Transmissions. E-mail messages containing or forwarding FOUO material will be encrypted and digitally signed using CAC based DoD PK certificates. Facsimile messages will be transmitted in accordance with communications security procedures whenever practicable.

i. Disclosing FOUO Material.

(1) Disclosures Within DOD. FOUO information may be disclosed within DOD Components and between officials of DOD Components and DOD contractors, consultants, and grantees to conduct official business for the Department of Defense provided such disclosures are not prohibited by the Privacy Act. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized disclosure.
(2) Disclosures Outside DOD. DLA holders of FOUO information are authorized to convey FOUO information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a Government function, subject to the limitations below:

(3) Privacy Act data will not be disclosed outside the Department of Defense without the approval of the designated Privacy Act system manager. Before conveying data taken from Privacy Act systems of records, DLA system managers will review the "Routine Use" clause of the governing Privacy Act system notice to determine if the disclosure is authorized. See 32 CFR 323 (http://www.access.gpo.gov/nara/cfr/cfr-table-search.html#page1) for further details. The DLA Privacy Act System Notices are available electronically at (http://www.defenselink.mil/privacy/notices/dla/). The designated Privacy Act system manager is listed in the "System Manager" clause of each notice.

(4) Release of FOUO information to Members of Congress is governed by DOD Directive 5400.4 (http://www.dtic.mil/whs/directives/corres/html/54004.htm). Release to the GAO is governed by DOD Directive 7650.1 (http://www.dtic.mil/whs/directives/corres/html/76501.htm). Records released to the Congress or GAO should be reviewed by the releasing authority to determine whether the information warrants FOUO status. If not, prior FOUO markings will be removed or effaced. If withholding criteria are met, the records shall be marked FOUO and the recipient provided an explanation for such exemption and marking. Alternatively, the recipient may be requested, without marking the record, to protect against its public disclosure for reasons that are explained.

(5) Any FOUO information disclosed outside DOD is to carry the standard FOUO warning markings. Further, an expanded marking that explains the significance and meaning of the FOUO marking will be included on the face of the document. This may be accomplished by typing, stamping, or appending a statement on the document restricting further release by the recipient. Use the following format for the statement, substituting the appropriate exemptions and the mailing address of the local FOIA Manager:

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom of Information Act (5 U.S.C. 552). FOIA Exemptions (b)(2), (b)(6), and (b)(7)(C) apply.
Refer all requests for this document to

HQ DLA, ATTN: DP (FOIA)
8725 John J. Kingman Road, Stop 6220
Fort Belvoir, VA 22060-6221

j. Safeguarding FOUO Material. DLA employees, military members, and contractors, grantees, and consultants have a duty to know, understand, and follow proper procedures with respect to safeguarding FOUO data that is accessed, reviewed, or processed in the course of conducting DLA business.

(1) During Duty Hours. During normal working hours, records determined to be FOUO will be placed in an out-of-sight location if the work area is accessible to individuals who have no need to access the records. Individuals will lock computer workstations housing FOUO data
if they will be away from their workstations for short or extended time periods.

(2) During Non-duty Hours. At the close of business, FOUO records shall be stored so as to prevent unauthorized access. Filing such material with other unclassified records in unlocked files or desks, etc., is adequate when normal U.S. Government or Government-contractor internal building security is provided during non-duty hours. When such internal security control is not exercised, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked receptacles such as file cabinets, desks, or bookcases. Computer workstations housing FOUO data will be fully shut down or placed in the locked position after duty hours. FOUO records that are subject to the provisions of the National Security Act of 1959 shall meet the safeguards outlined for that group of records.

(3) Safeguarding FOUO at non-DLA Work Sites. Individuals who have received authorization to use FOUO material at locations away from the DLA work site are responsible for taking necessary steps to ensure that the material is properly safeguarded and used in accordance with this Chapter.

k. Terminating FOUO Status.

(1) The originator of a FOUO document or other competent authority (e.g., initial denial and appellate authorities as defined in 32 CFR 1285.3 (http://www.access.gpo.gov/nara/cfr/cfr-table-search.html#page1) will terminate "For Official Use Only" markings or status when circumstances indicate that the information no longer requires protection from public disclosure.

(2) When FOUO status is terminated, all known holders will be notified to the extent practical. Upon notification, holders will line through or remove the "For Official Use Only" markings, but records in file or storage need not be retrieved solely for that purpose.

l. Disposing of FOUO Material.

