



governmentattic.org

"Rummaging in the government's attic"

Description of document: Defense Logistics Agency (DLA) FOIA Workshop and Conference Calls, 2010-2012

Requested date: 23-April-2012

Released date: 11-May-3012

Posted date: 16-December-2013

Source of document: Freedom of Information Act Request
DLA Headquarters
ATTN: DGA
8725 John J. Kingman Road, Suite 1644
Fort Belvoir, VA 22060-6221
Fax: 703-767-6091
Email: hq-foia@dla.mil

Note: PDF page 32 and beyond, turning on Layers in Adobe Acrobat will allow access to the speaker's notes

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

IN REPLY
REFER TO

MAY 11 2012

This letter responds to your April 23, 2012, Freedom of Information Act request for records concerning the Defense Logistics Agency FOIA Workshop and Conference Calls.

The enclosed CD and records are released to you in part as portions were found to be exempt from disclosure pursuant to 5 U.S.C. § 552 (b)(6), personal privacy. Exemption 6 protects information about individuals when disclosure of such information would constitute a clearly unwarranted invasion of personal privacy. Due to increased security of DoD personnel, the names of DLA employees who are not in the public domain are withheld.

You have the right to appeal this partial denial. An appeal must be made in writing to the General Counsel and reach the General Counsel's Office within 60 calendar days from the date of this letter, no later than 5:00 pm, Eastern Standard Time. The appeal should include your reasons for reconsideration and enclose a copy of this letter. An appeal may be mailed, emailed to hq-foia@dla.mil, or faxed to 703-767-6091. Appeals are to be addressed to the General Counsel, Defense Logistics Agency, ATTN: DGA, Suite 1644, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6221.

Should you have any questions or require further information, please contact Ms. Kathy Tennessee, DLA Headquarters FOIA and Privacy Officer, at 703-767-6183 or Kathy.tennessee@dla.mil. Please reference our case number DLA-12-HFOI-00095 in any subsequent communication regarding this request.

No fees are assessed. Should you have any questions or require further assistance, please contact Ms. Kathy Tennessee at 703-767-6183 or Kathy.tennessee@dla.mil.

Sincerely,

Walter Thomas, Jr.
Acting Deputy General Counsel

Enclosures
As stated

January 25, 2012 VTC

	Roll Call	Kathy Tennessee
	Welcome and Introduction Opening Remarks	Rix Edwards, Associate General Counsel and/or Mr. Fred Pribble, General Counsel
	Practice Group Intro/Charter	Lew Oleinick
	Privacy Breach Procedures	
	PROCLTR / Section (m) Contracts	
	PIA Privacy Review Cycle	Lew Oleinick
	FOIA Referrals & Consultations	Debbie Teer/Kathy Tennessee
	New DLA Form 1917	Debbie Teer
	MDR & FOIA	Lew Oleinick
	CUI & FOIA	Debbie Teer
	Misc FOIA	Debbie Teer/Kathy Tennessee
	Wrap up	

.....

Agenda

- Explanation / Introduction (why you were invited)
- Breach Procedures (send current copy to POCs with agenda)
 - Slide will contain:
 - Physical vs. Electronic
 - Reporting Timelines
 - Submitting Final Incident Reports (within 10 working days after Technical Assessment has been rendered by the DLA CERT/DLA NOSC)
 - Time to Destroy 09 Incident Files (FOIA / Privacy Retention Periods (Excerpts from DLA Records Schedule send to POCs))
- PROCLTR and Section (m) Requirements (send PROCLTR / FAR Clauses with agenda)
- PIA Review Cycle (Lew to present)
- FOIA Referrals
 - Consultations
 - Acknowledgment process
- New DLA Form 1917

MDR (send DoD Final Rule and MDR Addresses to POCs with agenda) NOTE:
Address for DLA is incorrect. New address is Defense Logistics Agency, Attention:
DLA Intelligence, 8725 John J. Kingman Road, Suite 3533, Fort Belvoir, VA 22060–
6221.

- FOIA and Controlled Unclassified Information (CUI)
 - HR Requests
 - D92-Full Releases
 - Technical Data Requests vs. FOIA requests for same info (existing DLA procedures for this data)
 - DCSO
 - PII in FOIA Description Blocks (FOIA Xpress)
 - Retention period for records in FOIA files

FOIA/Privacy Teleconference
May 4, 2011
2:30 – 3:30

Agenda

Privacy

1. For the Privacy POCs: Locate the materials (placards, posters, and "Reporting Privacy / PII Breaches" cards) used during the 2007 PII Stand-down. They were designed to be reused.
2. DLA's 2875 Process (System Authorization Access Requests)
3. Remind Privacy POCs to send Incident Reports and questions to the hq-privacy@dlm.mil mailbox.

Other

1. ASAP (Mansfield/Pasquinely/Silber)
2. Introductions ((b)(6))/Roddy)

FOIA

1. NSNs
2. FOIAXpress Users Group Conference (Chief Counsel must approve)
Wednesday June 15, 2011
3. Supreme Court Ruling on use of Exemption 2

FOIA/Privacy Teleconference
February 24, 2010

Agenda

Privacy (Jody)

- 2010 DOJ Privacy Overview:
 - The 2010 Edition of the DOJ Office of Privacy and Civil Liberties (OPCL) Overview is now available on OPCL's website at
<http://www.justice.gov/opcl/1974privacyact-overview.htm>
<<http://www.justice.gov/opcl/1974privacyact-overview.htm>> .
- PII Incident Reports
 - Format
 - Numbers on Final Incident Reports
- PII Reminders
 - Suggestions wanted
- Training Opportunity
 - International Association of Privacy Professionals 2010 Privacy Summit (April 2010)
(https://www.privacyassociation.org/events_and_programs/global_privacy_summit/)

FOIA/PA Conference – Stay tuned (Kathy)

FOIA (Debbie)

- Reading rooms (Lew)
- Chief FOIA Officer Report (Lew)
- Carve out
- FOIAXpress:
 - Data Call: What parts are used (ie, creating, redacting, document management)
 - Quick Guide, is it helpful
 - Use of invoices (b)(6)
 - Duplicate requester entries
- Referral reminder from DOD

DLA FOIA AND PRIVACY TRAINING WORKSHOP

TUESDAY, OCTOBER 26, 2010

8:00 to 8:15	Welcome and Introduction Opening Remarks	Mr. Rix Edwards, Associate General Counsel Mr. Fred Pribble, General Counsel
8:15 to 10:15	FOIA Administrative Guidance How we do it!	Ms. Debbie Teer, DLA HQ Ms. Kathy Tennessee, DLA HQ Ms. Pamela Tull, DSCP
10:15 to 10:30	Break	
10:30 to 11:45	FOIA/Privacy Act Recent Decisions	(b)(6) Office of Information Policy, DOJ
11:45 to 12:45	Lunch	
12:45 to 2:45	Privacy Act Overview / DoD Privacy Program	Mr. Lewis Oleinick, DLA HQ Ms. Jody Sinkler, DLA HQ
2:45 to 3:00	Break	
3:00 to 5:00	Getting to Know FOIA Xpress Hands-on training	Ms. Debbie Teer, DLA HQ Ms. Kathy Tennessee, DLA HQ
DELIVERABLE-FX QUICK GUIDE*		

WEDNESDAY, OCTOBER 27, 2010

7:00 - 7:50	DGA Network Breakfast (7:30 - Demonstration of DGA's New Employee Orientation)	
8:00 to 10:00	Panel: Our Privacy Program Partners - DLA Forms Program - DLA Records Mgmt Program - E-Gov Act Requirement (PIAs) - Paperwork Reduction Act	Panel Facilitator: Ms. Jody Sinkler, DLA HQ (b)(6) Mr. Lewis Oleinick, DLA HQ
10:00 to 10:15	Break	
10:15 to 11:45	Developing a Privacy Act System of Records Notice (SORN)	Mrs. Cindy Allard, Chief OSD&JS Privacy Officer Ms. Jody Sinkler, DLA HQ
DELIVERABLE: DEVELOPING A SORN*		
11:45 to 12:45	Lunch**	
12:45 to 2:45	OGIS/ADR/Public Liaison Training & Discussion	(b)(6) Mr. Lewis Oleinick, DLA HQ
2:45 to 3:00	Break	
3:00 to 5:00	Workshop: - DLA Incident Handling Procedures - Writing the Incident Report	Mr. Lewis Oleinick, DLA HQ Ms. Jody Sinkler, DLA HQ Ms. Kathy Tennessee, DLA HQ

DLA FOIA AND PRIVACY TRAINING WORKSHOP

THURSDAY, OCTOBER 28, 2010

7:00 – 7:50	DGA Network Breakfast	
8:00 to 10:00	FOIA Matters – Referrals – Fees – Reading Rooms	Referrals: Ms. Teer and Ms. Tennessee, FOIA Fees: Ms. Peggy Pasquinelly (DLA Land & Maritime) & Ms. Judith Mansfield (DLA Disposition Services) Reading Rooms: Lew Oleinick, DLA HQ
10:00 to 10:15	Break	
10:15 to 12:15	Commonly Used FOIA Exemptions: B(4), B(5), B(6) & 7(C) DELIVERABLE: EXEMPTION GUIDE*	Ms. Debbie Teer, DLA HQ Ms. Kathy Tennessee, DLA HQ Mr. Lewis Oleinick, DLA HQ
12:15 to 1:15	Lunch	
1:15 to 2:15	Workshop: Your Privacy Toolbox DELIVERABLE: PRIVACY TOOLBOX*	Ms. Jody Sinkler, DLA HQ Ms. Kathy Tennessee, DLA HQ Mr. Lewis Oleinick, DLA HQ
2:15 to 2:30	Closing Remarks	Mr. Rix Edwards, Associate General Counsel

* DGA will be responsible for finalizing and distributing the deliverables to attendees. Those not completed during the Workshop will be completed after and provided to the attendees at a later date.

Deliverables are identified as:

1. Updated FX Quick Guide
2. Developing a Privacy Act system of records notice (SORN)
3. FOIA Exemption Guide
4. Privacy Toolbox (Documents / Websites needed to run a successful Privacy Program)

DLA FOIA AND PRIVACY TRAINING WORKSHOP

DAY 1 – OCTOBER 26, 2010

FOIA Administrative Guidance -- This workshop will address the best DLA administrative practices for processing requests. Will discuss the Open Gov't Act of 2007 and its impact and how to set up a complete administrative record. Outcome will be an index for setting up the administrative file.

FOIA/Privacy Act Recent Decisions -- This workshop will provide a review of recent court cases and the rulings. Learn how these case decisions relating to various FOIA exemptions impact us as FOIA/PA practitioners.

Privacy Act Overview / DoD Privacy Program -- This workshop will discuss the basic scope of the Act and how DoD has implemented the Act's requirements

Getting to Know FOIAXpress -- This workshop will provide a hands-on, step-by-step journey for processing a FOIA request using FOIAXpress. Learn short cuts and must dos/don'ts. Will discuss DLA preferences for using FOIAXpress and develop a Quick Guide for reference.

DAY 2 – OCTOBER 27, 2010

Our Privacy Program Partners -- This workshop will teach the participants how the DLA Privacy Program depends on the DLA Forms Program, the DLA Records Mgmt Program, the Paperwork Reduction Act, and E-Gov Act.

Developing a Privacy System of Records Notice (SORN) -- This workshop will provide detailed understanding of SORNs and procedural guidance in writing/developing SORNs.

OGIS/ADR/Public Liaison -- The Open Gov't Act 2007 created the Office of Government Information Services (OGIS) within the National Archives and Records Administration (NARA). OGIS will provide services to mediate disputes between FOIA requesters and agencies. This workshop will teach participants how OGIS and the Public Liaison will act in these capacities and how to initiate alternative dispute resolution (ADR).

DLA PII Incident Handling Procedures/Writing the Incident Report -- This workshop will discuss the DLA PII Breach Procedures in detail and how to develop a final PII incident report.

DAY 3 – OCTOBER 28, 2010

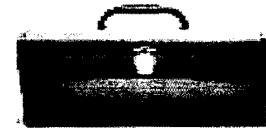
FOIA Matters: Referrals/Fees/Reading Rooms -- This workshop will address the requirements of each of these sections of FOIA and DLA preferences and best practices for each topic.

Commonly Used FOIA Exemptions: B(4), B(5), B(6) & 7(C) -- This workshop will provide an in depth discussion of these exemptions and how DLA applies them. Review of commonly requested records and how to apply the exemptions to facilitate consistency across the enterprise. Outcome will be a tip sheet for applying exemptions.

What's in Your Privacy Toolbox? -- A successful Privacy Program is not about knowing it all but knowing where to go to find the answer to your specific questions. This workshop will discuss the documents and websites needed to run a successful Privacy Program.

PRIVACY TOOLBOX

Updated July 27, 2011



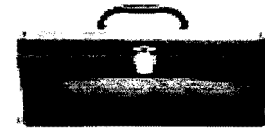
Your "Privacy Toolbox" is a list of the documents / websites needed to run a successful Privacy Program.

Federal Statutes

1. **Privacy Act of 1974, as amended (5 U.S.C. § 552a).** The Privacy Act of 1974, 5 U.S.C. § 552a (2006), which has been in effect since September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.
2. **Legislative History of the Privacy Act.** This is the legislative history of the Privacy Act that was prepared jointly by the U.S. Senate Committee on Government Operations and the U.S. House Government Operations Subcommittee on Government Information and Individual Rights. This history contains the text of the major bills considered by the House and Senate, with accompanying reports, the text of House and Senate Floor debate, related explanatory materials and case law, and regulatory documents issued pursuant to the public law. A Library of Congress publication.
3. **Freedom of Information Act (5 U.S.C. § 552).** The U.S. Freedom of Information Act (FOIA) is a law ensuring public access to U.S. government records. FOIA carries a presumption of disclosure; the burden is on the government - not the public - to substantiate why information may not be released. Upon written request, agencies of the United States government are required to disclose those records, unless they can be lawfully withheld from disclosure under one of nine specific exemptions in the FOIA. This right of access is ultimately enforceable in federal court.
4. **Department of Justice Freedom of Information Reference Materials.** DOJ's Office of Information Policy has compiled a website of primary reference material for the FOIA practitioner and supporting counsel.
5. **E-Government Act of 2002 (Pub. L. No. 107-347, 116 Stat. 2899).** To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.
6. **Federal Records Act of 1950 (44 U.S.C. Ch 31).** The Federal Records Act of 1950, as amended, establishes the framework for records management programs in Federal Agencies. As the primary agency for records management oversight, the National Archives and Records Administration (NARA) is responsible for assisting Federal agencies in maintaining adequate and proper documentation of policies and transactions of the Federal Government. This is done by appraising records (determining record value and final disposition of temporary or permanent records), regulating and approving the disposition of Federal records, operating Federal Records Centers and preserving permanent records.
7. **Administrative Procedure Act (5 U.S.C. §§ 551, 554-558).** The Administrative Procedures Act is the law under which the U.S. federal agencies create the regulations they enforce.

PRIVACY TOOLBOX

Updated July 27, 2011



8. **Paperwork Reduction Act of 1980 (44 U.S.C. § 3501, et seq.).** Minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information by or for the Federal Government;
9. **Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501 et seq., 16 CFR § 312).** The primary goal of COPPA is to place parents in control over what information is collected from their young children online. Designed to protect children under age 13 while accounting for the dynamic nature of the Internet. Applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13.
10. **Confidentiality of Records Statutes (Drug & Alcohol Abuse) (42 U.S.C. § 290dd-2)** Statute limits disclosures permitted.
11. **Homeland Security Presidential Directive-12 (HSPD-12).** Policy for a Common Identification Standard for Federal Employees and Contractors.
12. **Electronic Communications Privacy Act of 1986.** The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act") by extending government restrictions on wiretaps beyond telephone calls to apply to electronic data transmissions. "The PATRIOT Act also clarified and updated ECPA in light of modern technologies, and in several respects it eased restrictions on law enforcement access to stored communications."

PRIVACY TOOLBOX

Updated July 27, 2011



Office of Management and Budget (OMB) Guidance. The Privacy Act provides that the Office of Management and Budget shall "develop guidelines and regulations ... and provide continuing assistance to and oversight of the implementation of the ... " operative provisions of the Privacy Act by the agencies. Below are links to three areas of guidance.

- [OMB Circulars](#)
- [OMB Memoranda](#)
- [OMB Privacy Guidance](#)

Specific OMB Privacy Guidance:

1. [Privacy Act Implementation, Guidelines and Responsibilities \(July 9, 1975\)](#)
2. [Implementation of the Privacy Act of 1974, Supplementary Guidance \(December 4, 1975\)](#)
3. [Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act \(March 30, 1983\)](#)
4. [Privacy Act Guidance - Update \(May 24, 1985\)](#)
5. [Guidance on Privacy Act Implications of "Call Detail" Programs \(April 20, 1987\)](#)
6. [Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988 \(June 19, 1989\)](#)
7. [Proposed Guidance on Computer Matching and Privacy Protection Amendments of 1990 \(April 23, 1991\)](#)
8. [M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" \(January 7, 1999\)](#)
9. [M-99-18, Privacy Policies on Federal Web Sites \(June 2, 1999\)](#)
10. [Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act \(June 21, 2000\)](#)
11. [OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources \(November 28, 2000\)](#)
 - [PDF Version](#)
 - [HTML Version](#)
12. [M-00-13, Privacy Policies and Data Collection on Federal Web Sites \(June 22, 2000\)](#)
13. [Letter from Roger Baker to John Spotila on Federal agency use of Web cookies \(July 28, 2000\)](#)
14. [Letter from John Spotila to Roger Baker, clarification of OMB Cookies Policy \(September 5, 2000\)](#)
15. [M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy \(December 20, 2000\)](#)
16. [M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 \(September 26, 2003\)](#)

PRIVACY TOOLBOX

Updated July 27, 2011



17. M-05-04, Policies for Federal Agency Public Websites (December 17, 2004)
18. M-05-08, Designation of Senior Agency Officials for Privacy (February 11, 2005)
19. M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
20. M-06-16, Protection of Sensitive Agency Information (June 23, 2006)
21. M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)
22. Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006)
23. M-07-16, Safeguarding Against & Responding to Breach of Personally Identifiable Information (May 22, 2007)
24. M-07-20, FY 2007 E-Government Act Reporting Instructions (August 14, 2008)
25. M-08-15, Tools Available for Implementing Electronic Records Management (March 31, 2008)
26. M-10-06, Open Government Directive (December 8, 2009)
27. M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010)
28. M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010)

PRIVACY TOOLBOX

Updated July 27, 2011



Defense Privacy and Civil Liberties Office (DPCLO). The DPCLO is responsible for implementing the Department of Defense (DoD) Privacy and Civil Liberties Programs.

1. Defense Privacy and Civil Liberties Office.
 - a. DoD Component Privacy POCs
 - b. DoD Directive 5400.11, DoD Privacy Program (May 8, 2007)
 - c. DoD 5400.11-R, Department of Defense Privacy Program (May 14, 2007)
 - d. DA&M memo entitled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)" June 5, 2009
 - e. Defense Privacy Board Advisory Opinions The opinions will be incorporated into the next revision of 5400.11-R. Opinions appear at the bottom of the page.
 - f. DoD Blanket Routine Uses DoD has established 16 routine uses that apply to all DoD systems of records unless otherwise stated within the SORN.
 - g. DoD Privacy Act Systems of Records Notices. DPCLO is responsible for the maintenance of the Master Registry of DoD Privacy Act Systems of Records Notices (SORNs). All DoD Components with published SORNs are represented.
 - h. Government-wide Systems of Records Notices. Some Federal agencies have responsibility for one or more systems of records which are applicable Government-wide. This negates the need for an agency to publish a system notice if it maintains a record under a Government-wide system of records notice. DPCLO has put together a listing of these SORNs.
 - i. Computer Matching Reports. DLA does not currently participate in computer matching, i.e., the computerized comparison of two or more automated systems of records or a system of records with non-Federal records.

PRIVACY TOOLBOX

Updated July 27, 2011



Frequently Used Websites:

DoD Websites

1. Defense Freedom of Information Policy Office (DFOIPO). DFOIPO is responsible for implementation of the Department of Defense (DoD) FOIA Program.
 - a. Annual FOIA Reports
 - b. DoD Backlog Reduction Plans
 - c. DoD Executive Order 13392
 - d. DoD FOIA Handbook
 - e. DoD FOIA Improvement Plan
 - f. DoD FOIA Policy Guidance Includes the DA&M Memo, Subject: Withholding of Information that Personally Identifies DoD Personnel (September 1, 2005)
 - g. DoD FOIA Regulation
 - h. DoD Record Locator
 - i. FOIA Reference Materials
 - j. FOIA Training Resources
 - k. Major Info Systems
 - l. Sources of DoD Records
 - m. Text of the FOIA
2. DoD CIO Public Website
 - a. DoD CIO Policy Memo - Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII) (Aug 18, 2006)
 - b. DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance
3. Information Assurance Support Environment. Your "One-Stop-Shop" for IA Information. This DISA website is where the DoD PII Training is also available.
4. DoD Forms Management Program. Locate DD, SD, and Standard and Optional Forms.
5. DoD Issuances. Official DoD Website for DoD Issuances.
6. DoD Web Policy; Web Site Administration Policies & Procedures (November 25, 1998)
7. Joint Enterprise Directory Services (JEDS) (access is CAC enabled). JEDS is a central repository of contact and certificate information for members of the DoD-community and its commands, services, and agencies.

PRIVACY TOOLBOX

Updated July 27, 2011



DLA Websites

1. DLA FOIA/Privacy Webpage. DLA FOIA and Privacy Program Webpage.
2. DLA Records Schedule. DLA Records Management Program.
3. DLA PIAs. Completed Privacy Impact Assessments

Other Federal Agency Websites

1. National Personnel Records Center (NPRC). NPRC is a central repository of personnel-related records, both military and civil service.
 - a. Military Personnel Records
 - b. Civilian Personnel Records
2. Government Printing Office (GPO)
 - a. Federal Digital System (FDsys). FDsys provides free online access to official Federal Government publications. Through FDsys, you are able to access the following:
 - Code of Federal Regulations
 - Compilation of Presidential Documents
 - Congressional Bills
 - Congressional Documents
 - Congressional Hearings
 - Congressional Record
 - Congressional Reports
 - Constitution of the United States of America: Analysis and Interpretation
 - Economic Indicators
 - Federal Register
 - Public and Private Laws
 - United States Code
 - b. Federal Register Document Drafting Handbook. Handbook prescribes the Privacy Act system of records notice format.
3. U.S. Department of Justice, Office of Justice Programs, Justice Information Sharing Privacy and Civil Liberties
4. Department of Homeland Security Privacy Office
5. Paperwork Reduction Act Paperwork Requirements, Office of Information and Regulatory Affairs, OMB. Lists current OMB information collections, collections under review, expired collections, and reviews completed in the last 30 days for all Federal agencies.

PRIVACY TOOLBOX

Updated July 27, 2011



6. Office of Management and Budget MAX Homepage Federal Privacy Officers Community of Practice. Account required for access.
7. Department of the Navy, Chief Information Officer Webpage. Navy's CIO webpage has good resources.
8. Records Management Resources, National Archives and Records Administration (NARA). Website provides access to the NARA General Records Schedule.
9. Executive Orders Disposition Tables Index. The Disposition Tables list the status of Executive Orders from January 8, 1937 - May 21, 2010. Disposition Tables contain information about Executive Orders beginning with those signed by President Franklin D. Roosevelt and are arranged according to Presidential administration and year of signature. The tables are compiled and maintained by the Office of the Federal Register editors. The Disposition Tables include the following information:
 - Executive order number;
 - Date of signing by the President
 - Federal Register volume, page number, and issue date
 - Title
 - Amendments (if any)
 - Current status (where applicable)
10. Federal Trade Commission, Fighting Back Against Identity Theft. This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.
11. 2009 Compilation of Federal Systems of Records Notices. The Office of the Federal Register (OFR) biennially compiles and publishes The Privacy Act Compilation, as directed by the Privacy Act of 1974. All Federal Agencies with published SORNs are represented.
12. Federal Acquisition Regulation (FAR) Contracts requiring the maintenance or operation of a system of records or the portion of a system of records shall include in the solicitation and resulting contract such terms as are prescribed by the FAR. See Part 24, Protection of Privacy and Freedom of Information.
13. Defense FAR Supplement Part 224, Protection of Privacy and Freedom of Information
 - a. 52-224-1 Privacy Act Notification
 - b. 52-224-2 Privacy Act
14. Overview of the Privacy Act of 1974, 2010 Edition. The "Overview of the Privacy Act of 1974," prepared by the Department of Justice's Office of Privacy and Civil Liberties (OPCL), is a discussion of the Privacy Act's disclosure prohibition, its access and amendment provisions, and its agency recordkeeping requirements. Tracking the provisions of the Act itself, the Overview provides reference to,

PRIVACY TOOLBOX

Updated July 27, 2011



and legal analysis of, court decisions interpreting the Act's provisions. The Overview is not intended to provide policy guidance, as that role statutorily rests with the Office of Management and Budget (OMB), 5 U.S.C. § 552a(v). However, where OMB has issued policy guidance on particular provisions of the Act, citation to such guidance is provided in the Overview. The 2010 edition of the Overview was issued electronically and sent for publication in February 2010 and includes cases through November 2009.



National Institute of Standards and Technology (NIST) Guidance. NIST is a federal technology agency that works with industry to develop and apply technology, measurements, and standards

1. NIST SP 800-16, Information Technology Security Training Requirements (April 1998). Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. The Computer Security Act of 1987 (Public Law 100-235) required that, "Each agency shall provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."
2. NIST SP 800-30, Risk Management Guide for Information Technology Systems (July 2002). Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.
3. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems (February 2010). Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency. Security Certification and Accreditation is a big part of the FISMA process.
4. NIST SP 800-39, Managing Risk from Information Systems: An Organizational Perspective, Second Public Draft (April 2008).
5. NIST SP 800-53, Recommended Security Controls for Federal Information Systems (Rev. 3, August 2009). The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information. The SP 800-53 guidelines were developed to help achieve more secure information systems within the federal government.
6. NIST SP 800-83, Guide to Malware Incident Prevention and Handling (November 2005). Special Publication 800-83 provides recommendations for implementing and improving an organization's malware incident prevention measures. It also provides extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle virus / malware incidents, particularly widespread ones. The recommendations address

PRIVACY TOOLBOX

Updated July 27, 2011



several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies. It also addresses attacker tools such as backdoors and rootkits. The recommendations encompass various transmission mechanisms, including network services (e.g., e-mail, Web browsing, file sharing) and removable media.

7. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 6, 2010). Provides practical, context-based guidelines for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.

PRIVACY TOOLBOX

Updated July 27, 2011



U.S. Government Accountability Office. The U.S. Government Accountability Office (GAO) is known as "the investigative arm of Congress" and "the congressional watchdog." GAO supports the Congress in meeting its constitutional responsibilities and helps improve the performance and accountability of the federal government for the benefit of the American people. GAO Reports can be found at

1. GAO-09-759T, Governments Have Acted to Protect PPII, but Vulnerabilities Remain
2. GAO-09-136, Continued Efforts Needed to Address Significant Weaknesses at IRS
3. GAO-08-795T, Congress Should Consider Alternatives for Strengthening Protection of PII
4. GAO-08-536, Alternatives Exist for Enhancing Protection of Personally Identifiable Information
5. GAO-08-343, Protecting Personally Identifiable Information
6. GAO-07-935T, Agencies Report Progress, but Sensitive Data Remain at Risk
7. GAO-07-870, DHS Needs to Immediately Address Significant Weaknesses in Systems Supporting US-VISIT
8. GAO-07-837, Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses
9. GAO-07-751T, Persistent Weaknesses Highlight Need for Further Improvement
10. GAO-07-657, Lessons Learned about Data Breach Notification
11. GAO-07-1003T, Homeland Security Needs to Enhance Effectiveness of Its Program
12. GAO-06-897T, Leadership Needed to Address Weaknesses and Privacy Issues at Veterans Affairs
13. GAO-06-866T, Leadership Needed to Address Information Security Weaknesses and Privacy Issues
14. GAO-06-833T, Preventing and Responding to Improper Disclosures of Personal Information

DOD BLANKET ROUTINE USES

DoD has established 'Blanket Routine Uses' for all Department of Defense maintained systems of records. These apply to each system of records unless specifically stated otherwise within the particular record system notice. These additional routine uses are published only once in each DoD Component's Preamble in the interest of simplicity, economy and to avoid redundancy.

1. Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

2. Disclosure When Requesting Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

3. Disclosure of Requested Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4. Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

5. Private Relief Legislation Routine Use: Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular A-19, at any stage of the legislative coordination and clearance process as set forth in that Circular.

6. Disclosures Required by International Agreements Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

7. Disclosure to State and Local Taxing Authorities Routine Use: Any information normally contained in Internal Revenue Service (IRS) Form W-2 which is maintained in a record from a system of records maintained by a DoD Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, and 5520 and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

8. Disclosure to the Office of Personnel Management Routine Use: A record from a system of records subject to the Privacy Act and maintained by a DoD Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

9. Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

10. Disclosure to Military Banking Facilities Overseas Routine Use: Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer

DOD BLANKET ROUTINE USES

DoD has established 'Blanket Routine Uses' for all Department of Defense maintained systems of records. These apply to each system of records unless specifically stated otherwise within the particular record system notice. These additional routine uses are published only once in each DoD Component's Preamble in the interest of simplicity, economy and to avoid redundancy.

that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

11. Disclosure of Information to the General Services

Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

12. Disclosure of Information to the National Archives

and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

13. Disclosure to the Merit Systems Protection Board

Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

14. Counterintelligence Purpose Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

15. Data Breach Remediation Purposes Routine Use (May

10, 2007; 72 FR 26607): A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

16. Information Sharing Environment Routine Use

(December 28, 2007; 72 FR 73781): A record from a system of records maintained by a Component consisting of, or relating to, terrorism information (6 U.S.C. 485(a)(4)), homeland security information (6 U.S.C. 482(f)(1)), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment, November 22, 2006) may be disclosed to a Federal, State, local, tribal, territorial, foreign governmental and/or multinational agency, either in response to its request or upon the initiative of the Component, for purposes of sharing such information as is necessary and relevant for the agencies to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) and Executive Order 13388 (October 25, 2005). *NOTE: Information relating to, but not in and of itself constituting, terrorism, homeland security, or law enforcement information, as defined above, may only be disclosed upon a showing by the requester that the information is pertinent to the conduct of investigations of, or the development of analyses regarding, terrorism.*

Contents of a DoD Privacy Act System of Records Notice (DoD 5400.11-R)

C6.3.2. System Identifier. The system identifier must appear on all system notices and is limited to 120 positions, unless an exception is granted by the Defense Privacy Office, including Component code, file number and symbols, punctuation, and spacing.

C6.3.3. System Name

C6.3.3.1. The name of the system reasonably identifies the general purpose of the system and, if possible, the general categories of individuals involved.

C6.3.3.2. Use acronyms only parenthetically following the title or any portion thereof, such as, "Defense Civilian Payroll System (DCPS)." Do not use acronyms that are not commonly known unless they are preceded by an explanation.

C6.3.3.3. The system name may not exceed 55 character positions, unless an exception is granted by the Defense Privacy Office, including punctuation and spacing.

C6.3.3.4. The system name should not be the name of the database or the IT system if the name does not meet the criteria in subparagraph C6.3.3.1.

C6.3.4. System Location

C6.3.4.1. For systems maintained in a single location provide the exact office name, organizational identity, and address.

C6.3.4.2. For geographically or organizationally decentralized systems, specify each level of organization or element that maintains a segment of the system, to include their mailing address, or indicate that the official mailing addresses are published as an Appendix to the Component's compilation of system of records notices, or provide an address where a complete listing of locations can be obtained.

C6.3.4.3. Use the standard U.S. Postal Service two-letter State abbreviation symbols and 9-digit Zip Codes for all domestic addresses.

C6.3.5. Categories of Individuals Covered by the System

C6.3.5.1. Set forth the specific categories of individuals to whom records in the system pertain in clear, easily understood, non-technical terms.

C6.3.5.2. Avoid the use of broad over-general descriptions, such as "all Army personnel" or "all military personnel" unless this actually reflects the category of individuals involved.

C6.3.6. Categories of Records in the System

C6.3.6.1. Describe in clear, non-technical terms the types of records maintained in the system.

Contents of a DoD Privacy Act System of Records Notice (DoD 5400.11-R)

C6.3.6.2. Only documents actually maintained in the system of records shall be described, not source documents that are used only to collect data and then destroyed.

C6.3.7. Authority for Maintenance of System

C6.3.7.1. Cite the specific provision of the Federal statute or Executive Order that authorizes the maintenance of the system.

C6.3.7.2. Include with citations for statutes the popular names, when appropriate (for example, Section 2103 of title 51, United States Code, "Tea-Tasters Licensing Act"), and for Executive Orders, the official title (for example, Executive Order No. 9397, "Numbering System for Federal Accounts Relating to Individual Persons").

C6.3.7.3. If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

C6.3.7.4. If direct or indirect authority does not exist, the DoD, as well as the Army, Navy, and Air Force general "housekeeping" statutes (e.g., section 301 of 5 U.S.C.) may be cited if the Secretary, or those offices to which responsibility has been delegated, are required to collect and maintain systems of records in order to discharge assigned responsibilities. If the housekeeping statute is cited, the regulatory authority implementing the statute within the Department of Defense or Component also shall be identified.

C6.3.7.5. If the SSN is being collected and maintained, Executive Order 9397 shall be cited.

C6.3.8. Purpose or Purposes

C6.3.8.1. List the specific purposes for maintaining the system of records by the Component.

C6.3.8.2. All internal uses of the information within the Department or Component shall be identified. Such uses are the so-called "internal routine uses."

C6.3.9. Routine Uses

C6.3.9.1. Except as otherwise authorized by Chapter 4 of this Regulation, disclosure of information from a system of records to any person or entity outside the Department of Defense (See subparagraph C4.1.2) may only be made pursuant to a routine use that has been established for the specific system of records.

C6.3.9.2. Each routine use shall include to whom the information is being disclosed and what use and purpose the information will be used. Routine uses shall be written as follows:

C6.3.9.2.1. "To....[person or entity outside of DoD that will receive the information] to....[what will be done with the information] for the purpose(s) of ...[what objective is sought to be achieved]."

C6.3.9.2.2. To the extent practicable, general statements, such as “to other Federal agencies as required,” or “to any other appropriate Federal agency” shall be avoided.

C6.3.9.3. Blanket routine uses have been adopted that apply to all Component system notices. The blanket routine uses appear at the beginning of each Component’s compilation of its system notices.

C6.3.9.3.1. Each system notice shall contain a statement whether or not the blanket routine uses apply to the system.

C6.3.9.3.2. Each notice may state that none of the blanket routine uses apply or that one or more do not apply.

C6.3.10. Policies and Practices For Storing, Retiring, Accessing, Retaining, and Disposing of Records. This caption is subdivided into four parts:

C6.3.10.1. Storage. Indicate the medium in which the records are maintained. For example, a system may be “automated, maintained on compact disks, diskettes,” “manual, maintained in paper files,” or “hybrid, maintained in a combination of paper and automated form.” Storage does not refer to the container or facility in which the records are kept.

C6.3.10.2. Retrievability. Specify how the records are retrieved (for example, name, SSN, or some other unique personal identifier assigned the individual).

C6.3.10.3. Safeguards. Identify the system safeguards, such as storage in safes, vaults, locked cabinets or rooms, use of guards, visitor registers, personnel screening, or password protected IT systems, encrypted IT systems. Also identify personnel who have access to the systems. Do not describe safeguards in such detail as to compromise system security.

C6.3.10.4. Retention and Disposal. Indicate how long the record is retained. When appropriate, also state the length of time the records are maintained by the Component, when they are transferred to a Federal Records Center, time of retention at the Records Center and when they are transferred to the National Archivist or are destroyed. A Reference to a Component regulation without further detailed information is insufficient. If records are eventually destroyed instead of retired, identify the method of destruction (e.g., shredding, burning, pulping).

C6.3.11. System Manager(s) and Address

C6.3.11.1. List the title and address of the official responsible for the management of the system.

C6.3.11.2. If the title of the specific official is unknown, such as for a local system, specify the local commander or office head as the systems manager.

C6.3.11.3. For geographically separated or organizationally-decentralized activities for which individuals may deal directly with officials at each location in exercising their rights, list the position or duty title of each category of officials responsible for the system or a segment thereof.

C6.3.11.4. Do not include business or duty addresses if they are listed in the Component address directory.

C6.3.12. Notification Procedures

C6.3.12.1. Describe how an individual may determine if there are records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

C6.3.12.2. As a minimum, the caption shall include:

C6.3.12.2.1. The official title (normally the system manager) and official address to which the request is to be directed;

C6.3.12.2.2. The specific information required to determine if there is a record of the individual in the system;

C6.3.12.2.3. Identification of the offices through which the individual may obtain notification; and

C6.3.12.2.4. A description of any proof of identity required. See paragraph C3.1.3. of Chapter 3.

C6.3.12.3. When appropriate, the individual may be referred to a Component official, who shall provide this information to him or her.

C6.3.13. Record Access Procedures

C6.3.13.1. Describe how an individual can gain access to the records pertaining to him or her in the system. The procedural rules may be cited, but include a brief procedural description of the needed data. Provide sufficient information in the notice to allow an individual to exercise his or her rights without referral to the formal rules.

C6.3.13.2. As a minimum, the caption shall include:

C6.3.13.2.1. The official title (normally the system manager) and official address to which the request is to be directed;

C6.3.13.2.2. A description of any proof of identity required. (See paragraph C3.1.3. of Chapter 3); and

Contents of a DoD Privacy Act System of Records Notice (DoD 5400.11-R)

C6.3.13.3. When appropriate, the individual may be referred to a Component official, who shall provide the records to him or her.

C6.3.14. Contesting Record Procedures

C6.3.14.1. Describe how an individual may contest the content of a record pertaining to him or her in the system.

C6.3.14.2. The detailed procedures for contesting a record need not be identified if the Component procedural rules are readily available to the public. (For example, “The Office of the Secretary of Defense” rules for contesting contents are contained in 32 CFR 311.) All Component procedural rules are set forth at a Departmental public Web site (see <http://www.defenselink.mil/privacy/cfr-rules.html>).

C6.3.14.3. The individual may also be referred to the system manager to determine these procedures.

C6.3.15. Record Source Categories

C6.3.15.1. Describe where (the individual, other Component documentation, other Federal agencies, etc.) the information contained in the system was obtained.

C6.3.15.2. Specific individuals or institutions need not be identified by name, particularly if these sources have been granted confidentiality. See paragraph C5.4.2. of Chapter 5.

C6.3.16. Exemptions Claimed for the System

C6.3.16.1. If no exemption has been claimed for the system, indicate “None.”

C6.3.16.2. If an exemption is claimed, cite the exemption as well as identifying the CFR section containing the exemption rule for the system.

C6.3.17. Maintaining the Master DoD System Notice Registry

C6.3.17.1. The Defense Privacy Office maintains a master registry of all DoD record systems notices.

C6.3.17.2. The Defense Privacy Office also posts all DoD system notices to a public Web site (see <http://www.defenselink.mil/privacy/notices>).



ADMINISTRATION AND
MANAGEMENT

OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

MEMORANDUM FOR DEPARTMENT OF DEFENSE (DoD) FREEDOM OF
INFORMATION ACT (FOIA) PUBLIC LIASONS

SUBJECT: The Office of Government Information Services (OGIS)

The OPEN Government Act of 2007 amended the FOIA by establishing the OGIS within the National Archives and Records Administration and assigned responsibility to FOIA Public Liasons to assist in the resolution of FOIA disputes. Public Law 110-175 states that the OGIS shall:

- review policies and procedures of agency FOIA programs;
- review agency compliance with the FOIA;
- recommend FOIA policy changes to Congress and the President;
- offer mediation services to resolve disputes between FOIA requesters and agencies as an alternative to litigation; and
- issue advisory opinion, at the discretion of the OGIS, if mediation has not resolved a dispute.

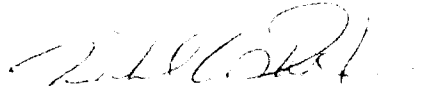
When a FOIA requester contacts OGIS to resolve a dispute, the OGIS will directly contact either the DoD FOIA Public Liasons or an alternative point of contact. If an alternative point of contact is identified, the applicable component shall provide the alternate's contact information to both OGIS and the Defense Freedom of Information Policy Office (DFOIPO) to ensure that future contacts are made appropriately.

After initial contact by OGIS, the DoD FOIA Public Liaison will attempt to resolve the dispute with the requester without further OGIS assistance. The applicable DoD FOIA Public Liaison will advise DFOIPO and OGIS of the outcome. If OGIS decides to pursue resolution of disputes which are not resolved by the DoD FOIA Public Liaison, OGIS will make appropriate inquiries of both the requester and the Public Liaison as to whether the disputed issue is a candidate for mediation. If OGIS determines that both of the interested parties (DoD and the requester) would agree to mediation, OGIS will contact DFOIPO. DFOIPO will then work with the DoD Alternative Dispute Resolution (ADR) Liaison to identify a shared neutral venue for the mediation process. The decision to accept or reject the offer of mediation services will be made by the applicable DoD Component in accordance with the Component's ADR policy and issuances after consulting with DFOIPO.



When the mediation is completed, OGIS may issue an advisory opinion pursuant to Public Law 110-175. When applicable, DFOIPO will consult with the DoD Office of General Counsel and notify the concerned DoD FOIA Public Liaison of the Department's views regarding the OGIS' advisory opinion.

I have also requested that all contacts concerning OGIS' responsibilities to review policies and procedures of agency FOIA programs and agency compliance with the FOIA be directed to me. A copy of my letter to OGIS explaining this guidance is attached. My point of contact for this is Ms. Stephanie Carr, DFOIPO, (703) 588-6807.



Michael L. Rhodes
Director

Attachment:
As stated

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

Personally Identifiable Information

PII

“Detect it, Protect it, Report it, Prevent it”



What You Will Learn

- **What is Personally Identifiable Information (PII).**
- **Why safeguarding PII is critical.**
- **How to keep PII secure in the workplace.**
- **What to do if there is a PII information breach.**



Purpose

This training will help all DLA civilian and military employees, to include contractors, understand the procedures for the proper handling and storage of personally identifiable information (PII) included under

- the Privacy Act of 1974, and
- For Official Use Only (FOUO) requirements.