(1) Non-record copies of FOUO materials may be destroyed by shredding or tearing each copy into pieces to prevent reconstructing, and placing them in regular trash containers. Alternatively, the shredded paper may be placed in recycle bins if the local contract permits shredded paper to be placed in the recycle bins. When local circumstances or experience indicates that this destruction method does not sufficiently protect FOUO information, local authorities may direct other methods but must give due consideration to the additional expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

(2) Record copies of FOUO documents will be disposed of in accordance with the disposal standards established in the Records Management One Book Chapter and Information Operations.

(3) Electronic records may be destroyed by overwriting, degaussing, or other appropriate methods consistent with Records Management One Book Chapter and Information Operations.

m. Handling Unauthorized Disclosures.
(1) FOUO information is not considered to be in the public domain unless it has been the subject of an official disclosure. Therefore, where FOUO data has been "leaked" to the public, has become the subject of unsubstantiated speculation, or has otherwise been improperly disclosed, the documents will retain their FOUO markings and continue to be handled as such.

(2) Unauthorized Disclosures of FOUO Data. Where DLA employees, military members, or DLA contractors become aware of an unauthorized or an inadvertent disclosure of FOUO data, it is that individual's responsibility to notify the appropriate officials. DLA employees and military members shall notify the FOIA Manager of the DLA Activity of any such disclosures. DLA contractors will notify their administrative contracting officer, who will forward the report to the local FOIA Manager. Local FOIA Managers will notify the originating Component or agency so that a damage assessment may be conducted if deemed appropriate.

(3) Lost, Stolen, or Compromised Personal Data. Whenever a DLA employee, military member, or contractor becomes aware that protected personal data about a Service member, civilian employee, military retiree, family member, or other individual affiliated with DoD (e.g., a volunteer) has been lost, stolen or compromised, the DLA individual will notify the Privacy Act Officer immediately. Where the data has been entrusted to a contractor or the contractor discovers the incident, the administrative contracting officer will also be immediately notified. The following actions will be taken by the official with overall responsibility for safeguarding the data:

(4) Notify the affected individuals as soon as possible, but not later than 10 days after the loss or compromise is discovered. If the affected individuals cannot be readily identified, the DLA individual will provide a generalized notice to the potentially affected population.

(5) At a minimum, advise individuals of the specific data involved; the circumstances surrounding the loss, theft, or compromise; and what protective actions the individual can take, including the guidelines provided by the Federal Trade Commission at its website www.consumer.gov/idtheft).

(6) If the DLA individual with responsibility for safeguarding the data is unable to notify the affected person(s) within the 10-day time period, the DLA individual will immediately inform the Deputy Secretary of Defense of the reasons why notice was not provided. A copy will be provided to the DLA Privacy Act official. If delayed notification was requested by DCIA or other law enforcement entity, a copy of the notification letter will also be provided to that entity.


(1) Full Releases. When a determination has been made that a FOUO document may be fully released to a requester under any public information program, the FOUO markings will be removed from the requester's copy by lining through in pen. In cases where a person seeks access to his or her own record and the record is marked FOUO to protect that person's personal or proprietary interests, the FOUO marks will be lined through on the requester's copy even though the FOUO status has not been terminated. In such cases, the official file copy will retain the FOUO warning.
(2) Partial Releases. When a determination has been made that a document marked as FOUO may be partially released to a requester after removing the FOUO portions, then the exempt portions will be deleted using approved techniques. Exempt portions of documents will be thoroughly removed in such a manner to ensure that no trace of a letter or a portion of a letter remains visible.

(3) Paper Records. Use one of the following methods to make deletions.

- Cut out the material with an Exacto-style razor knife or similar device.

- Black out or tape over the FOUO using Chartpak Graphic Black Plastic tape; 3M Post-It Correction and Cover-up Tape; Avery-Dennison Pres-A-Ply Correction Tape; or PaperMate Liquid Paper Dryline (white).

- After the process is complete, photocopy the document. Review the photocopy to verify that no deleted information is visible. Distribute the photocopy as required.

(4) Electronic Records. Use one of the methods discussed below to prepare documents for public release.

- Commercial off-the-shelf software products, such as AINS Redact XPress, may be used to create a redacted camera-ready version of the document.

- If redaction software product is not available, use word processing to delete the FOUO portions. However, the following additional steps must be taken to ensure that the recipient cannot reconstruct the deletions by using the "undo" or "reviewing" toolbar features of most word processing software packages. After making the deletions, print a copy of the redacted document. Next, manually rescan the document and convert it to a graphics format (e.g., .tif or .pdf). Upload to the appropriate information system and conduct any additional format conversions to facilitate distribution. The document may be distributed via electronic mail, website posting, or as a printed copy.