What is PII

Personally Identifiable Information is personal information about an individual that identifies, links, relates, is unique to, or describes him or her, that can be used to distinguish or trace an individual's



Home Phone Number
Personnel Information

Financial Transactions

Medical Information

Social Security Number

Personal E-mail Address



What is PII: Examples

PII is a combination of either your name or Social Security Number linked with each other or with other personal information. The following are examples of other personal information:

Age

Marital status

Race and national origin

Home phone number

Home address

Medical information

Financial transactions

Mother's maiden name

Biometric information, i.e., fingerprints

**This is NOT an
all-inclusive list.**



What is PII: Where is it Found?

PII can be found in electronic & paper-based formats in places such as:

- Web sites
- Mobile/remote devices (e.g., PDA, Blackberry, cell phones)
- E-mail and attachments
- Filing cabinets
- Binders on bookshelves
- Shared online folders
- Local drives (C:) on desktop or laptop PCs
- Removable media (e.g., floppy disks, CDs, memory sticks, flash memory, etc.)
- Databases/business applications (e.g., Defense Travel System)



What is PII: What Form Can it Take?

Location – Common examples of hardcopy / electronic records containing PII.

- Timekeeping records
- Travel records
- Personnel files
- Medical documentation
- Recall lists
- Legal files
- Criminal investigations



What is PII: What Form Can it Take?

Form – Files & records containing PII are found in both hardcopy and electronic form.

- Hardcopy files in folders and binders
- Web pages and Web applications
- Word Processing files (e.g., MS Word®)
- Spreadsheet files (e.g., MS Excel®)
- E-mail and attachments
- PDF Files—such as those created by most copiers in use throughout DLA



Safeguarding PII is Critical

The following list identifies why safeguarding PII is critical.

- Protecting and safeguarding PII is the law.
- Respecting our employees' and customers' privacy is a cornerstone of our business and a core value.
- Protecting our employees' and customers' personal information is essential when doing business with DLA.
- Protecting our bond of trust and keeping it strong must be an ongoing effort.
- Personal privacy is at stake.



Penalties and Repercussions

Possible administrative, disciplinary, and criminal penalties.

- Unauthorized disclosure of personal information subject to the Privacy Act is prohibited and subject to possible criminal penalties and/or administrative actions.
- DLA and our employees, military members, and contractors are subject to civil and criminal penalties for certain breaches of privacy (*misdemeanor criminal charges and fines up to \$5,000*).
- DLA is diligent in pursuing appropriate actions against individuals who violate privacy rules.



Safeguards Employed By DLA

Safeguards must:

- Be Administrative, Technical, and Physical.
- Be based on the storage media (paper, electronic, etc.) used.
- Ensure the security and confidentiality of records.
- Protect against any anticipated threats or hazards to the security or integrity of records.
- Prevent compromise or misuse during storage, transfer, or use, including working at authorized alternative worksites.





How To Keep PII Secure

What To Do:

- Challenge ANYONE who asks to see PII in your possession.
- Mark privacy records appropriately: “FOUO: Privacy Act.”
- Collect the minimum amount of PII necessary for the proper performance of a documented agency function.
- Safeguard at a level equal to the risk and degree of harm resulting from the loss, misuse, or unauthorized access.



How To Keep PII Secure

What To Do:

- Ensure that PII is accessible only to those authorized to have access. Confidentiality is one of the cornerstones of information security.
- If you are ever in doubt or have a question relating to the Privacy Act, contact your local Privacy Act Officer.
- To learn more about the Privacy Act and for names of the Privacy Act Officers, go to DLA's Privacy Act web-site at:

<http://www.dla.mil/FOIA-Privacy>



How To Keep PII Secure

What Not To Do:

- DO NOT collect PII without proper authorization.
- DO NOT distribute or release PII to other employees unless you know that the release is authorized.
- DO NOT use interoffice or translucent envelopes to mail paperwork with PII.



How To Keep PII Secure

What Not To Do:

- DO NOT place PII on local drives, shared drives, e-mail folders, multi-access calendars, or the Intranet (eWorkplace or Outlook) unless it is password protected or encrypted.
- DO NOT place PII on the Internet under any circumstances.
- DO NOT create a "System of Records" before contacting your local Privacy official or local Counsel.



Privacy Act System of Records

A System of Records

- is a group of records under the control of a DoD Component,
- contains personal information about an individual, and
- is retrieved by the name of the individual or by some other personal information unique to the individual.



Privacy Act System of Records


Examples of System of Records include:

- Facility Access Records (badging/motor vehicle information)
- Personnel Security Files
- EEO records



Securing PII

Marking PII / FOUO Material



PRIVACY ACT - FOR OFFICIAL USE ONLY

**Mark document “Privacy Act – For Official Use Only”
at the top and bottom of each page or screen.**

Applies whether you create or receive documents.



THE MATERIAL/INFORMATION CONTAINED HEREIN FALLS
WITHIN THE PURVIEW OF THE **PRIVACY ACT of 1974** AND WILL
BE SAFEGUARDED IN ACCORDANCE WITH THE APPLICABLE
SYSTEM OF RECORDS NOTICE AND 32 CFR PART 323.

DLA FORM 1461, JULY 2005

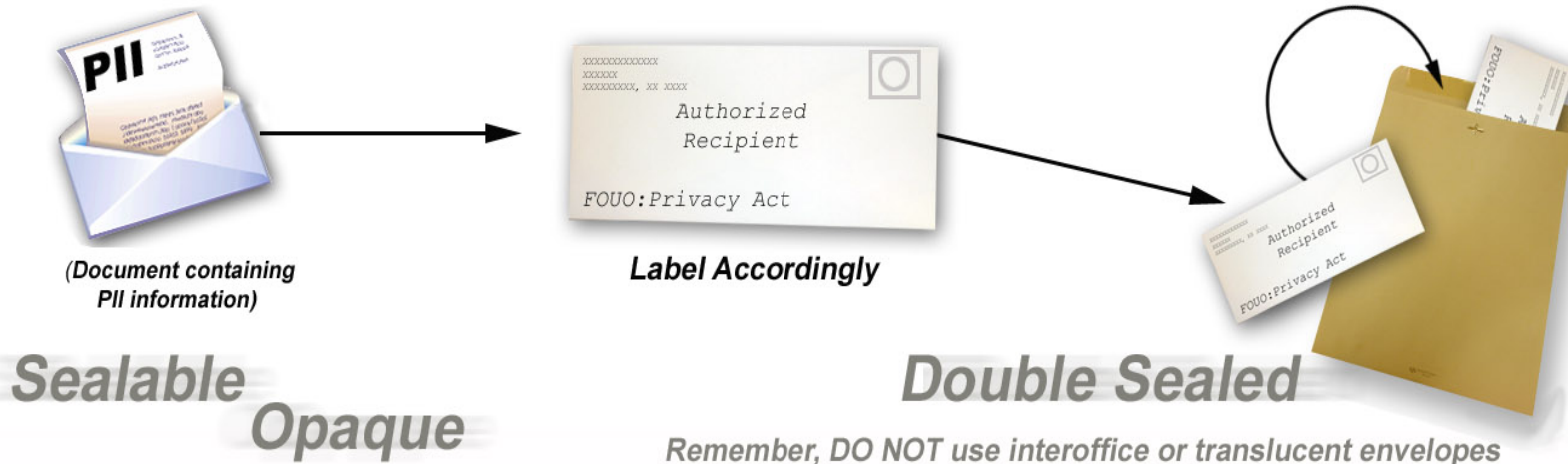
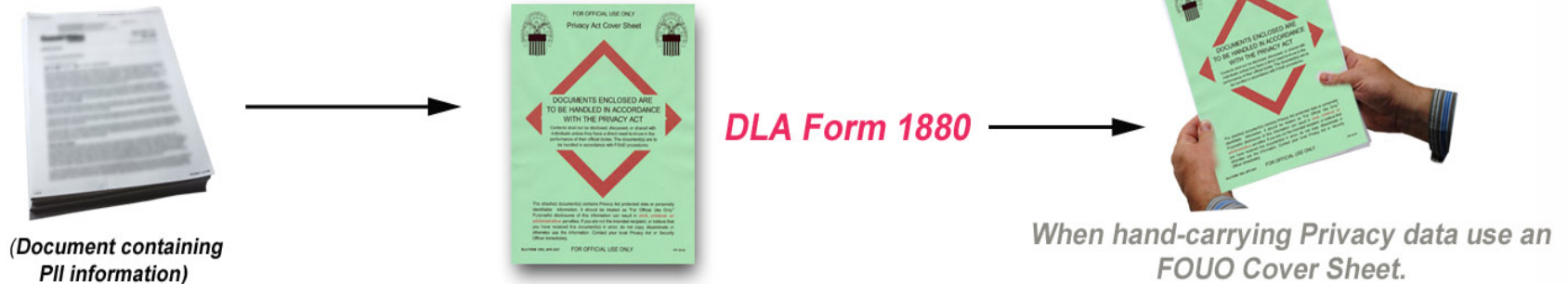
Mark housing devices with DLA Form 1461, Privacy Act Label



Securing PII

Transmitting PII/FOUO Material—Hard Copy

Prevent Disclosure of Privacy/FOUO Contents





Securing PII

Transmitting PII/FOUO Material—Electronic

Prevent Disclosure of Privacy/FOUO Contents

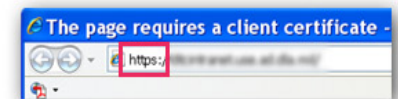
Electronic Mail

*Electronic mail
will be encrypted and
digitally signed using
Common Access Card (CAC).
In the subject line/opening sentence
state you are sending FOUO material.*



Intranet

*Via the Intranet use
Secure Socket Layer (SSL)
connections.*



"https" rather than "http."



Disposing of PII

Disposing of PII / FOUO material:

- A disposal method is considered adequate if it leaves the information unrecognizable or beyond reconstruction.
- The two authorized disposal methods for DLA are burning and shredding. Consult your supervisor to determine which is in use at your activity.
- Comply with DLA Records Management Procedures.



Information Breach & the Consequences

- An information breach is the loss, theft, or compromise of PII whether in electronic or physical form.
- Consequences of an information breach include
 - substantial harm, embarrassment, inconvenience, or unfairness to an individual,
 - negative consequences for the DLA Enterprise, and
 - potential legal ramifications.



Reporting a Breach

Upon discovery you must report the incident to:

Network Operations & Security Center (NOSC)

Call 1-877-DLA-NEMO / 1.877.352.6366

**All PII breaches must be reported
to the NOSC immediately!**

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The DLA seal is a circular emblem. It features a globe in the background with a grid of latitude and longitude lines. Overlaid on the globe is an eagle with its wings spread, perched atop a shield. The shield has a blue top section with white stars and a bottom section with red and white vertical stripes. A yellow banner curves around the top of the globe with the word "LOGISTICS" in blue. Two other yellow banners curve around the sides of the globe, with "DEFENSE" on the left and "AGENCY" on the right, both in blue.

DLA FOIA/PRIVACY WORKSHOP

DAY 2

WELCOME

Mickey Slater, 703.767.2171

DLA Information Management Control Officer

October 27, 2010

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DLA FOIA/PRIVACY WORKSHOP

Information Collections

Mickey Slater, 703.767.2171

DLA Information Management Control Officer

October 27, 2010



DOD Requirement

- DOD policy is that we license all information collections or surveys that require responses from internal DLA, internal DOD, other Federal Agencies, or 10 or more members of the public.
- We are expected to control and minimize costs and burden (time spent) associated with the collection and reporting of information.



DOD Policies

- DOD Directive 8910.1 “Management and Control of Information Requirements”
- DOD Manual 8910.1 “DOD Procedures for Management of Information Requirements”
- DOD Instruction 1100.13, “Surveys of DOD Personnel”



Types of Approvals

- DLA Report Control Symbol – respondents are from DLA only or other Federal Agencies (30-day turnaround)
- AT&L – respondents include military services (30-day turnaround). Use Form SD455.
- OMB – respondents are expected to include 10 or more members of the public (5-month approval process, allowing for Federal Register comments and OMB decision). Use OMB Form 83-I, “Paperwork Reduction Act Submission” package.
- Degree requirement for student – approval is needed by only the manager of the office involved. Add note on the survey “necessary for degree requirement. RCS not required.”



Process

- If you are planning an information collection:
 - Obtain management buy-in
 - Notify DLA IMCO (Mickey Slater)
 - Define who your respondents will be to determine which approval will be needed.
 - Forward the draft survey to the IMCO.
 - If an AT&L approval is needed, the survey will be reviewed by Defense Manpower Data Center.
 - If OMB approval is needed, Federal Register Notices must be posted for 90 days to alert the public of the survey plan.
 - All approval numbers will be delivered to the IMCO. Then the IMCO will deliver the RCS, AT&L, or OMB number to the customer. The customer will place the approval number on the survey.




Successful Collections

- Minimal burden time
- User-friendly surveys or collections
- Good response rate
- Quality information obtained

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The DLA seal is a circular emblem featuring a globe with a grid of latitude and longitude lines. A bald eagle with its wings spread is perched atop a shield with vertical red and white stripes. A yellow banner arches over the eagle with the word "LOGISTICS" in black capital letters. Two vertical yellow banners on either side of the shield contain the words "DEFENSE" and "AGENCY" respectively.

DLA FOIA/PRIVACY WORKSHOP

Forms Management Program

Sylvia Nance, DLA Forms Manager
October 27, 2010



DLA Forms Management Program

Governance – DLA is mandated to:

- Establish & manage a forms management program to implement:
 - DoD Instruction 7750.07, DoD Forms Management Program
 - DoD 7750.07-M, DoD Forms Management Program Procedures Manual
- Establish internal procedures for creating, revising, distributing, and canceling DLA-level forms
 - DLA Instruction 5302, DLA Forms Management Program (<http://www.dla.mil/dlaps>)
- Reduce or eliminate the use of SSNs wherever possible in accordance with:
 - Directive-Type Memorandum 07-015-USD(P&R) – DoD Social Security Number (SSN) Reduction Plan, March 28, 2008



DLA Forms Management Program

Definition of a Form:

A fixed arrangement of captioned spaces designed to collect, compile, display, transmit, or analyze prescribed information quickly and efficiently, regardless of media. An official form can be in hard copy, soft copy (electronic) or a web-based interfacing/output tool.



DLA Forms Management Program

All DLA Forms Shall:

- Have a prescribing document or issuance mandating its use.
- Be designed in Adobe Designer (the Forms Program's approved software application).
- Satisfy a valid need – information collected shall be essential to accomplish a mission need and necessary for the efficient and economical operations of DLA and DoD.
- Properly designed with clear instructions and standardized data for easy processing and retrieval of information collected in accordance with DoD 7750.7-M.



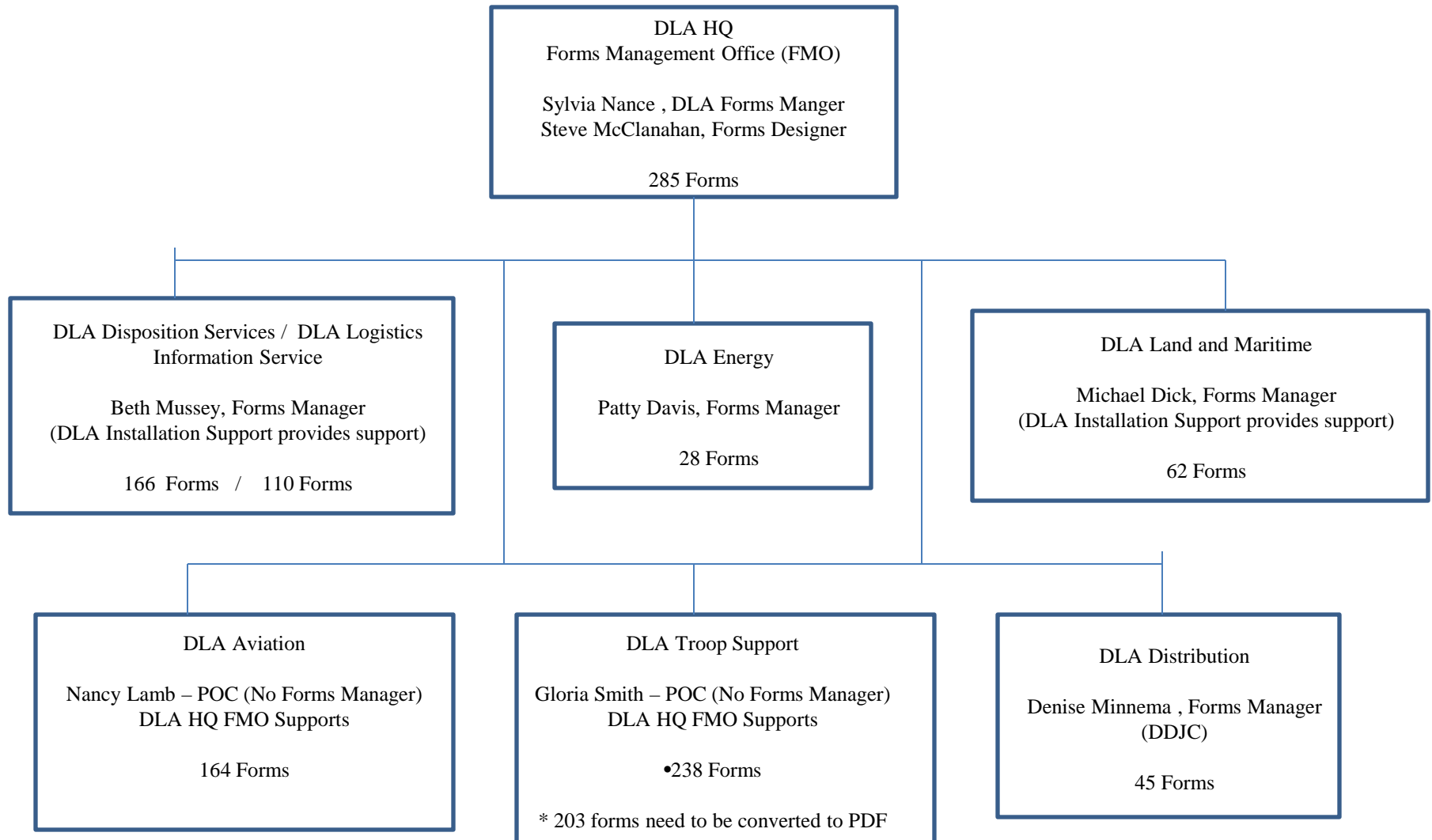
DLA Forms Management Program

All DLA Forms Shall:

- Reduce or eliminate the use of the Social Security Number within forms wherever possible in accordance with DTM 07-015-USD(P&R).
- Promote the use of technology to facilitate the creation, distribution, and use of electronic forms.
- Promote the use of electronic transactions and electronic signatures in accordance with Public Laws 105-277, Government Paperwork Elimination Act and 106-229, Electronic Signatures in Global and National Commerce Act of 2000.



DLA Forms Management Program



Total DLA Forms = 1098
DD forms sponsored by DLA = 68



DD Form 67

FORM PROCESSING ACTION REQUEST (Read instructions on back and in DoD 7750.07-M before completing this form.)				1. DATE OF REQUEST (YYYYMMDD)	
2. FROM (DoD Component OPR Organization and complete mailing address)		3. THRU (DoD Component FMO Organization and complete mailing address)		4. TO (Organization and complete mailing address)	
5. FORM DESIGNATION AND NUMBER (Leave blank if a new form)		6. EDITION DATE (Enter only if cancelling a form)		7. FORM TITLE	
8. ACTION TYPE (Select one)		9. FORM TYPE (Select one)		10. SUBJECT GROUP (Leave blank if a new form)	
11. PRESCRIBING ISSUANCE(S)		12. FORM DISPOSITION (List all forms to be replaced by proposed form)		13. PROPOSED FORM DESIGN CONSIDERATIONS	
a. FORM NUMBER (Enter "N/A" if none)		b. EDITION DATE		c. DISPOSITION	
d. DESIGN TYPE		e. SUGGESTED SIZE		f. PRINTING SPECIFICATIONS	
g. CLASSIFIED		h. CONTROLLED FORM		i. DIGITAL SIGNATURE FIELD	
j. AVAILABILITY (Select one)					
14. PURPOSE AND DESCRIPTION OF USE (Attach continuation page if necessary.)					
15. INTERNAL COORDINATION AND CONCURRENCE					
(1) APPLICABLE CABLE (Yes/No)		(2) REMARKS (Enter applicable remarks related to coordination, and attach appropriate documentation. If space permits, enter coordinator email address here.)		(3) COORDINATOR	
a. PRIVACY ACT				NAME	
b. POSTAL				OFFICE SYMBOL	
c. DATA ELEMENTS				TELEPHONE NO. (Include area code/DSN)	
d. RECORDS MGMT				EMAIL ADDRESS	
e. OTHER				INITIALS	
f. REPORTS					
RCS					
OMB					
16. EXTERNAL COORDINATION AND CONCURRENCE (Not required for SD, DoD Component, or Command forms. Attach continuation page if necessary.)					
a. DOD COMPONENT		b. COORDINATOR			
NAME		OFFICE SYMBOL		TELEPHONE NO. (Include area code/DSN)	
EMAIL ADDRESS		INITIALS			
CERTIFICATION OF DOD COMPONENT OPR AND/OR ACTION OFFICER, APPROVING OFFICIAL, AND FMO I hereby certify that all of the above coordinations have been completed as indicated.					
17. DOD COMPONENT OPR AND/OR ACTION OFFICER					
a. TYPED NAME AND TITLE		b. TELEPHONE NUMBER (Include area code/DSN)		c. SIGNATURE	
18. DOD COMPONENT APPROVING OFFICIAL					
a. DATE SIGNED (YYYYMMDD)		b. TYPED NAME, TITLE, AND SIGNATURE			
19. DOD COMPONENT OR COMMAND FORMS MANAGEMENT OFFICER					
a. DATE SIGNED (YYYYMMDD)		b. TYPED NAME, TITLE, AND SIGNATURE			
20. APPROVING FORMS MANAGEMENT OFFICER					
a. TYPED NAME		b. DATE SIGNED (YYYYMMDD)		c. SIGNATURE	

From and To Section

Meta data about the form

Mandatory Coordination Section

For Non-DLA forms only

Signatures and Approval



Mandatory Coordination Section

15. INTERNAL COORDINATION AND CONCURRENCE						
	(1) APPLICABLE? (Yes/No)	(2) REMARKS (Enter applicable remarks related to coordination, and attach appropriate documentation.) (If space permits, enter coordinator email address here.)	(3) COORDINATOR			
			NAME	OFFICE SYMBOL	TELEPHONE NO. (Incl. area code/DSN)	INITIALS
a. PRIVACY ACT						
b. POSTAL						
c. DATA ELEMENTS						
d. RECORDS MGMT						
e. OTHER						
f. REPORTS						
RCS						
OMB						

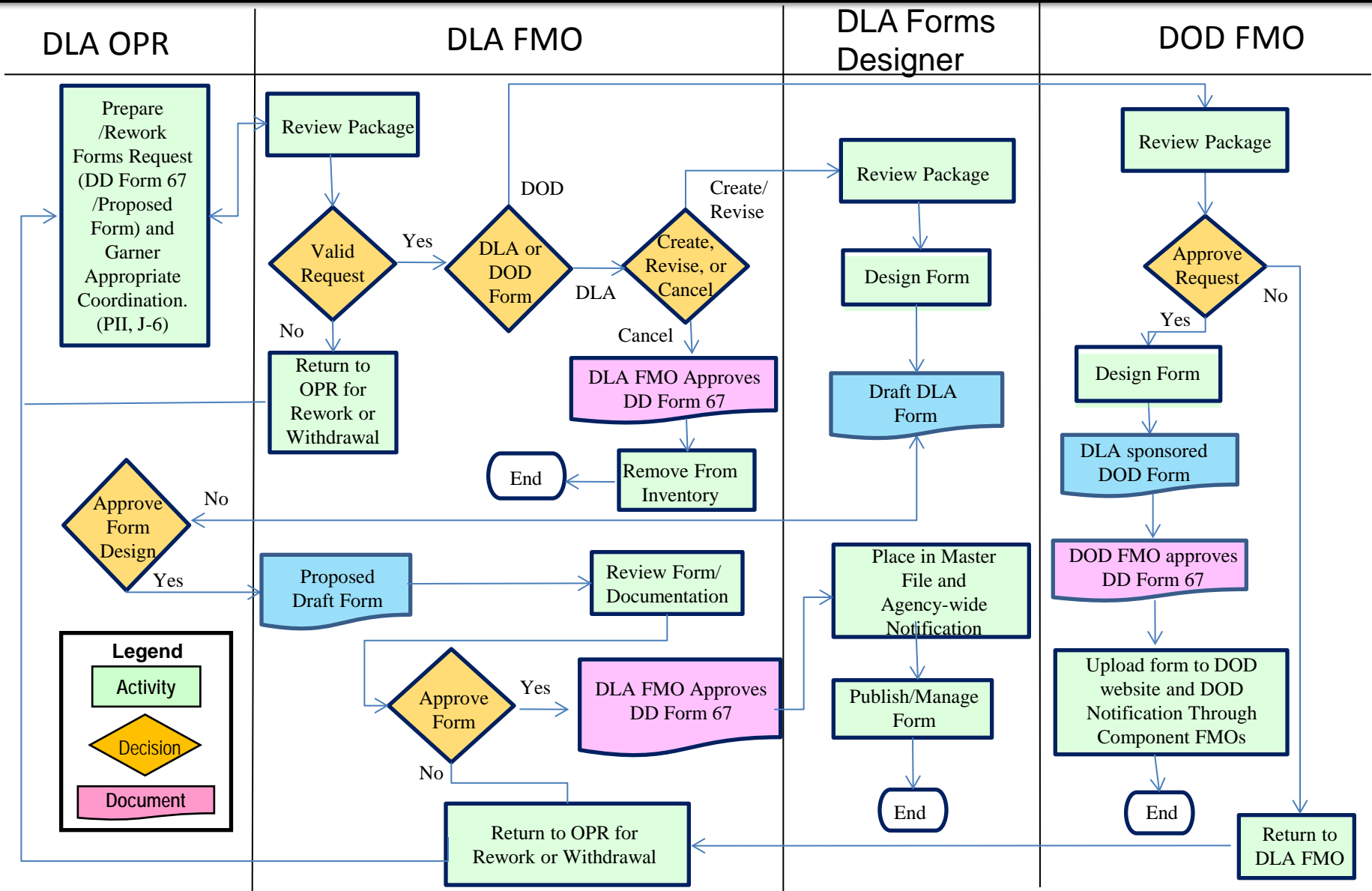
16. EXTERNAL COORDINATION AND CONCURRENCE (Not required for SD, DoD Component, or Command forms. Attach continuation page if necessary.)

Within the originating Component, obtain the coordination of the Component Program Manager for each of the programs listed. The Program Manager will determine applicability and coordinate on the form where indicated.

- 15.a. Privacy Act: DoD 5400.11-R, DoD Privacy Program, will apply if an individuals SSN, home address, home phone number or other personal information is requested on the form.
- 15.b. Postal: DoD 4525.8-M, DoD Official Mail Manual, will apply if the form is used as any type of mailer. The form shall be designed to meet USPS requirements and specifications.
- 15.c. Data Elements: In accordance with DoD Directive 8320.02, Data Sharing in a Net-Centric Department of Defense, all forms requests require coordination with the DoD Component data administration POC.
- 15.d. Records Mgmt: Enter the records disposition schedule under “remarks” in accordance with DLA Instruction 5304, Records Management.
- 15.f. Reports: DoD 8910.1-M, Department of Defense Procedures for Management of Information Requirements will apply if a form is used as an instrument to collect information from subordinate commands within a DoD Component, other DoD Component, other Federal agencies, or the public. The appropriate report control data must be displayed on the form and controlled as instruments to collect information.



DLA Forms Management Program





References

References are attached to the DLA Forms
Management Program Slide Handout

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The logo of the Defense Logistics Agency (DLA) is centered in the background. It features a globe with a yellow banner arched over the top that says "LOGISTICS". A bald eagle with spread wings is perched on a shield with vertical red and white stripes. The shield is set against a blue background with white stars. The words "DEFENSE" and "AGENCY" are written vertically on banners on either side of the shield.

DLA FOIA/PRIVACY WORKSHOP

Privacy Impact Assessments

Mr. Chris Requa, J-651

Leonard.Requa@dla.mil

703.767.4975

October 27, 2010



PIA Overview

- A Privacy Impact Assessment (PIA) is an analysis of whether personally identifiable information (PII) in electronic form is collected, stored, shared, and managed in a manner that protects the privacy of individuals and reduces the risk to their information.
- Section 208 of the E-Government Act of 2002 requires all Federal government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates PII on the public.



Essential Elements of the PIA

- What privacy information is collected
- Why the information is collected
- What the intended uses are for the information
- With whom the information is shared
- What opportunities individuals have to decline to provide PII
- How information is secured
- Whether a System of Records Notice (SORN) exists
- What privacy risks need to be addressed



When is a PIA Required?

- If PII is collected, a PIA is required for the following conditions:
 - For existing DoD information systems and electronic collections for which a PIA has not previously been completed to include systems that collect PII about Federal personnel and contractors.
 - For new information systems or electronic collections a PIA will be completed:
 - Prior to developing or purchasing new information systems or electronic collections
 - When converting paper-based records to electronic systems.



When is a PIA not Required?

PIAs are NOT required for:

- Systems that do not contain, process, or transmit PII
- National Security Systems



PRIVACY IMPACT ASSESSMENT (PIA)
For the

Enter DoD Information System/Electronic Collection Name
Enter DoD Component Name

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- ☐ (1) Yes, from members of the general public.
- ☒ (2) Yes, from Federal personnel* and/or Federal contractors.
- ☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- ☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☒ **New DoD Information System** ☐ **New Electronic Collection**
☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**
☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number **12464**
☐ **Yes, SIPRNET** Enter SIPRNET Identification Number
☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes** ☐ **No**
If "Yes," enter UPI **007-97-01-02-02-0002-00**
If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes** ☐ **No**
If "Yes," enter Privacy Act SORN Identifier **F024 AF USTRANSCOM A**
DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk

PIA	SORN
What privacy information is collected	Categories of Records in the System
Why the information is collected	Authority/Purpose(s)
What the intended uses are for the information	Purposes(s)
With whom the information is shared	Routine Uses
What opportunities individuals have to decline to provide PII	Privacy Act Statement/Notification procedure
How information is secured	Safeguards
What privacy risks need to be addressed	Narrative Statement/Probable or potential effects on the privacy of individuals.
Whether a System of Records Notice (SORN) exists	(Not applicable) Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk

PIA	SORN
<p data-bbox="19 511 685 554">What privacy information is collected?</p> <ul data-bbox="115 614 598 756" style="list-style-type: none"><li data-bbox="115 614 598 656">• Nature of the information<li data-bbox="115 714 598 756">• Scope of the information	<p data-bbox="985 511 1603 554">Categories of Records in the System</p> <ul data-bbox="1081 614 1893 806" style="list-style-type: none"><li data-bbox="1081 614 1893 806">• Describe the types of individually identifiable information maintained in the system, e.g., social security number, date of birth, patient medical history, school applications

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.



Yes

Enter OMB Control Number

Enter Expiration Date



No

Information Collection website:

<http://www.reginfo.gov/public/do/PRAMain>

Example OMB control number: [0701-0026](#)

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

EXAMPLE:

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; DoD Instruction 1100.13, Surveys of DoD Personnel; DoD Directive 6490.2, Comprehensive Health Surveillance; DoD Directive 6490.3, Deployment Health; DoD Directive 1404.10, Civilian Expeditionary Workforce; AR 600-63, The Army Health Program and E.O. 9397(SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Purpose:
Briefly describe the types of Personal Information

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

SAMPLE words:

Identity theft, blackmail and public embarrassment are some of the risk associated with the Personally Identifiable Information (PII) and Protected Health Information (PHI) collected by this system. These risks are addressed by the use of strong passwords or smart cards used to access the system, Advanced Encryption Standards (AES), encryption of data at rest and in transit, and finally role-based security, which ensures that access to the Information in the system is limited by job requirement and authorization to view the data.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.



Within the DoD Component.



Specify.



Other DoD Components.



Specify.

Other Federal Agencies.



Specify.



State and Local Agencies.

Specify.



Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.



Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?



Yes

☐

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

SAMPLE words:

Initial consent occurs prior to the set up of NCAT testing. Individuals are alerted by test proctors of the demographics data collection. A second consent opportunity is provided by clicking the "Save" button on the NCAT demographics collection screen presented to the tested individuals. However, to successfully proceed into the NCAT test process, individual~ must provide consent and the First Name, Last Name, SSN, Date of Birth and Gender information must be recorded by clicking "Save. "

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?



Yes

☐

No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

SAMPLE words:

The information collected is used for the specific purposes of evaluating treatment of TBI and providing feedback on further psychological health care. PII/PHI is only used and disclosed as permitted by 000 6025.18-R. Individuals are alerted to the voluntary nature of providing their PHI. To successfully proceed into the NCAT test process, individuals must sign a form that complies with section C5.2 and C5.3 of 000 6025.18-R. Choosing to sign or not sign this form gives individuals the opportunity to give or withhold consent to providing their PHI.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.



☒ Privacy Act Statement



Other



Privacy Advisory



None

Describe
each
applicable
format.

SAMPLE words:

A Privacy Act Statement is presented to individuals prior to beginning the NCAT testing and prior to each of their PII/PHI being collected.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Other Names Used | <input checked="" type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Truncated SSN | <input type="checkbox"/> Driver's License | <input type="checkbox"/> Other ID Number |
| <input checked="" type="checkbox"/> Citizenship | <input type="checkbox"/> Legal Status | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Birth Date | <input checked="" type="checkbox"/> Place of Birth |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number | <input type="checkbox"/> Personal Email Address |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Security Clearance |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Mother's Middle Name | <input type="checkbox"/> Spouse Information |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Biometrics | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Medical Information | <input type="checkbox"/> Disability Information |
| <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Employment Information | <input type="checkbox"/> Military Records |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Education Information | <input type="checkbox"/> Other |

If "Other," specify or explain any PII grouping selected.

SAMPLE words:

Other PII may be "sensitive" depending on its context

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Describe here.

The source of the PII collected will be the individual, Defense Enrollment Eligibility Reporting System (DEERS), Ambulatory Data System DEERS (ADS DEERS) extract, Common Access Card (CAC), and AHLTA. This will be a paperless transaction.

(3) How will the information be collected? Indicate all that apply.



☒ Paper Form



☐ Telephone Interview



☐ Email



☐ Information Sharing - System to System



☐ Other



☒ Face-to-Face Contact



☐ Fax



☐ Web Site

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

SAMPLE words:

We verify the individual's credentials to access the system; we identify the individual as being the right person to have the NCAT assessment performed on; we authenticate that the user is authorized to use the system; we match the collected demographics data to the individual's identity record to ensure proper association of the NCAT record to the unique individual's identity.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

SAMPLE words:

Mission is supported by identifying and treating those individuals with TBI to ensure NCAT information becomes a permanent part of their medical history.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)



Yes



No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

SAMPLE words:

The possible impacts to an individual's privacy are mitigated through the de-identification of the aggregated data. When the data is aggregated it is de-identified to ensure that no PII/PHI is available in the reports. Additionally, reports are accessed based on user-defined criteria and are controlled by an access control list. Access to the NCAT is restricted to individuals who require the data in the performance of official duties.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.



☒ Users



Developers



☒ System Administrators



☒ Contractors



Other

If "Other," specify here.

d. How will the PII be secured?



(1) Physical controls. Indicate all that apply.



☒ Security Guards



☒ Identification Badges



☐ Key Cards



☒ Safes



☐ Cipher Locks



☒ Combination Locks



☐ Closed Circuit TV (CCTV)



☐ Other

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.



☐ User Identification



☒ Password



☐ Intrusion Detection System (IDS)



☒ Encryption



☐ External Certificate Authority (CA) Certificate



☐ Other



☒ Biometrics



☒ Firewall



☐ Virtual Private Network (VPN)



☒ DoD Public Key Infrastructure Certificates



☐ Common Access Card (CAC)

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☐ Methods to Ensure Only Authorized Personnel Access to PII
- ☐ Encryption of Backups Containing Sensitive Data
- ☒ Backups Secured Off-site
- ☐ Other

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ Yes. Indicate the certification and accreditation status:

- | | | | |
|-------------------------------------|---|---------------|--------------|
| <input checked="" type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | 10 June 2010 |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | |

☐ No, this DoD information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Describe here.

SAMPLE words:

Collection: Members PII information is collected with their urinalysis sample via a bar code on the sample bottle. Drug and Alcohol Abuse Reports (DAARs) are input directly into the ADMITS database through the web application.

Use, Retention, and Processing: Only personnel with the "need to know" can access a member's PII information.

Disclosure: No other personnel other than those with a "need to know" can access a member's PII information unless permission is granted from the individual in writing to release the information.

Destruction: Data is destroyed in accordance with the Navy's Records Management Manual.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe here.

SAMPLE words:

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.

Mitigation (example responses):

The following controls are used to mitigate the risks:

a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.

b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.

d) Audits. This includes review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.

e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.

f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers.

An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

**Program Manager or
Designee Signature**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Senior
Information Assurance
Officer Signature or
Designee**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Privacy Officer
Signature**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component CIO Signature
(Reviewing Official)**

COCOM CIO

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.



DLA CIO PIA Process

1. A PIA is required if it is determined that an information system or electronic collection of information will collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally.
2. Program Manager (PM) or designee drafts the PIA using DD Form 2930 and forwards an unsigned version to J-651 (Leonard.Requa@dla.mil) for review.



DLA CIO PIA Process (*cont.*)

3. J-65 will review the PIA for completeness.

- J-651 coordination process to include (when applicable):
 - DLA Information Management Control Officer reviews for requirements under the Paperwork Reduction Act
 - DLA Records Manager reviews to ensure the collection has an approved records retention IAW DLA Records Management Program
 - DLA Forms Manager reviews to ensure collection mechanism (whether paper or electronic) meets with the requirements of the DLA Forms Program
 - J-61 reviews when PIAs are submitted without ATO data
 - J-62 reviews to ensure IT system is documented in DITPR & ProSight



DLA CIO PIA Process (*cont.*)

4. Once J-651 has completed its review, the PIA is emailed to the DLA FOIA/Privacy Office for review and coordination.
5. Any outstanding issues identified are rectified by J-651.
6. Signatures are obtained (in this order)
 - Program Manager (or designee)
 - Information Assurance Manager/Officer
 - DLA FOIA/Privacy Office (Mr. Lewis Oleinick)
 - DLA CIO



DLA CIO PIA Process (*cont.*)

7. After all signatures are obtained, the PIA is posted to the DLA PIA web page:

<http://www.dla.mil/j-6/PIA.aspx>

and a copy of the PIA is sent to the DoD CIO:

pia@osd.mil.

8. Final step is to ensure that the PIA fields in DITPR and Prosight are updated and that the information is consistent.



Backup Material



PIA Guidance

- **M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002**
 - <http://www.whitehouse.gov/sites/default/files/omb/memoranda/m03-22.html>
- **DoD PIA guidance**
 - DoDI 5400.16, Privacy Impact Assessment Guidance
 - <http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf>
 - DD Form 2930, Privacy Impact Assessment
 - <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo/3438.html>
 - DoD CIO Privacy Impact Assessment Web Site
 - <http://cio-nii.defense.gov/policy/pia.shtml>



Definition of Personal Information

- Personal Information. Information about an individual **maintained by the agency** that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information also is known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).
Reference: DoD 5400.11-R



Additional Definitions

- Certification & Accreditation
 - Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
 - Accreditation: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.



Additional Definitions

National Security System (NSS)

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency,

- (1) the function, operation, or use of which:
 - involves intelligence activities;
 - involves cryptologic activities related to national security;
 - involves command and control of military forces;
 - involves equipment that is an integral part of a weapon or weapon system; or
(subject to Subparagraph (B)*) is critical to the direct fulfillment of military or intelligence missions; or
- (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

*Subparagraph B – Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 44 U.S.C. 3542, Federal Information Security Management Act of 2002)



PIA Review and Update Cycle

- Review and update of existing PIAs for DoD information systems must be synchronized with the information system's certification and accreditation (C&A) cycle.
- Review and update of existing PIAs for electronic collections must be completed within 3 years of PIA approval date.
- Review and update of a PIA is required when a significant system change or a change in privacy or security posture occurs.

(Per DODI 5400.16)

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DLA FOIA/PRIVACY WORKSHOP

DLA Records Management

Kayte Vo, DLA Records Manager

October 27, 2010



Purpose

To provide an informational briefing about the DLA Records Management (RM) Program including:

- RM overview
- Program strategy
- Accomplishments
- Current initiatives
- Relation to FOIA/Privacy issues



Agenda

☐ Records Management

- Records Lifecycle
- Why is RM Important?
- RM in the Spotlight

☐ RM Overview

- What is a Record?
- Records Schedules and Series
- Types of Records
- DLA Records Schedule

☐ DLA RM Program

- RM Program Revitalization Strategy
- RM Program Status
- RM Roles and Responsibilities

☐ RM Practical Approaches

- File Plan
- Unscheduled Records

☐ Getting Help

☐ Questions?