(5) Effects on FOIA. There is no FOIA exemption to cover the deletion of the FOUO marks. However, deletion of FOUO marks is necessary to show that protection requirements have ended. Therefore, while FOUO material is to be thoroughly deleted to make it unreadable, the FOUO marks are only to be lined through in pen, making them readable but nonetheless signifying that FOUO status has ended. The lining through of the FOUO marks does not constitute a denial for FOIA purposes.

o. Additional Considerations for Privacy Act Material. DLA employees, military members, and contractors who come in contact with Privacy Act data are required to follow the DLA Code of Fair Information Principles, a set of 10 policies that DLA individuals will follow when collecting, using, handling, and storing For Official Use Only data subject to the Privacy Act.
Principle 1 – The Principle of Openness: When we collect personal data from you, we will inform you of the intended uses of the data, the disclosures that will be made, the authorities for the collection, and whether the collection is mandatory or voluntary. We will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the Master List of Privacy Act Systems or Records Notices website, available at: http://www.dla.mil/public_info/privacy.asp.

Principle 2 - The Principle of Individual Participation: Unless DLA has claimed an exemption from the Privacy Act, we will, upon request, grant you access to your records; provide you a list of disclosures made outside the Department of Defense; and make corrections to your file, once shown to be in error.

Principle 3 - The Principle of Limited Collection: DLA will collect only those personal data elements required to fulfill an official function or mission grounded in law. Those collections are conducted by lawful and fair means.

Principle 4 - The Principle of Limited Retention: DLA will retain your personal information only as long as necessary to fulfill the purposes for which it is collected. Records will be destroyed in accordance with established DLA records management principles.

Principle 5 - The Principle of Data Quality: DLA strives to maintain only accurate, relevant, timely, and complete data about you.

Principle 6 - The Principle of Limited Internal Use: DLA will use your personal data only for lawful purposes. Access to your data will be limited to those Department of Defense individuals with an official need for access.

Principle 7 - The Principle of Disclosure: DLA employees and military members will zealously guard your personal data to ensure that all disclosures are made with your written permission or are made in strict accordance with the Privacy Act.

Principle 8 - The Principle of Security: Your personal data is protected by appropriate safeguards to ensure security and confidentiality. Electronic systems will be periodically reviewed for compliance with the security principles of the Privacy Act, the Computer Security Act, and related statutes. Electronic collections will be accomplished in a safe and secure manner.

Principle 9 - The Principle of Accountability: DLA and our employees, military members, and contractors are subject to civil and criminal penalties for certain breaches of Privacy. DLA is diligent in sanctioning individuals who violate Privacy rules.

Principle 10 - The Principle of Challenging Compliance: You may challenge DLA if you believe that DLA has failed to comply with these principles, the Privacy Act, or the rules of a system of records notice. Challenges may be addressed to the person accountable for compliance with this Code, the local DLA Privacy Act manager, or the HQ DLA Privacy Act manager.
Enclosure 3
Additional Information

a. Only that information that is determined to be exempt from public release under FOIA exemptions 2 through 9 is to carry the FOUO marking. The policy of what data elements are considered to be releasable or not releasable may change as a result of policy changes and court decisions handed down. Below is a list of the FOIA exemptions, along with examples of data to be treated as FOUO.

(1) FOIA Exemption 2 Material: Predominantly internal data, the disclosure of which could allow someone to circumvent, frustrate, or render ineffective laws, statutes, or agency regulations. Examples:

- Government credit card account numbers
- An individual’s security clearance level; designations of positions requiring clearance
- Guidelines for conducting investigations
- Security* plans and procedures
- Security* weaknesses and vulnerabilities
- Answers to test questions
- Strategies for handling high risk issues
- Guidelines for detecting fraud
- Benchmarks and criteria used in evaluating job applicants
- Security classification guides, including actual classification levels
- Procedures for securing assets, firearms, and controlled forms and devices
- Procedures for identifying, neutralizing, or responding to security threats

*“Security” covers a broad range of programs designed to protect the agency, civilian employees, military members, and resources (information security, computer security, building security, personnel security, etc.)

(2) FOIA Exemption 3 Material: Information prohibited from release by Federal statute. Examples:

- Export trade certificate details
- Maps, Charts, and Geodetic Data
- Medical data
- Contractor proposals
- Financial Disclosure Reports of Special Government Employees
- Unclassified Technical Data with Military or Space Application
- Arms Exports
- Drug Abuse Rehabilitation
- Employee Complaints to the Inspector General
- The name, duty station, and contact data for individuals stationed in foreign territories.