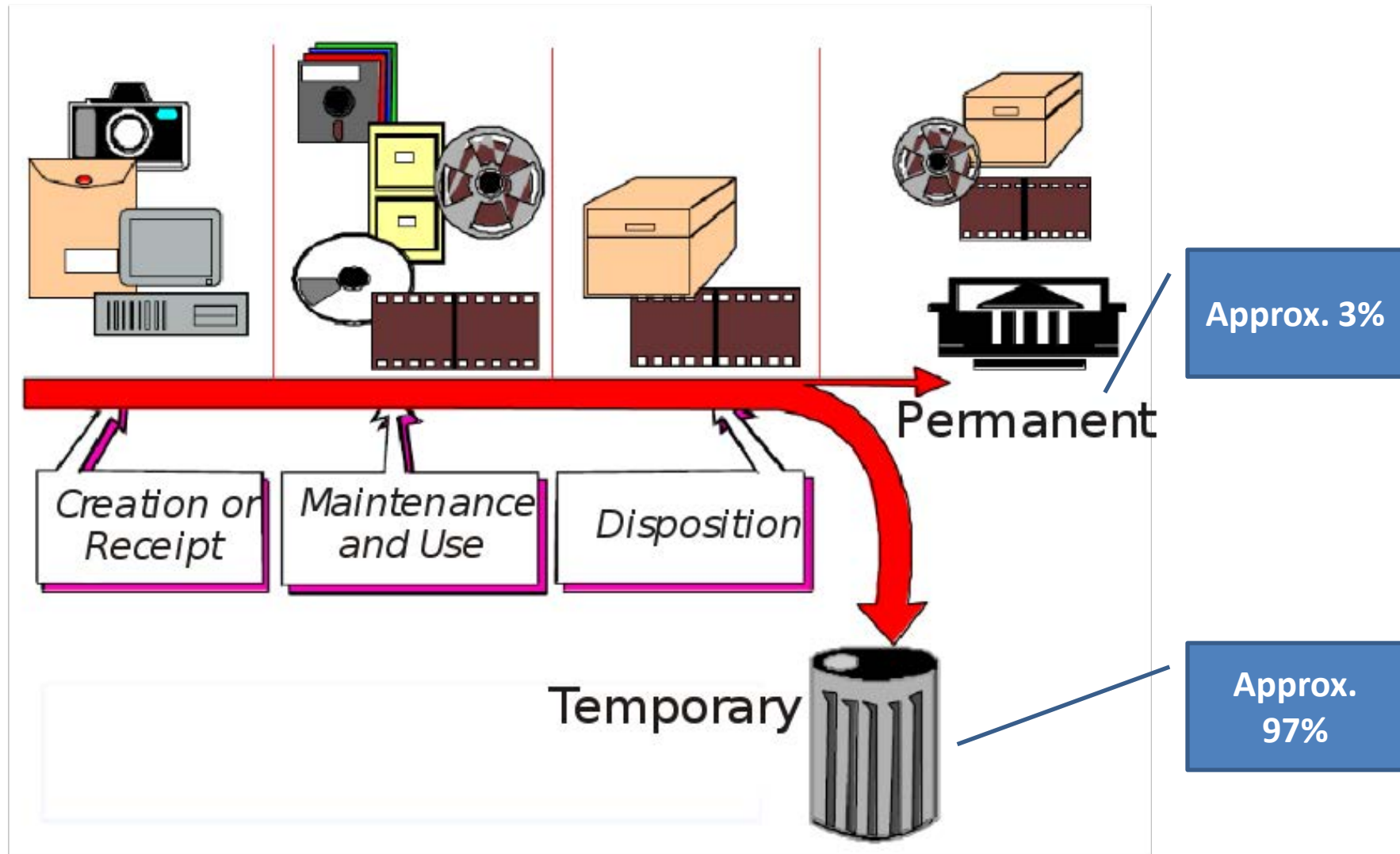
Records Management

- Under the Federal Records Act, each federal agency is required to make and preserve records that:
 - Document the organization, functions, policies, decisions, procedures, and essential transactions of the agency
 - Provide the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities

(44 U.S.C. § 3101)



Records Lifecycle





Why is RM Important?

1. It's the law!
2. Records document Agency activities and protect legal and financial rights.
3. Keeping records longer than required takes up space and creates unnecessary storage costs.
4. Records remain subject to FOIA requests and legal discovery if they are kept past the approved retention period.
5. Practicing RM can help you get organized and make it easier to find the information you need.



RM in the Spotlight

- Open Government Initiative
 - “There can be no accountability if the Government does not preserve—and cannot find—its records...Good records management is the backbone to open government.”
 - David S. Ferriero, Archivist of the United States

(Prepared remarks of Archivist of the United States David S. Ferriero at the Department of the Treasury, Washington, DC, April 1, 2010)
- Poor records management is highly publicized
 - “Records are like oxygen. Nobody really notices them until they’re gone.”
 - Cass R. Sunstein, Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget

(Cass Sunstein, “Keynote Address: Open Government and the Implications for Federal Agencies,” presented at NARA RACO 2010, May 12, 2010)



What is a Record?

- Records are defined in 44 U.S.C. 3301 as including:
 - ``all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics,
 - made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business
 - and preserved or appropriate for preservation by that agency or its legitimate successor
 - as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them."



A record...

1. Can be in any format, paper or electronic.
 2. Is something you create in carrying out your official duties or something you receive in carrying out your duties that requires you to take action.
 3. Is appropriate for preservation. (If you think something is worth documenting as evidence of your work, then it is appropriate for preservation.)
 4. Is evidence of the Agency or its functions, policies, decisions, procedures, operations, or other activities.
- ❖ Extra copies of materials kept only as reference and publication stock are NOT records.



Records Schedules and Series

- A Records Schedule identifies types of records, called records series, produced by an agency and their corresponding retention requirements.
- Within a records schedule, records are divided into records series, a group of related records having the same retention.
- Each records series has its own disposition instruction, which defines how long to maintain the records and what to do with them once the retention requirement has been met.



Types of Records

1. Administrative records common to all agencies are included in the General Records Schedule (GRS) created by the National Archives and Records Administration (NARA).
2. Program records specific to DLA are “scheduled” individually. The DLA Records Manager defines each program records series and submits a proposed retention period to NARA via SF-115. Upon NARA approval, the new series is added to the DLA Records Schedule and becomes legally binding and mandatory.

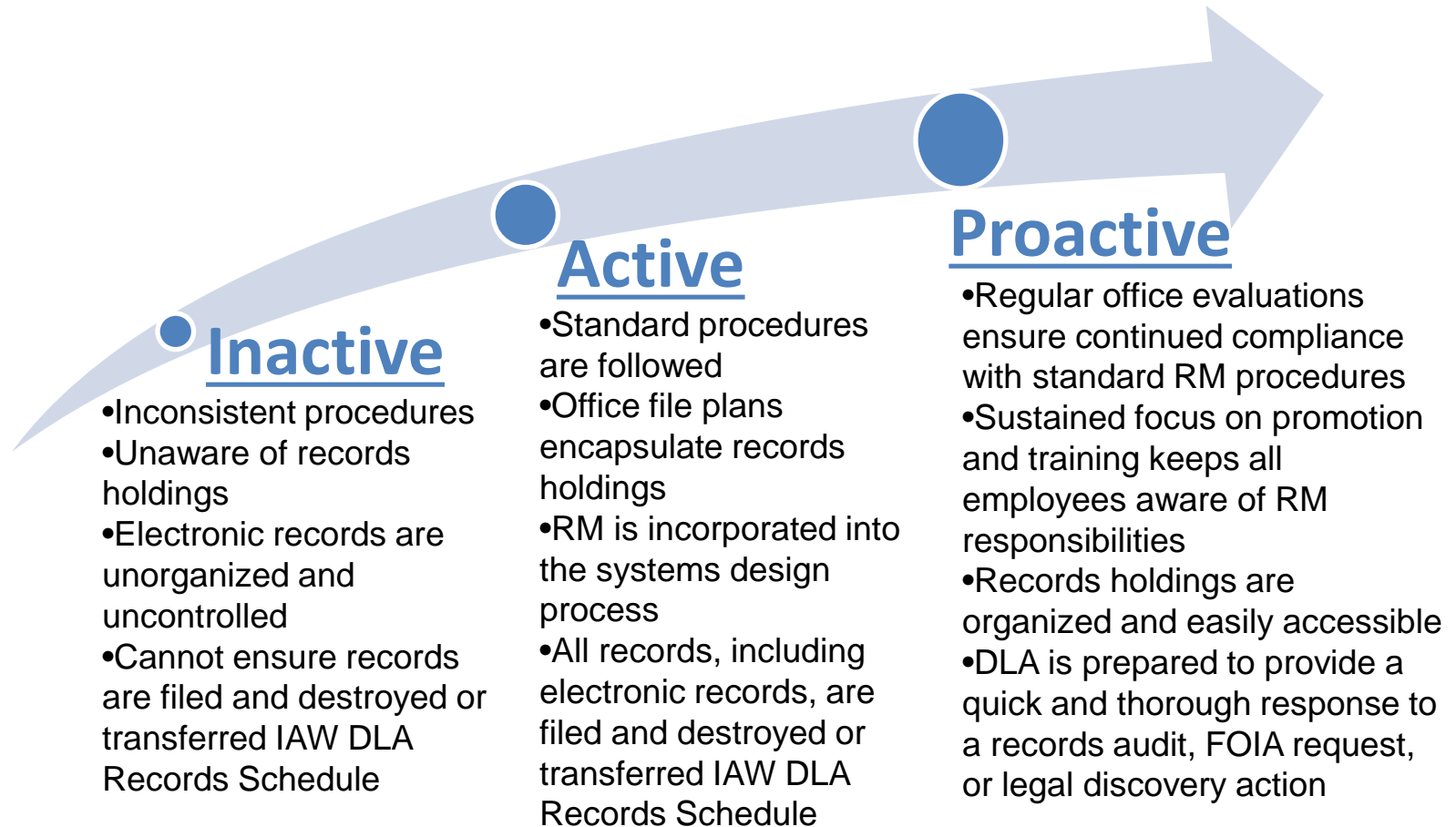


DLA Records Schedule

- Both GRS records series and DLA-specific records series are incorporated into the comprehensive DLA Records Schedule, found here: <https://headquarters.dla.mil/J-6/records/tools.asp>
- The DLA Records Schedule is the **ONLY** authoritative source for records series and disposition instructions (retention requirements) approved for use by DLA.
 - Sometimes regulations or other policy sources specify time periods for records retention. These requirements are incorporated into the NARA-approved records series that appear in the DLA Records Schedule.
 - If a new/updated regulation or policy instruction specifies a time period for records retention, this should be used as justification to modify the DLA Records Schedule. Contact your Component Records Officer to initiate changes to the DLA Records Schedule.



DLA RM Program Revitalization Strategy





DLA Records Management Program

Description of Project

- Establish governance necessary to manage the creation, maintenance, and disposition of DLA paper and electronic records.
- Authorities: Title 44 U.S.C.; Ch XII, Title 36 CFR; DODD 5015.2; Vol I, AI 15; DLAI 5304

Recent Accomplishments

- Completed NARA 2010 RM Assessment*
- Updated DLA Annual RM Training**
- Arranged funding for FY11 records storage and servicing (\$148,220)
- Increased EIS scheduling completion from 62% to 90%

Current Initiatives

- Complete EIS scheduling
- Update RM procedures
- Modernize DLA Records Schedule

Overall Status

- RM POC network established, making progress with RM training and awareness

G

Annual RM Training
January 2011

NARA 2011 RM Assessment
May 2011

Streamline DLA Records
Schedule by Sept 2012

Update RM Procedures;
Finish EIS scheduling
March 2011

RM Site Visits
2011

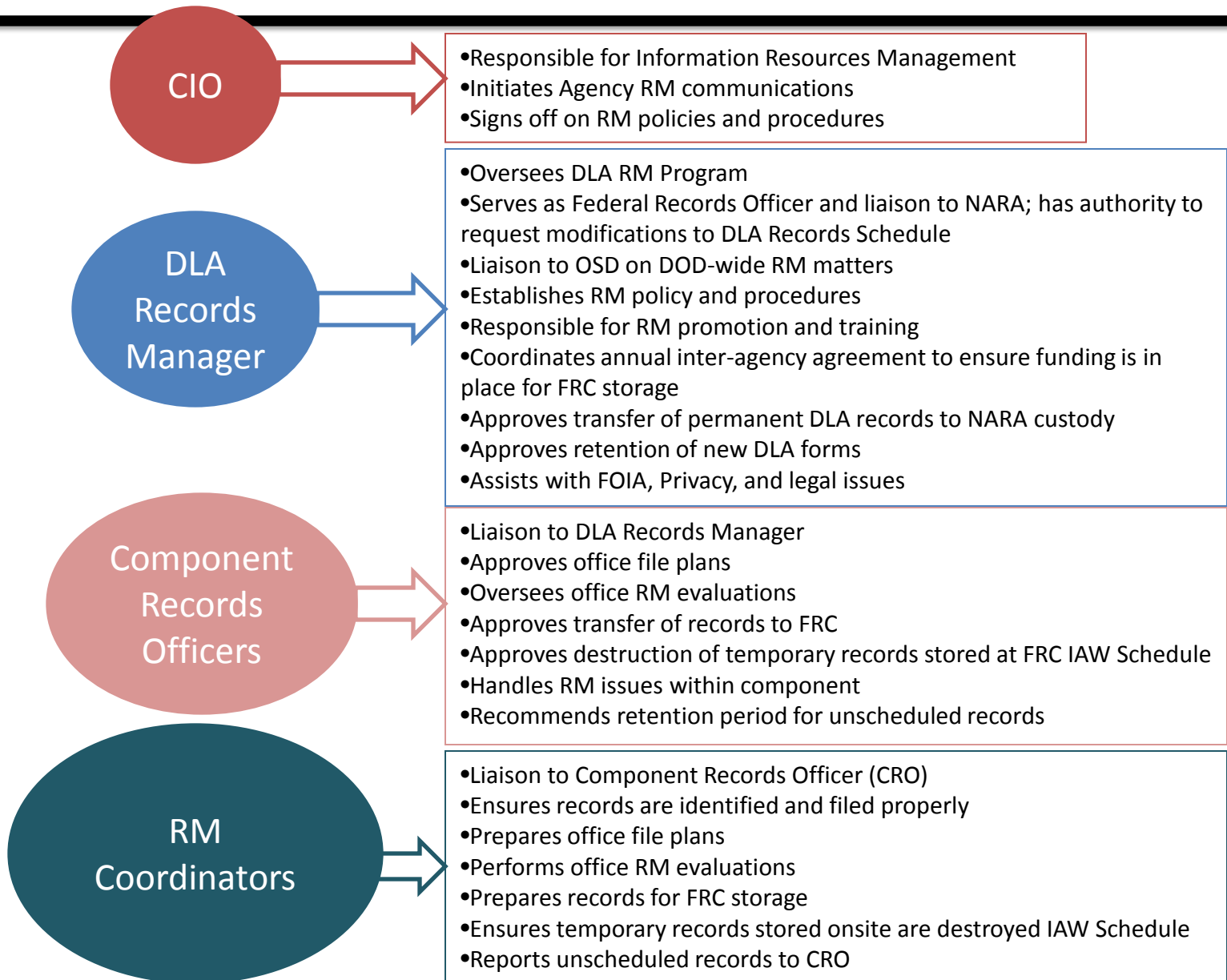
On schedule and no
significant issues

Behind schedule with
significant issues

Behind schedule
With mission impact



RM Roles & Responsibilities





RM Practical Approaches

- If your component has not yet implemented a certified RMA to automate Records Management, you can still take practical steps to organize and control both your paper and electronic records.
 1. Create a file plan to identify which records series from the DLA Records Schedule you use, where you store those records, and how long to keep them.
 - Tip: The DLA 1689 form is a file plan template. The form is currently in the process of being reinstated.



File Plan

- Outlines each group of records within an office
- Describes the records in detail including:
 - Title
 - Beginning and ending dates
 - Format
 - Location
 - Disposition instruction and date
 - Whether or not the records are Vital Records
- Tip: Be as specific as possible when completing a file plan. Spell out acronyms and be descriptive.
 - Records are often disposed of years after they were created. The person carrying out the disposition is usually not the same person that created the records, and they may not be familiar with the record content.



DLA File Plan Form

Office:

Date Prepared:

Prepared By (Name, Title, & Phone):

RM Coordinator (Name, Title, & Phone):

Approved By (Name, Title, & Phone, to be completed by Component Records Officer):

<u>Vital Records</u> Indicate Y/N.	<u>Records Series</u> Mark UNSCHEDULED if records cannot be assigned to any existing records series in the DLA Records Schedule.	<u>Records Title</u>	<u>Records Description</u> Spell out acronyms and include pertinent dates.	<u>Format & Location</u> Indicate if the records are kept on paper (P), electronically (E), or both (B). Describe the exact location (physical location of paper records, pathname of shared folder, room and folder in eWorkplace, etc). If records are kept both electronically and on paper, indicate which version is considered the official record.	<u>Records Disposition & Disposition Authority</u>
<u>Example:</u> N	510.16B	FY10 Records Management routine correspondence and memoranda.	FY10 Routine correspondence and memoranda regarding the DLA Records Management program, such as general inquiries. Does not include records disposition or scheduling.	B – Official records are on paper. (P) Top drawer of filing cabinet in Kayte Vo's cubicle, 5450 Carlisle Pike, Bldg 9, Mechanicsburg, PA 17050. Approx. 2 cubic ft. (E) \\mdt1sp0008\hq users\kvo\Work\510_16B FY10 Routine Correspondence Destroy October 2012; 72.1 MB.	Destroy when 2 years old. GRS 16, Item 2b. Cutoff FY10 records on September 30, 2010. Destroy October 1, 2012.



Unscheduled Records

- Records that are not associated with any existing records series in the DLA Records Schedule are called unscheduled records.
- DO NOT destroy unscheduled records!
- Contact your Component Records Officer to initiate the process of creating a new records series to be added to the DLA Records Schedule.



RM Practical Approaches (cont'd)

2. Organize your shared drive and e-mail archive folders by records series and date, and file records accordingly.
 - For example, a folder entitled “510_16B FY10 RM Routine Correspondence” could be placed on the shared drive to capture documents and spreadsheets. A folder with the same title could be placed within the archive structure in Outlook to capture e-mails.



RM Practical Approaches (cont'd)

3. Establish an annual Records Clean-up Day to review your paper and electronic records and destroy the temporary records that have met their retention.
 - Tip: Have Records Clean-up Day the first Monday in January. Both records arranged by fiscal year and by calendar year will have met retention by this time.



RM Practical Approaches (cont'd)

4. On Records Clean-up Day, use your file plan to find records due for destruction and the location of those records.

- Tip: Enter the specific date the records become eligible for destruction in the Disposition column of the file plan (Example: “Destroy October 1, 2012”). It will make it easier to quickly scan this column to find records past due for destruction.
- Tip: You can also add the destroy date to the folder name to make it easier to search for electronic records due for destruction. Example: “510_16B FY10 RM Routine Correspondence Destroy October 1 2012”

5. Follow appropriate security procedures to destroy records.



Getting Help



- List of DLA CROs: <https://headquarters.dla.mil/j-6/records/faq.asp>
- DLA RM Policy Instruction: Located in eWorkplace under Resources -> DLA Issuances -> Records Management (DLAI 5304)
- DLA RM Tools (Procedural Guide, Evaluation Guide, DLA Records Schedule):
<https://headquarters.dla.mil/j-6/records/tools.asp>
- National Archives and Records Administration (NARA): <http://www.archives.gov/records-mgmt/>



Questions?



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY





Break time!



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DLA FOIA/PRIVACY WORKSHOP

Systems of Records Notices

Cindy Allard, Chief of the OSD/JS Privacy Office

Jody Sinkler, Privacy Officer, DLA HQ

October 27, 2010



Systems of Records Notices

- **Required by the Act (5 U.S.C. 552a(e)(4))**
- **Format prescribed by Federal Register Document Drafting Handbook**
- **Act covers records maintained in a “system of records” that are retrieved by an individual’s name or other personal identifier**
- **Penalties for non-compliance**
- **Reviewed every two years for accuracy**



Systems of Records Notices

- DLA's UNIQUE SYSTEM NUMBER
- System name:
- System location:
- Categories of individuals covered by the system:
- Categories of records in the system:



Systems of Records Notices

- Authority for maintenance of the system:
- Purpose(s):
- Routine uses of records maintained in the system, including categories of users and the purposes of such uses:
- Disclosure to consumer reporting agencies:



Systems of Records Notices

- Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:
- Storage:
- Retrievability:
- Safeguards:
- Retention and disposal:



Systems of Records Notices

- System manager(s) and address:
- Notification procedure:
- Record access procedures:
- Contesting record procedures:
- Record source categories:
- Exemptions claimed for the system:



Penalties for Non-compliance

- **Civil Remedies**

- The cost of actual damages suffered (\$1000 minimum)
- Costs and reasonable attorney's fees.

- **Criminal Penalties**

- Charge of a misdemeanor
- Maximum fine of \$5,000



Privacy Partners

Keys to Success

- Identify what kinds of records you are maintaining that are retrieved by a name and/or personal identifier
- Relationships are key-
 - program managers,
 - forms managers,
 - records managers
 - IMCOs
 - CIO / IA / IT managers



Now That You Know

What should you do?

1. Locate your systems of records notices
2. Identify the systems managers
3. Look at the last date the document was updated
4. Ask questions to the systems managers
 - i. Is this still current?
 - ii. Are we still conducting business this way?
 - iii. Are the individuals who work with the system aware of the notice – safeguards – retention requirements – disclosure accounting, etc?
5. Make appropriate changes
6. Make a strong administrative record of changes



Conduct Regular Reviews

1. Make it a point to review your systems of records regularly. After all, without regular review – the system of records notice loses its viability and visibility.
2. DITPR entries
3. DoD or Component forms
4. SSN Justifications
5. Privacy Impact Assessments
6. Records Management
7. Train! Train! Train!



Last Important Thought

Take The Pain Out Of The Process

- If you make the process hard or cumbersome it won't get done. By taking the pain out of the process, you build alliances and opportunities.
- The process never ends.

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY





Lunch!



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



OGIS/ADR/Public Liaison Training/Discussion

Ms. Beth Lagana, Associate General Counsel
Mr. Lewis Oleinick, DLA FOIA Public Liaison

October 27, 2010



Break Time!



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DLA PII Incident Handling Policies and Procedures: An Overview



PII Incident Policies and Procedures

- Statutory basis
- OMB Policy and DoD Regulation
- What needs to be reported?
- Overview of DLA PII Incident Policies and Procedures
 - The parties roles
 - Reporting time lines



Statutory Basis

- Why do we have to protect PII?
 - Privacy Act requirement to protect data is found in 5 U.S.C. § 552a (e)(10)
- Why do we have to report incidents?
 - OMB's authority to issue additional implementing guidance, regulations, and "continuing assistance" under the Privacy Act is found in 5 U.S.C. § 552a (v)(1) and (v)(2)



OMB and DoD Requirements

- OMB PII Breach Reporting
 - OMB Memorandum M-06-15, “SUBJECT: Safeguarding Personally Identifiable Information,” May 22, 2006.
 - OMB Memorandum M-06-19, “SUBJECT: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,” July 12, 2006
 - OMB Memorandum M-07-16, “SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” May 22, 2007.
- DoD Regulation (Protecting PII and Reporting Incidents, respectively)
 - 32 CFR § 310.13 and 32 CFR § 310.14



What needs to be reported?

- First some definitions
 - What is “personal information” or PII?
 - What is a “breach”?
 - What is “high risk”?
- Who should be called?
 - When an actual or potential breach is discovered the individual discovering it should immediately call:
 - 1-877-DLA-NEMO (352-6366)



The parties' roles

- The person who discovers the “breach”
- The NOSC
- The Incident Response Team (IRT)
 - The Field Activity
 - IAO or IAM → Electronic Incidents
 - Privacy Officer → Physical Incidents
 - Local Counsel
 - Accountability Office → AR 15-6 Investigations
- Headquarters – Involved with “High Risk” Breaches
 - HQ Privacy Officer
 - The CIO
 - The General Counsel
 - The Director



Incident Response Team

- Why Incident Response Team (IRT)?
 - Gov't-wide best practice is use of Incident Response Team for PII incidents
 - IRT's leverage maximum skill sets of experts from IT, Privacy (or Info Security), and Counsel
- IRT needs to ask, "Is notification necessary?"
 - Answer is based on results of outcome from Risk Analysis Model



Performing Risk Analysis

- Why use Risk Analysis Model
- Which Risk Analysis Model?
 - IRT should use Appendix B, “Likelihood Determination Methodology,” from DLA’s “Policies and Procedures when Personal Information is Lost, Stolen, or Compromised”
- What the heck is a “threat-source” anyway?
 - NIST Term
 - In short: to whom the PII was breached, or potentially breached.



Reporting Time Lines

- Immediately: Upon Discovery to the DLA NOSC
- Within 1 Hour of Discovery:
 - Electronic Incident
 - DLA NOSC notifies DLA Office with Primary Responsibility and HQ
 - DLA CERT determines if the PII has been accessed.
 - Physical Incident
 - Same as above, but with twist:
- Within 48 Hours:
 - Interim Report to Defense Privacy Office → HQ Privacy submits
- 10 Days (DoD Best Practice):
 - Final Report to Defense Privacy Office
 - Local Privacy Officer & IAM responsible to submit to HQ Privacy Office
- Each incident's report metrics are reported to the DLA General Counsel on a weekly basis.



Questions?



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DLA FOIA/PRIVACY WORKSHOP

DoD Breach Reporting

Jody Sinkler
Kathy Tennessee
October 28, 2010



DoD Breach Reporting

- Required by Chapter 10 of DoD 5400.11-R, Department of Defense Privacy Program (May 2007).
- DoD-wide template was developed by the Defense Privacy and Civil Liberties Office (DPCLO).



DoD Breach Reporting

- Reporting Timelines:
 - Within 24 hours SAOP is notified.
 - Interim Report
 - Within 48 hours due to DPCLO.
 - DGA prepares interim report from initial NOSC notification email, and sends it to DPCLO and the DLA Component Privacy Officer.
 - Final Reports
 - Currently no timeline.
 - DLA Component Privacy Officer must ensure report is accurate & complete.
 - Reports leave DLA!



DoD Breach Reporting

MEMORANDUM FOR DoD BREACH REPORTING

SUBJECT: Lost, Stolen, or Compromised PII Breach Report

REF: DLA NOSC Ticket #12345 (Interim / Final Report)

- 1.a. Date of Breach:
- 1.b. Breach Discovery Date:
- 2.a. US-CERT Number:
- 2.b. Date Reported to US-CERT:
3. Is this the initial report to the Defense Privacy Office? **Yes or No.**
(If **No**, what were the dates of the previous reports? **[enter dates of previous reports]** (Note: Report updates should be made in **RED** text.)



DoD Breach Reporting

4. DoD Component and organization involved:

Component Name **Defense Logistics Agency**

Organization [identify the DLA PLFA]

POC Title/Organization [usually this is the Privacy Official within the DLA PLA or could be the IAO/IAM]

Telephone [telephone number of the POC above]

Email [work email address of the POC above]

5. Person to contact for further information regarding this report.

Name **Patricia Kolonoski**

Address **DLA Distribution, Mission Drive, Building 81, New Cumberland, PA 17070-5000**

Title/Organization **DLA Distribution Privacy Officer**

Telephone **717-770-5238**

Email **Patricia.Kolonoski@DLA.MIL**



DoD Breach Reporting

5. Person to contact for further information regarding this report.

Name Jody Sinkler OR Kathy Tennessee OR Lewis Oleinick

Address Defense Logistics Agency Headquarters, 8725 John J.
Kingman Road, Fort Belvoir, VA 22060-6221

Title/Organization DLA HQ Privacy Officer

Telephone 703-767-5045

Email Jody.Sinkler@DLA.MIL



DoD Breach Reporting

6. Total number of individuals affected by breach: ____ Unknown: ____

Breakout number by category:

Government Civilians _____

Government Contractors _____

Military (Reserve) _____

Military (Dependent) _____

Military (Active) _____

Military (Retired) _____

Other/Unknown (*please specify*) _____



DoD Breach Reporting

7. Did this incident involve one of the following:

(select those that apply)

Paper Records

Info-Sharing

Equipment

Record Disposal

E-mail

Other *(specify)*



DoD Breach Reporting

7.a. If the incident involved equipment, what was lost, stolen or breached? How many pieces of equipment were involved in the incident? N/A ____

Type of Equipment	How Many
CPU	_____
External Hard drive	_____
Laptop	_____
IPOD	_____
Blackberry	_____
Cell Phone	_____
Data Stick	_____
Network Intrusion	_____
Flash drive	_____
Other (<i>specify</i>)	_____



DoD Breach Reporting

7.b. How was the equipment protected? *(select all that apply)*

- Personally Owned _____
- Password Protected _____
- Encryption Software installed _____
- PKI/CAC Enabled _____
- Contractor Owned _____
- Not protected _____
- Government Owned _____
- Other *(specify)* _____



DoD Breach Reporting

7.c. If the incident involved e-mail, select all that apply:

	Yes	No
E-mail was encrypted	_____	_____
E-mail sent outside of DoD	_____	_____
E-mail sent to non-Federal agency	_____	_____
Other (<i>specify</i>)	_____	_____



DoD Breach Reporting

7.d. Type of Personally Identifiable Information involved in the incident *(select all that apply)*:

Type of PII

Select all that apply

Name

Date of Birth

Social Security Number

Health information

Personal home address

Financial information

Personal telephone number

Password

Personal e-mail address

Other *(specify)*



DoD Breach Reporting

8. Description of breach *(150 words or less)*

- i. Facts and circumstances surrounding the loss, theft, or compromise. **In simple terms, explain the facts as we know them. Do not use any person's name when describing the incident. Always remember that these reports leave DLA.**
- ii. Was breach internal, external, accidental, or intentional? **Pick the appropriate explanation. This information must match with what you've provided above.**
- iii. Type of incident and if the data was in a secure location (locked room, cabinet, etc.).



DoD Breach Reporting

8. Description of breach (*cont'd*)

- v. Were any documents were posted to DoD's Internet or Intranet? **Yes or no.**
- vi. Were any documents faxed inside or outside of DoD? **Yes or no.**
- vii. Was the breach investigated? **Yes or no. *When would this ever be no?***
- viii. Who conducted the investigation (*identify by titles*)? **By title only, identify who conducted the investigation.**



DoD Breach Reporting

8. Description of breach (*cont'd*)

- viii. Preliminary investigation results: **Provide the results of your investigation. No names; don't identify any friction among components of the PLFA; simple explain what happened.**
- ix. Is the breach an isolated or a systematic problem: **Most will be isolated; however, when incidents keep recurring you can not keep claiming isolated. DPCLO keeps track of these reports as does DGA.**
- x. Will impacted individuals be notified, and if so, how? (*keep in mind that DLA has 10 work days to notify the individual, or if necessary, initiate action to notify the Deputy Secretary of the inability to meet this notification requirement*): **If affected individuals will be provided written or verbal notification/courtesy notification, state so. Whether written or verbal will depend on the impact level of the incident.**
- xi. Please provide any other information deemed relevant and pertinent.



DoD Breach Reporting

9. **Describe actions taken in response to the breach** (*150 words or less, for example, actions taken to mitigate any harm that could result from the loss; remedial actions that have been, or will be taken to prevent similar incidents in the future, if the data was recovered, additional training conducted, policy or guidance issued.*) **Provide what your component did in response to the incident/breach.**



DoD Breach Reporting

10. Potential impact of the breach (*High, Medium, or Low*):

Impact Definition

High -- Exercise of the breach/vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly harm or impede an organization's mission; (3) may significantly harm or violate an organization's or individual's reputation or interest; or (4) may result in human death or serious injury.



DoD Breach Reporting

10. Potential impact of the breach *(cont'd) (High, Medium, or Low):*

Impact Definition

Medium -- Exercise of the breach/vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may harm or impede an organization's mission; (3) may harm or violate an organization's or individual's reputation or interest; or (4) may result in human injury.



DoD Breach Reporting

10. Potential impact of the breach (*cont'd*) (*High, Medium, or Low*):

Impact Definition

Low -- Exercise of the breach/vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission; (3) may noticeably affect an organization's or individual's reputation or interest.

11 and 12 currently not used.

Reference: DLA Policies and Procedures when Personal Information is Lost, Stolen, or Compromised

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

DLA FOIA/Privacy Training Workshop

Day 1

WELCOME

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

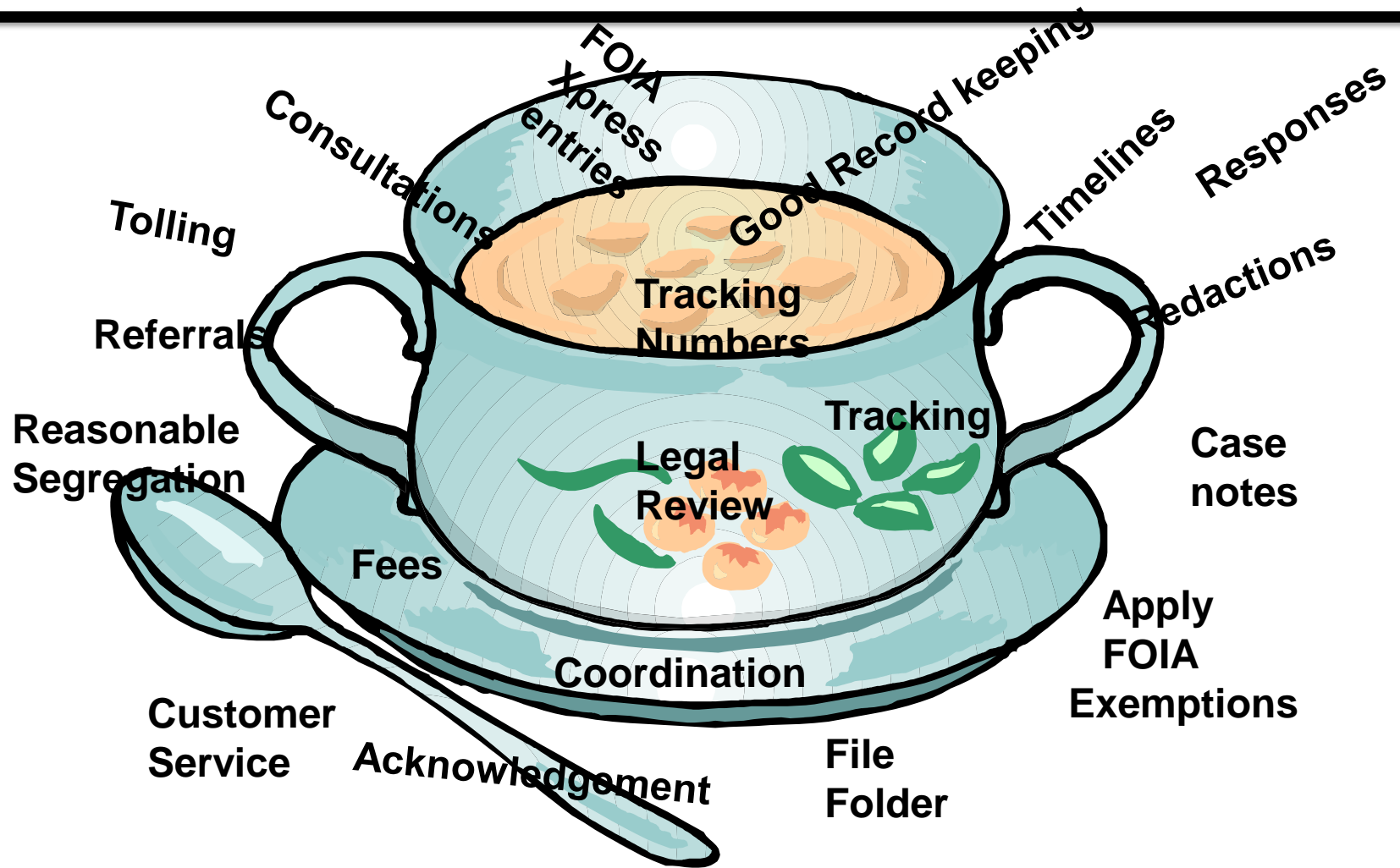
The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched atop a shield with vertical red and white stripes. Above the eagle is a yellow banner with the word "LOGISTICS" in blue. The shield is set against a blue globe with white stars. The words "DEFENSE" and "AGENCY" are written vertically on banners on either side of the shield.

FOIA Administrative Guidance How we do it!

October 26, 2010

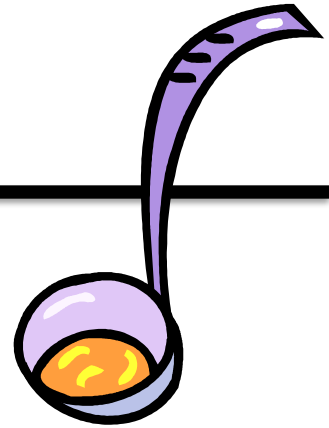


DLA FOIA Process Ingredients





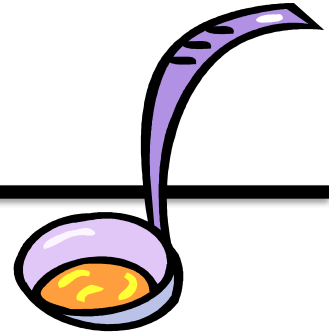
Receipt of a FOIA Request



- **Determine the Proper FOIA Office**
 - 10 days to route
- **Create a Tracking Number (FOIA Xpress)**
- **Create a File Folder**



Perfecting the Request



- **Scope of the request**
 - Reasonable
 - Overly Broad
 - Fee Declaration
 - Postal Mailing Information
- **Privacy Act Request**
 - Declaration



Privacy Act Request



- Identity Declaration Statement

"I declare under penalty of perjury that I am, in fact, [insert name and SSN] and that I currently reside at [insert complete mailing address] and that the documents requested in my FOIA/Privacy Act request of [insert date] filed with the Defense Logistics Agency pertain to me. Executed on [date] [signature]."



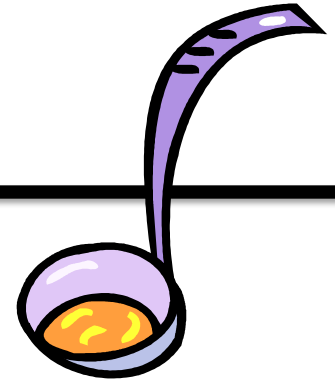
Multi-track Processing



- **Simple**
 - 20 days or less
- **Complex**
 - 20 days + 10 additional days
 - Unusual Circumstances
- **Expedited**
 - Compelling Need



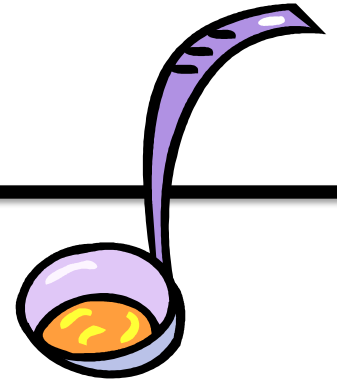
Acknowledgement



- **Acknowledgement Letter**
 - Perfected
 - Clarification Needed



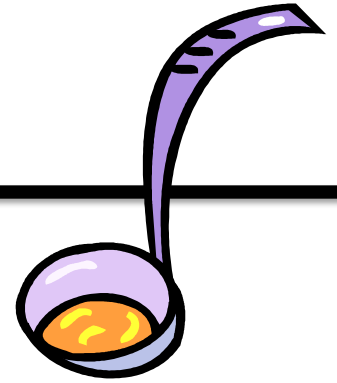
Request for Documents



- **Task the Action Office**
 - DLA Form 1471
 - DD 2086 (Fees)
 - Document Search



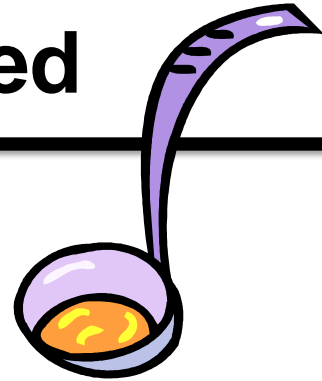
Detachments



- Records at Detachments
 - Processed by the responsible DLA PLFA
 - General Order determines record ownership cut-off
- Task the Detachment



Request for Documents Completed

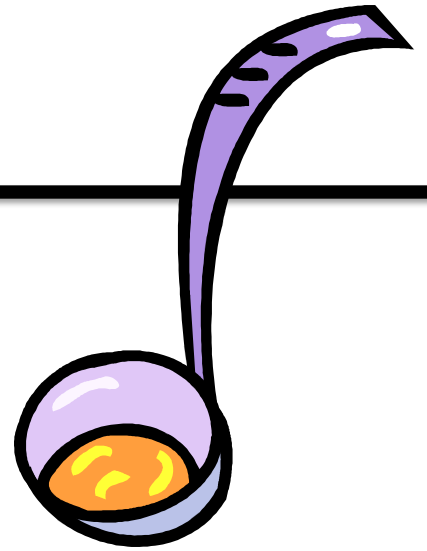


- **Records found**
 - All aspects of request covered.
- **No Records found**
 - Justification for no records.
- **Upload documents into FOIA Xpress**
- **Review**
 - Apply Exemptions
 - Consider reasonable segregation
 - Clearly display exemption codes for redacted documents.



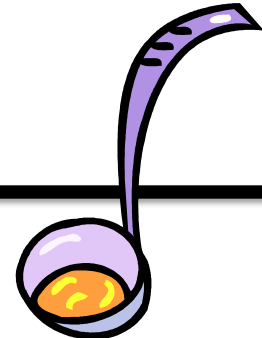
Final Response

- **Preparing the Final Response**
 - Components of the letter
 - Introduction
 - Records





Final Response

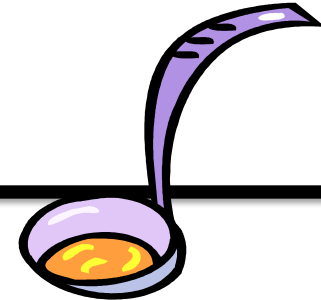


- **Preparing the Final Response Cont.**
 - **Determination/Exemptions claimed**

“The enclosed records are being released to you in part as portions were found to be exempt from disclosure pursuant to 5 U.S.C. § 552 (b)(6), personal privacy. Exemption 6 protects information about individuals when disclosure of such information would constitute a clearly unwarranted invasion of personal privacy. We have withheld personal identifying information of the selectee. Also, due to the increase in security awareness DoD provides greater protection of information identifying DoD personnel to the general public; therefore, we have withheld supervisor names and phone numbers.”