(3) FOIA Exemption 4 Material: Trade Secret, Commercial, and Financial Data Submitted in Confidence. The exemption covers a wide range of “submitters” including businesses, not-for-profit groups, state, local, & foreign governments, consultants, etc. Examples:
■ Names of customers, suppliers, consultants, subcontractors
■ Business, financial, pricing, and management strategies
■ Raw research data
■ Profit and loss data, break-even calculations
■ Technical, cost, and management proposals
■ Assets, liabilities and net worth
■ Purchase records, actual cost data
■ Unannounced future or planned products
■ Descriptions of plants or facilities; assembly line setups
■ Scientific and manufacturing processes
■ Statistical data concerning contract performance
■ Copyrighted computer software
■ Proprietary information submitted strictly on a voluntary basis

(4) FOIA Exemption 5 Material: Information that would not be disclosable in litigation under discovery rules. There are many discovery privileges; the most widely claimed are the deliberative process, attorney-client, attorney work product, and government commercial privileges. Examples:

■ Internal advice, recommendations and subjection evaluations
■ Non factual parts of after-action reports, lessons learned, situation reports.
■ Advice, suggestions, or evaluation provided by consultants, boards, or committees.
■ Non factual portions of evaluations of contractors and their products.
■ Reports of inspection, reports of IG audits, investigations, or surveys pertaining to safety, security or the internal management, administration or operation of DoD
■ Drafts or proposed policies, statements, reports, etc.
■ Interpretations of technical or statistical data,
■ Confidential communications between attorney and client.
■ Attorney work products.
■ Government background documents used to calculate its bid in a “contracting out” procedure (i.e., OMB Circular A-76).
■ Agency cost estimates for use in evaluating contractor proposals; formulas or methods for conducting such evaluations.
■ Planning, programming, and budgetary information that is involved in the defense planning and resource allocation process.
■ Information of a speculative, tentative, or evaluative nature such as proposed plans to procure, lease, or otherwise acquire and dispose of materials, real estate, facilities or functions, when such information would provide undue or unfair competitive advantage to private personal interests or would impede government functions.

(5). FOIA Exemption 6 Material: Any material, the release of which could invade an individual’s privacy; embarrass an individual; violate the Privacy Act; or promote threats of terrorism. Examples:

■ Financial, credit, and medical information
■ The fact of participation in Employee Assistance Programs
■ An employee's or military member's take-home pay
- The fact of and level of security clearance; types of positions requiring clearance.
- Federal health and life insurance options selected by an employee
- Leave balances; type of leave taken
- Drug test results and the fact of participation in rehabilitation programs
- Home addresses/telephone numbers/home web addresses
- Social Security Number; Mother’s maiden name; other names used
- Spouse and children data, including photographs of family members.
- Religion, race, national origin
- Performance ratings; Awards (if they reveal performance ratings)
- Government issued credit card account numbers, credit balances, and credit limits
- Names and complete employment applications of vacancy nonselectees
- Suggestions submitted to the agency
- Identity of low- and mid-level employees accused of misconduct
- Names and/or identities of employees who hold government issued travel cards

(6) FOIA Exemption 7 Material: Records compiled for law enforcement purposes. Examples:

- The fact of ongoing undercover investigations
- The fact that an individual is the subject of or named in an investigative report
- The names and/or identities of investigators
- Investigative techniques and methods
- Names of and information that would reveal a confidential source
- Procedures for conducting investigations
- Surveillance techniques, methods, and protocols
- Procedures/methods for verifying data developed during investigations
- Techniques/methods for law enforcement prosecutions

(7) FOIA Exemption 8 Material: Records relating to examination or supervision of financial institutions. This exemption is not relied on within DLA.

(8) FOIA Exemption 9 Material: Geological and Geophysical information and data, including maps, concerning wells. This exemption has never been relied on within DLA.

b. FOIA Websites.

(1) The Department of Defense and the Department of Justice maintain websites with useful information.

(i) The Department of Justice Office of Information and Privacy website at http://www.usdoj.gov/oip/oip.html contains information on the exemptions, court decisions, and policies in the following documents:

(ii) The Department of Justice National Advocacy Center website at (http://www.usdoj.gov/usao/oeusa/ole.html) contains information on FOIA training that focuses on the exemptions.
(iii) The Department of Defense FOIA Website at
http://www.defenselink.mil/pubs/foi/ information on exemptions, policies, and training.