Final Response

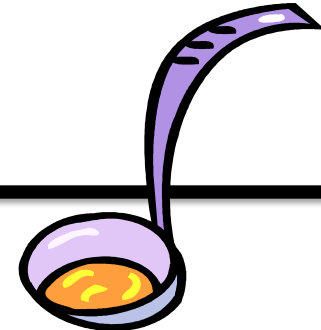


- **Preparing the Final Response Cont.**
 - **Appeal information**

“You have the right to appeal this (full/partial denial or no records response). An appeal must be made in writing to the General Counsel and reach the General Counsel’s office within 60 calendar days from the date of this letter. The appeal should include your reasons for reconsideration and enclose a copy of this letter. An appeal may be mailed, emailed to hq-foia@dla.mil, or faxed to 703-767-6091. Appeals are addressed to the General Counsel, Defense Logistics Agency, ATTN: DGA, Suite 1644, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6221. “



Final Response

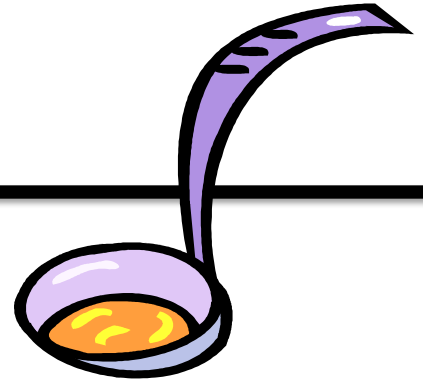


- **Preparing the Final Response Cont.**
 - **Fees assessed**
 - **Contact information**

“As a commercial requester, you may be charged search, review, and duplication fees. The total fees for processing your request are \$110 which includes one half hour of search at \$22.00 per hour, and two hours of review at \$44.00 per hour. Please send your check or money order payable to the Department of Treasury to the above letterhead address, ATTN: DGA (FOIA), Room 1644. Include our case number, DLA-10-HFOI-00133, on the face of the check and attach a copy of this letter.”



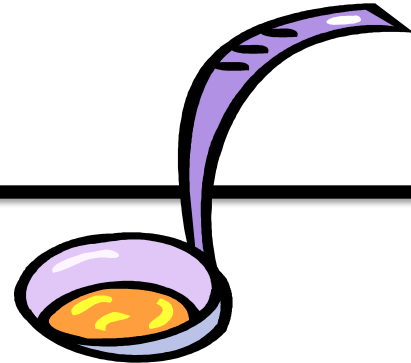
Coordination



- Who should review the initial determination?
 - FOIA Office
 - Subject Matter Expert/Action Office
 - General Counsel
 - Initial Denial Authority
 - Any others?



Closing the Request



- Acceptable Reasons for Closing
 - Granted in Full
 - Granted/Denied in Part
 - Denied in Full
 - Other
 - Other Other
- FOIAXpress



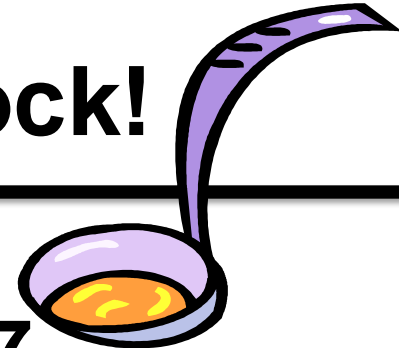
Tolling- Stopping the Clock!



- **The Open Government Act 2007**
 - Tolling Time Limits.
 - When/How often can you toll.
 - When does the toll period end.
 - Can't meet 20 day time limit.



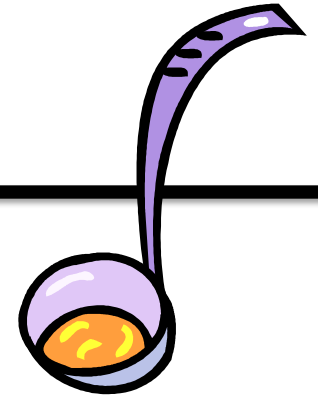
Tolling- Stopping the Clock!



- **The Open Government Act 2007**
 - The purpose of the Act is intended to ease the burden of the FOIA process by establishing:
 - Tracking numbering system
 - Methods to obtain status of request
 - Create a FOIA Liaison
 - Define agency records
 - **Establish time lines**
 - Routing misdirected requests
 - Assessment of fees



Tolling- Stopping the Clock!



- **Tolling Time Limits**

- Tolling is a legal principle which allows for the pausing or delaying of the period of time set by a statute of limitations
- Timelines begin on the date of receipt of a “proper” request; but not later than 10 days after it is received within a component of an agency
- The 10 days time limit applies to agency routing only



Tolling- Stopping the Clock!

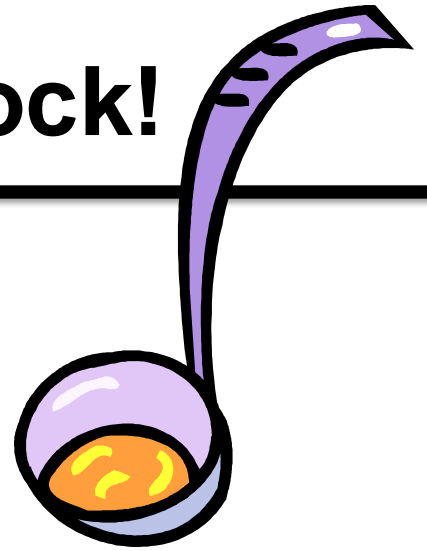


- When/How often can you toll?
 - There are only two circumstances for which you can toll:
 - To obtain information from the requester
 - Only once
 - To clarify fee related issues
 - No limit



Tolling- Stopping the Clock!

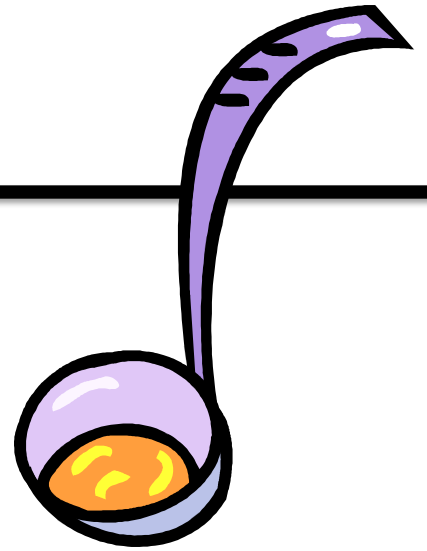
- When does the toll period end?
 - Answer received
 - Clock restarts
 - Perfect in FOIAXpress





The Case File

- What is the Case File?
- Organization of the Case File
- Retention
 - DLA Records Schedule Series 510.18 to 510.28





The Case File

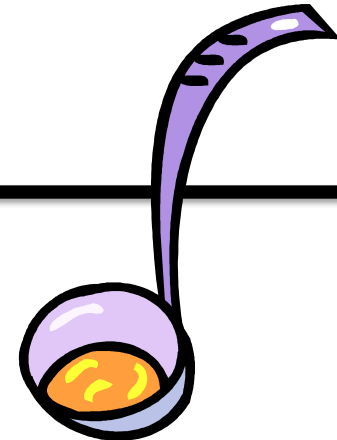
- **What is the Case File?**



The case file is the official file which contains all requests, records, correspondences, notes, etc., pertaining to the request and is maintained in accordance with the DLA Records Schedule.



The Case File



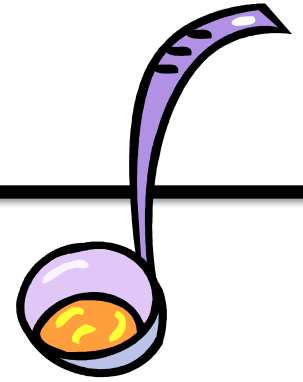
- Organization of the Case File

All case files are organized in accordance with the following format :

- Staff Summary Sheet
- Tab 1- Response Letter w/ attachment(s)
(a copy will be maintained in folder)
- Tab 2- FOIA Request
- Tab 3- Original document(s)
- Tab 4- Supplemental Information
(i.e., case notes, email, etc.)



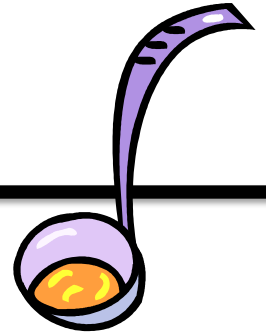
The Case File



- Retention
 - DLA Records Schedule Series 510.18 to 510.28
- **510.18 Freedom of Information Act (FOIA) Request Files-** Destroy 2 years after date of reply
- **510.20 FOIA Request Denial Files-** Destroy after 6 years if not appealed
- **510.22 FOIA Appeal Files-** Destroy 6 years after final denial by agency, or 6 years after the time at which a requester could file suit, or 3 years after adjudication by courts, whichever is later
- **510.24 FOIA Control Files-** Destroy 6 years after date of last entry
- **510.28 FOIA Report Files-** Destroy when 2 years old



Administrative Appeals



- Requester Rights.
- Reasons to Appeal.
- How are Appeals Processed.
- Last of the Administrative Remedies.



FOIA Tools

- Reference materials:
 - DOJ Guide, FOIA Post & Update, Hotline
http://www.justice.gov/oip/04_7.html
202-514-3642
 - DoD Regulation and Hotline
<http://www.dod.mil/pubs/foi/dfoipo/>
703-696-3329
 - DLA Regulation
 - DLA FOIA Staff
 - Other agencies

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



WARFIGHTER SUPPORT ENHANCEMENT

STEWARDSHIP EXCELLENCE

WORKFORCE DEVELOPMENT



Break time!



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

FOIA/Privacy Act Recent Decisions

**Ms. Caroline Smith, Attorney-Advisor
Office of Information Policy, DOJ**

October 26, 2010



Lunch!



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The logo of the Defense Logistics Agency (DLA) is centered in the background. It features a globe with a yellow banner arched over the top that says "LOGISTICS". A bald eagle with spread wings is perched on a shield. The shield has a grey top section and red and white vertical stripes below. Two yellow banners hang on either side of the shield, with "DEFENSE" on the left and "AGENCY" on the right.

DLA FOIA/PRIVACY WORKSHOP

Privacy Act Overview

October 26, 2010



Privacy Act Overview

The Privacy Act of 1974 (5 U.S.C. 552a), Public Law 93-579, was created in response to concerns about how the use of computerized databases / records impact an individuals' privacy rights.



Implementing Documents

- The Privacy Act of 1974 (5 U.S.C. 552a), Public Law 93-579
- OMB Circular A-130, Management of Federal Information Resources; and other OMB Memos
- Department of Defense Privacy Program (DoD Directive 5400.11 & DoD 5400.11-R)
- DLA Privacy Program



Definitions

- **Personal Information.** Information about an individual that identifies, links, relates, or is unique to, or describes him or her. Such information is also known as *personally identifiable information*.
- **Individual.** A *living* person who is a U.S. citizen or an alien lawfully admitted for permanent residence.



Definitions

- **System Manager.** The DLA official responsible for the operation and management of a system of records.
- **Record.** Any item, collection, or grouping of information about an individual maintained by DLA, whatever the storage media (paper, electronic, etc.).



Definitions

- **System of Records.** A group of records under the control of DLA from which personal information about an individual is retrieved by the name of the individual.
- **Routine Use.** The disclosure of a record ***OUTSIDE*** the DoD for a use that is compatible with the purpose for which the information was collected and maintained.



Conditions of Disclosure

No agency shall disclose any record in a system of records except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, . . .



Conditions of Disclosure

. . . unless disclosure of the record would be

- 5 U.S.C. § 552a(b)(1) ("need to know" within agency)
- 5 U.S.C. § 552a(b)(2) (required FOIA disclosure)
- 5 U.S.C. § 552a(b)(3) (routine uses)



Conditions of Disclosure

- 5 U.S.C. § 552a(b)(4) (Bureau of the Census)
- 5 U.S.C. § 552a(b)(5) (statistical research)
- 5 U.S.C. § 552a(b)(6) (N A R A)



Conditions of Disclosure

- 5 U.S.C. § 552a(b)(7) (law enforcement request)
- 5 U.S.C. § 552a(b)(8) (health or safety of an individual)
- 5 U.S.C. § 552a(b)(9) (Congress)



Conditions of Disclosure

- 5 U.S.C. § 552a(b)(10) (G A O)
- 5 U.S.C. § 552a(b)(11) (court order)
- 5 U.S.C. § 552a(b)(12) (Debt Collection Act)



Accounting of Disclosures

- An agency must keep accurate accounts of when and to whom it has disclosed personal records, including
 - Name and address of the person or agency to whom the disclosure is made, and
 - Date, nature and purpose of each disclosure.

GSA FORM 3363 (6-76)



Individual's Right of Access

- **DLA must, upon request, unless the record is exempt from disclosure:**
 - Permit an individual to access any record pertaining to him or her which is contained in the system of records (section (d)(1)).
 - Permit the individual to be accompanied by a person of their choosing (section (d)(1)).
 - Permit the individual to obtain a copy of any such record in a comprehensible form at a reasonable cost (section (d)(1)).



Individual's Right of Access

- **DLA must, upon request, unless the record is exempt from disclosure:**
 - Permit the individual to request amendment of a record contained in the system of records (section (d)(2)).
 - Permit the individual to seek review of the denial to amend (section (d)(3)).
 - Permit the individual to file a statement of disagreement in the file regarding the refusal to amend (section (d)(4)).
 - An individual is not permitted access to any information compelled in reasonable anticipation of a civil action or proceeding (section (d)(5)).



Agency Requirements

- Maintain only information about an individual that is relevant and necessary to accomplish a legal purpose of the agency (section (e)(1)).
- Collect information to the greatest extent practicable directly from the subject individual if that information may have an adverse effect upon that individual (section (e)(2)).



Agency Requirements

- Privacy Act Statements; required when collecting information from the individual to be maintained in a “system of records.” (section (e)(3)).
 - Authority
 - Principal purpose(s)
 - Routine uses *(to include DoD Blanket Routine Uses)*
 - Disclosure (voluntary or mandatory); and the effects on the individual of not providing the information.
 - *DLA identifies the applicable SORN.*
- Publish the existence and character of the system of records (section (e)(4)) .



Agency Requirements

- Maintain all records about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual when making any determination (section (e)(5)).
- Except for FOIA releases, make reasonable efforts to assure that records are accurate, complete, timely, and relevant for agency purposes prior to disseminating any record OUTSIDE of DoD (section (e)(6)).



Agency Requirements

- Maintain no record describing how any individual exercises rights guaranteed by the First Amendment (section (e)(7)).
- Make reasonable efforts to serve notice on an individual when any record is made available to any person under court order when such process becomes a matter of public record (section (e)(8)).



Agency Requirements

- Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records (section (e)(9)).



Agency Requirements

- **DoD Rules of Conduct for DoD Personnel Shall:**
 - Take such actions, as considered appropriate, to ensure that any personal information contained in a system of records, of which they have access to and are using to conduct official business, shall be protected so that the security and confidentiality of the information shall be preserved.
 - Not disclose any personal information contained in any system of records, except as authorized. *Personnel willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.*
 - Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized to the applicable Privacy POC for his or her DoD Component.



Agency Requirements

- **DoD Rules of Conduct for Privacy System Managers:**
 - Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities and are properly trained to safeguard personal information being collected and maintained.
 - Prepare any required new, amended, or altered system notices for and submit them to DGA for publication in the Federal Register.
 - Not maintain any official files on individuals, which are retrieved by name or other personal identifier, without first ensuring that a SORN has been published in the Federal Register. *Any official who willfully maintains a system of records without meeting the publication requirements is subject to possible criminal penalties and/or administrative sanctions.*



Agency Requirements

- Establish appropriate ***administrative, technical,*** and ***physical*** safeguards to insure the security, confidentiality, and integrity of the records (section (e)(10)).
- Publish any new routine uses and/or new uses of the data in a SORN in the Federal Register for public comment (section (e)(11)).
- Same as above except for Computer Matching Agreements (section (e)(12)).



Agency Rules

- Agency must promulgate rules to carry out the requirements of the Privacy Act (section (f)).
 - Rules must describe how an agency is complying with the Act; and how an individual can exercise their rights under the Act.



Penalties for Non-compliance

- **Civil Remedies** (section (g))
 - The cost of actual damages suffered (\$1000 minimum)
 - Costs and reasonable attorney's fees



Penalties for Non-compliance

- **Criminal Penalties** (section (i))
 - Charge of a misdemeanor
 - Maximum fine of \$5,000



Privacy Act Exemptions

- Agency head may exempt a system of records from specific requirements of the Act.
- Two “self executing”; while the General and Specific exemptions must be published in the Federal Register.
 - (c)(3); self executing
 - (d)(5); self executing
 - General Exemptions: (j)(1) and (j)(2)
 - Specific Exemptions: (k)(1) through (k)(7)



Privacy Act Exemptions

- **(j)(1) Exemption:** Records maintained by the C I A.
- **(j)(2) Exemption:** Records maintained by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws.
 - OSI, Air Force
 - CID, Army
 - NCIS, Navy
 - DoD Inspector General



Privacy Act Exemptions

- **(k)(1) Exemption:** Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1-R.
- **(k)(2) Exemption:** Investigatory material compiled for law enforcement purposes, other than material within the scope of (j)(2).
- **(k)(3) Exemption:** Pertain to the protective services to the President or other individuals pursuant to section 3056 of Title 18.



Privacy Act Exemptions

- **(k)(4) Exemption:** Required by statute to be maintained and used solely as statistical records.
- **(k)(5) Exemption:** Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information.



Privacy Act Exemptions

- **(k)(6) Exemption:** Testing and examination material.
- **(k)(7) Exemption:** Evaluation material used to determine potential for promotion in the Armed Services.



Government Contractors

- When a DLA contract requires the operation or maintenance of a system of records or requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records, the record system or the portion of the record system affected are considered to be maintained by DLA and are subject to the DoD Privacy Program (section (m)).



Government Contractors

- DLA applies the requirements of the Privacy Act to the contractor by placing the Federal Acquisition Regulation (FAR) clauses (Part 24, Protection of Privacy and Freedom of Information) in the contract.
- The contractor and its employees are to be considered employees of DLA for purposes of the criminal provisions during the performance of the contract.



Disclosure of the SSN

Section 7 (not codified as part of the Act)

- It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN.
- Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.



Other DoD Requirements

- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information; Reduce the Use of Social Security Numbers.
 - Eliminate Unnecessary Use.
 - Explore Alternatives.
- OUSD(P&R) Directive-Type Memorandum 07-015-USD(P&R) – “DoD Social Security Number (SSN) Reduction Plan” dated March 28, 2008



Other DoD Requirements

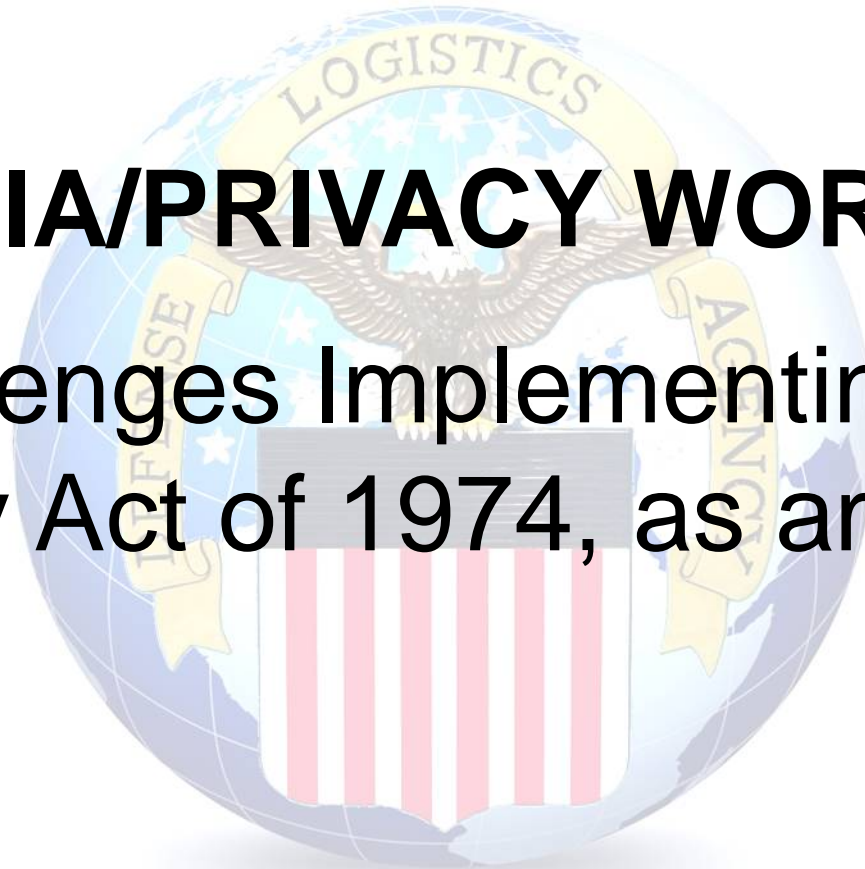
- OSD(DA&M) memo “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” dated June 5, 2009.
 - Privacy training is a prerequisite before an employee or contractor is permitted access to DoD information / systems.
 - Privacy training required annually.
 - Employees / contractors annually sign a document describing their responsibilities acknowledging their understanding.

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

DLA FOIA/PRIVACY WORKSHOP

**Challenges Implementing the
Privacy Act of 1974, as amended**





Privacy Implementation Challenges

1. Technologies' Rapid Pace of Change
 2. Timeliness of Guidance and Legislation
 3. System Dependence on Unique Identifiers
 4. Increased Demands for Appropriate Sharing of PII
 5. Ensuring Contractor Compliance
-
- I. Background Slides
 - A. ISPAB



Technologies' Rapid Pace of Change

- PII can be found anywhere:
 - Portable mass storage
 - *thumb drives, portable HD's, CDs*
 - Ubiquitous storage in common work appliances
 - copiers, faxes, B-berries
- Internet behavior is easily tracked:
 - Web browser tracking
 - cookies, zero pixel gifs, flash cookies
- Social Media is complex -- Web 2.0
 - Facebook, Twitter, YouTube
- Cloud Computing presents new issues
 - Gov't Cloud vs. Commercial Cloud
 - Geolocation and Jurisdiction



Timeliness of Guidance and Legislation

- Is OMB Guidance too old?
 - Privacy Act – published 1975 (40 FR 28948)
 - Computer Matching Act – published 1989 (54 FR 25818)
- Is Privacy Act still current? (Sep. 29, 1975)
 - Passed in response to:
 - abuse of Executive power, surveillance, wrongful disclosures
 - Amended by Computer Matching Act of 1988
 - Do definitions still have currency?
 - “System of Records”
 - Routine Use



System Dependence on Unique Identifiers

- IT Systems need unique ID's
 - SSN usage in DoD systems governed by SSN Reduction Plan
 - DoD Directive-Type Memorandum, 07-015-USD(P&R) “DoD Social Security Number Reduction Plan”
 - Several requirements for continued collection of SSNs
 - Truncated SSN's included
 - DLA Forms and J-6 Effort
- Biometrics seen as one option
 - ❖ DLA's involvement in Biometrics
 - DLA's Defense Standardization Program Office
 - The DoD Electronic Biometric Transmission Specification – Sept. 2008
 - Privacy Issues with Biometrics Include:
 - Statistical concerns
 - Due process for biometrics



Increased Demand for Sharing of PII

- **“Debt collection” drove demand in 1990’s**
- **“Terrorism Information” drives demand now.**
- **Information Sharing Environment (ISE) –**
 - **“Intelligence Reform and Terrorism Prevention Act of 2004,” Pub.L.108–458, Dec. 17, 2004**
 - **DoD is participant in ISE**
 - **Defense Privacy Office Director is DoD’s Privacy and Civil Liberties Officer (42 USC § 2000ee–1).**
 - **DoD’s ISE Privacy Framework is being developed.**
 - **Privacy Framework sets forth how ISE will function in compliance with Fair Information Practice Principles**



Sharing and the Labeling of PII

- **Labeling of PII when shared with others within the ISE must use new “Controlled Unclassified Information” labeling framework.**
 - **Presidential Memorandum (May 9, 2008)**
 - **DOJ & DHS Co-Chaired Task Force on Controlled Unclassified Information – Report to President (Aug. 25, 2009)**
 - **DoD Implementation:**
 - **DoD 5200. 1-R, “Information Security Program”**
 - **DTM 08-027 – “Security of Unclassified DoD Information on Non-DoD Information Systems,” September 16, 2010**



Contractor Compliance

- **For contracts involving operation of a “system of records,”**
 - **Contractors “shall be considered to be an employee of an agency.” -- 5 U.S.C. § 552a(m)(1)**
- **The FAR and DFARS refer to parts & clauses implementing requirement:**
 - FAR Part 24.1
 - Clauses 52.224-1, 52.224-2
 - FAR Part 39.1
 - Especially Part 39.105, “Privacy.”
 - DFARS Subparts 224.1 and 239.71



BACKGROUND



Information Security & Privacy Advisory Board

- **ISPAB reviewed Privacy Act and associated Gov't Privacy Policies/Practices – believes improvements need to be made. Recommends:**
 - Amendments to the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002.
 - Improvements to Government leadership on privacy.
 - Other necessary changes to privacy policy.

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY





Break time!



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched on a shield with vertical red and white stripes. Above the eagle is a banner with the word "LOGISTICS". The entire seal is set against a blue globe with white grid lines.

Freedom of Information Act Exemption 4

Debbie Teer
October 26, 2010



Exemption 4

- Protects Release of:
 - Trade secrets
 - Commercial or Financial Information
 - Obtained from a person.
 - Privileged or confidential.



Voluntary or Required

- Critical Mass

(Critical Mass Energy Project v. NRC, 975 F.2d 871
(D.C. Cir. 1992))

- Voluntarily submitted

- Did agency exercise authority

- National Parks

(Nat'l Parks & Conservation Ass'n v. Morton, 498 F.2d 765
(D.C. Cir. 1974))

- Required

- Impairment prong
- Competitive harm prong
 - EO 12600



EO 12600

- Requires federal agencies to establish certain predisclosure notification procedures which will assist agencies in developing adequate administrative records.
 - Submitters of confidential commercial information.
 - Notify requester



Submitter Notice

- Letter includes:
 - Identifies requester and records requested
 - Factors to consider
 - National Parks
 - Reasonable period of time to respond
 - Contact information
 - FOIA case number
 - Copy of records
 - Submitter Notice Instructions



Submitter Notice

- Review the response
 - Has the submitter objected to release
 - Objection adequately supported
 - No response received
- Document your review and determination
 - Competitive harm analysis
 - Case-by-case
 - Reasonable segregation
 - Cannot withhold information created by the Federal Government



Intent to Release

- Submitter objections not sustained
 - Notify requester of intent to release
 - Provide reason for release
 - Use case law
 - Close letter with rights
 - Reverse FOIA



Unit Prices

- Definition:
Specified amounts to be paid by the government per item for goods or services
- Burden of Proof
 - Submitter
- Release of Unit Price



Unit Prices

- Federal Acquisition Regulation (FAR)
 - 15.506 Postaward debriefing of offerors.
 - Subpart 24.2—Freedom of Information Act



Unit Prices

– Reverse FOIAs

- Withheld

- McDonnell Douglas Corp. v. NASA , 180 F.3d 303 (D.C.C. 1999)
- McDonnell Douglas Corp v. USAF, 375 F.3d 1182 (D.C.C. 2004)

- Released

- Boeing Co. v. U.S. Department of the Air Force, 616 F Supp 2d 40, 2009 U.S. Dist.
- Pacific Architects and Engineers Inc., v. US Dept of State, 906 F.2d 1345 (1990)
- Martin Marietta Corp. v. John H. Dalton, 974 F. Supp. at 37 (1997)

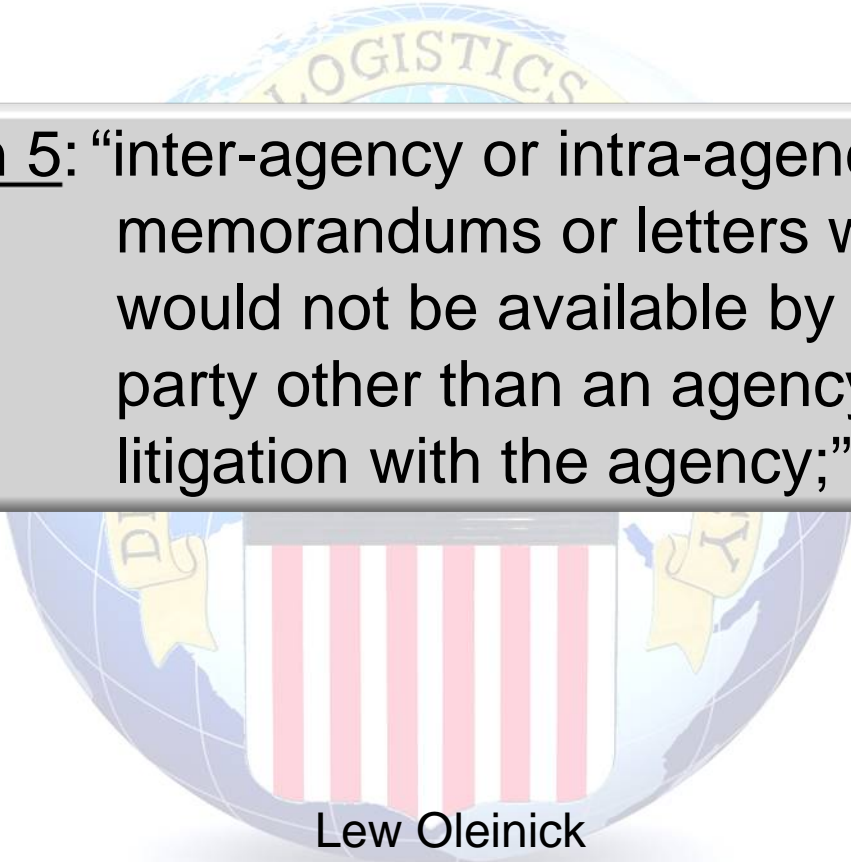
DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



Exemption 5: “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;”

Lew Oleinick

October 26, 2010



Outline

- What types of records are covered?
- What is Exemption 5 intended to protect?
- Purpose of Exemption 5
- Recognized privileges for Exemption 5
- Implications of President Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines and Proactive Disclosure



Exemption 5 Coverage

- Inter or intra agency records
- Records “normally privileged in the context of civil discovery”
- “To qualify, a document must thus satisfy two conditions:
 - its source must be a Government agency, and
 - it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it.¹”

1. DOI v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 8-9 (U.S. 2001)
– Consultant Test



Purpose of Exemption 5

- to encourage open, frank discussions on matters of policy between subordinates and superiors;
- to protect against premature disclosure of proposed policies before they are finally adopted;
- protect against public confusion that might result from disclosure of reasons and rationales that were not in fact ultimately the grounds for an agency action.



Common privileges for Exemption 5

- Deliberative process
- Attorney work product
- Attorney-client



Deliberative Process

- Question to ask: What is the status of the record?
 - Two-part test: pre-decisional? deliberative?
 - Burden is upon agency to show record satisfies both parts of test.
- Deliberative portions protected:
 - analysis, evaluations, recommendations, advice
 - but see Tax Analysts v. IRS, 117 F. 3d 607, 617 (D.C. Cir. 1997).
- Factual portions generally not protected



Attorney Work-Product

- “reasonable anticipation of litigation”
 - although specific claim need not be identified
- Covers: civil, administrative, and criminal proceedings.
 - Caveats
 - Documents not originally prepared in anticipation of litigation can’t assume work-product privilege
 - Documents prepared in “normal course of business” – not related to litigation – may not be protected.
- Prepared by: (1) attorney or (2) non-attorney supervised by attorney.



Attorney Client

- What is covered?
 - "confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice."
 - applies to facts divulged by a client to his attorney
 - any opinions given by an attorney to his client based upon, and thus reflecting, those facts
 - Not limited to litigation context
- Does the "client" have to be specified?
 - Maybe: see Elec. Privacy Info. Ctr. v. DOJ, 584 F. Supp. 2d 65, 80 (D.D.C. 2008)



Presidential and AG FOIA Policy

- President's January 21, 2009 and Attorney General's March 19, 2009 memoranda apply to Exemption 5.
 - President's on "presumption of openness"
 - "In face of doubt, openness prevails."
 - Do not withhold because of "speculative or abstract fears."
 - AG's Policy
 - Agency should not withhold information simply because it may do so legally.
 - If full release is not possible, agency "must consider whether it can make partial disclosure."
 - Recognizes FOIA disclosure requirement is not



Foreseeable Harm Analysis

- Primary Factors to Guide Analysis
 - The nature of the decision
 - The nature of the decision-making
 - The status of the decision
 - The status of the personnel involved
 - The potential for process impairment
 - The significance of any process impairment
 - The age of the information
 - The sensitivity of individual record portions



Impact of FOIA Release on Privilege

- Discretionary disclosure under the FOIA does not waive privilege on similar records.
 - See
 - Nat'l Inst. of Military Justice v. United States DOD, 404 F. Supp. 2d 325, 2005 U.S. Dist. LEXIS 33154 (D.D.C. 2005)
 - Students Against Genocide v. Dep't of State, 257 F. 3d 828, 835-36 (D.C. Cir. 2001)
 - Salisbury v. United States, 690 F.2d 966, 971 (D.C. Cir. 1982)

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched on a shield with vertical red and white stripes. Above the eagle is a banner with the word "LOGISTICS". The shield is flanked by two banners, one on each side, with the words "DEFENSE" and "AGENCY" respectively. The entire seal is set against a light blue globe with white stars.

Freedom of Information Act Exemptions 6 & 7(C)

Kathy R. Tennessee
October 26, 2010



Exemptions b(6) & 7(C)

The following analysis is used for both exemptions:

1. Is the exemption's threshold met?
2. Is there a privacy interest?
3. Is there a qualifying public interest?
4. Balance Public vs. Privacy Interest.



Exemption b(6)

Exemption b(6) threshold language:

“Personnel and medical files and similar files” when disclosure of such information “would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6).



Exemption b(7)(C)



- Exemption 7(C) threshold language:
 - Protects “records or information compiled for law enforcement purposes,” the disclosure of which “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”



Law Enforcement Records



According to the U.S. Department of Justice, “the mention of an individual's name in a law enforcement file will engender comment and speculation and carries a stigmatizing connotation.”

- Persons who are **NOT** targets of an investigation.

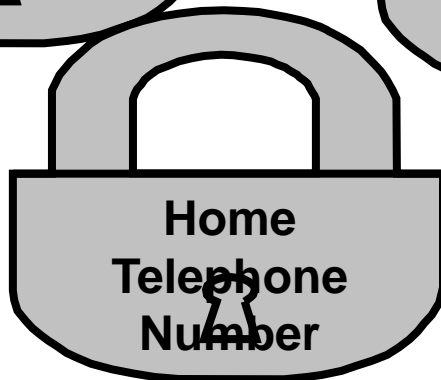
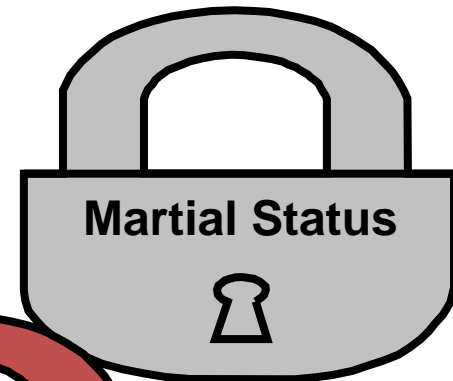
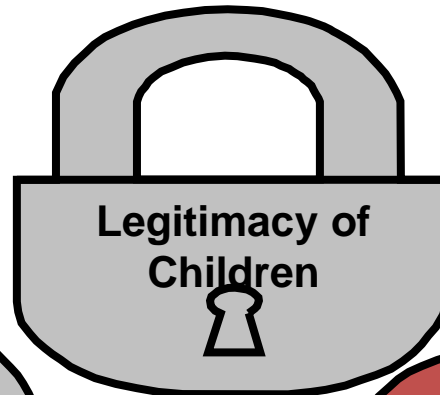
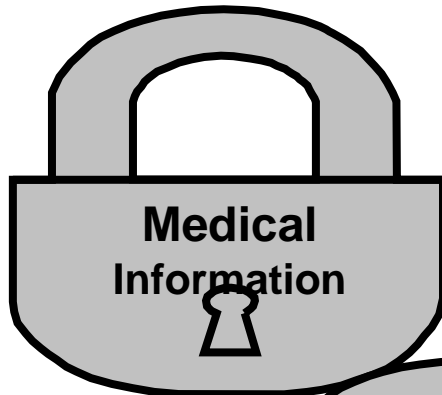
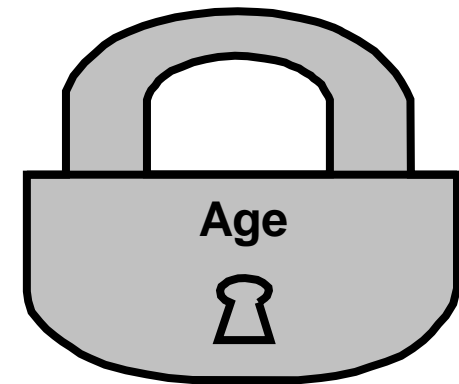
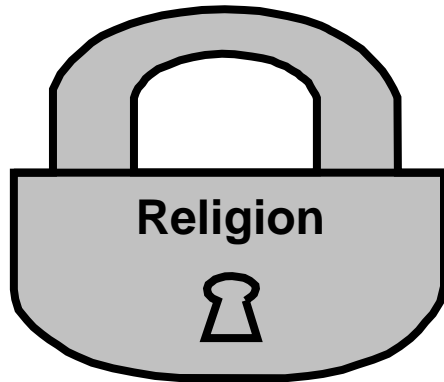


Is There a Privacy Interest?

- Consider the Sensitivity of Information
- Consider Adverse Consequences
- The passage of time does **not** diminish a privacy interest.



Identifying a Privacy Interest





Where There is No Privacy Interest

- **Corporations** – except small companies
- **Deceased Individuals** (except in extreme cases)
- **Public Records** – unless they are practically obscure.
- **Federal Employees** – OPM regulation, 5 C.F.R. 293.311
- **Identities of FOIA Requesters** – except personal information.



Balance the Privacy and the Public Interests

- If there is NO privacy interest, disclose the information.
- If there is a privacy interest, and no qualifying public interest, withhold the information.
- If there is a privacy interest and a public interest, balance them to determine which is greater.





Is There a Qualifying Public Interest?

The Supreme Court ruled in Reporters Committee that the public interest must fall within the FOIA's "core purpose" of shedding light on an agency's performance of its duties.



Is There a Qualifying Public Interest

Is the public interest directly served by the disclosure.





References

- U.S. Department of Justice(2009) *Guide to the Freedom of Information Act.*
- Office of Secretary of Defense Memo (2005) *Withholding of Information that Personally Identifies DoD Personnel.*

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

DLA FOIA and Privacy Training Workshop

October 26 – 28, 2010

WELCOME

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

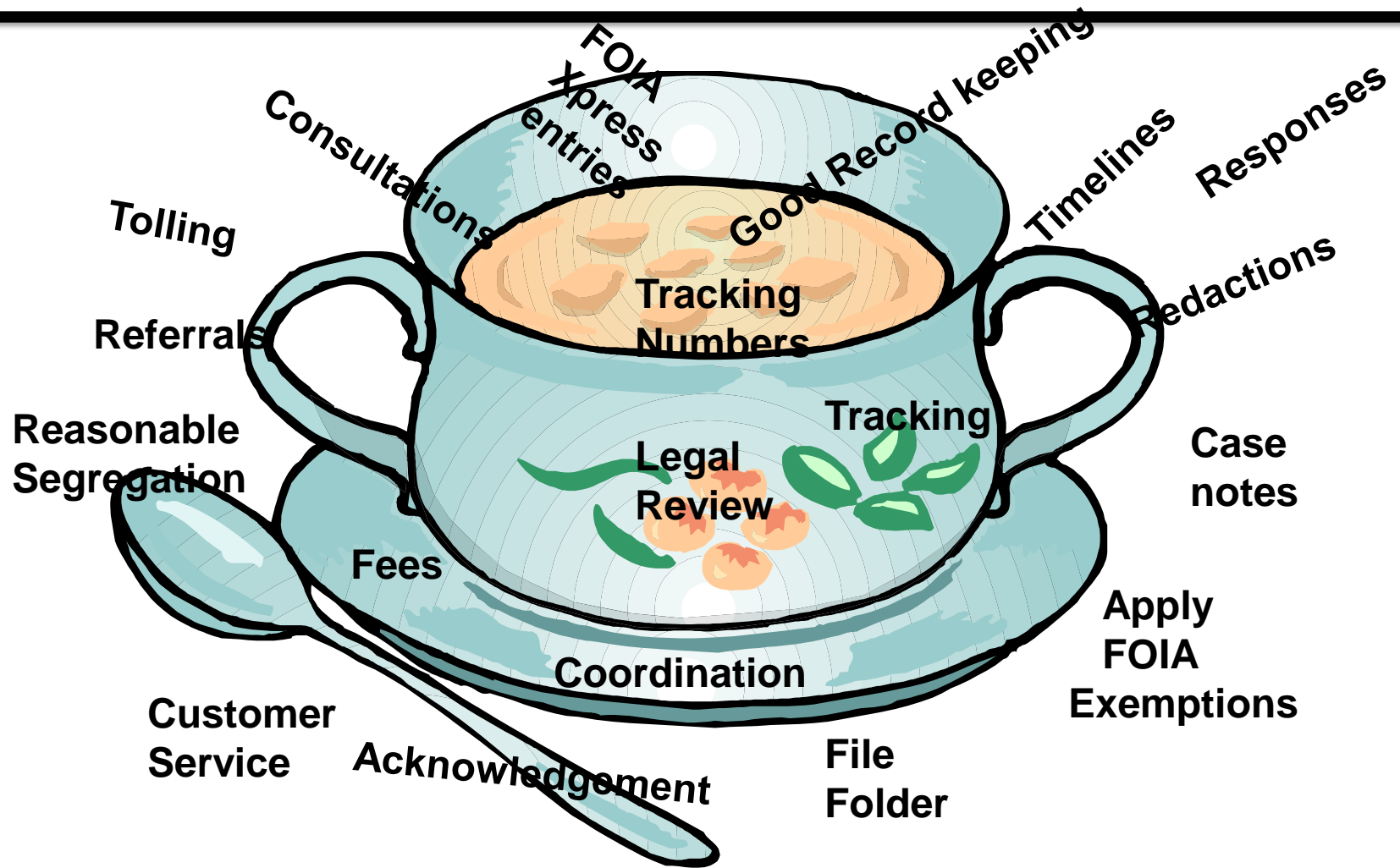
The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched atop a shield with vertical red and white stripes. The shield is set against a blue globe with white stars. A yellow banner arches over the eagle with the word "LOGISTICS" in black. Two vertical yellow banners on either side of the eagle contain the words "DEFENSE" and "AGENCY" respectively.

FOIA Administrative Guidance How we do it!

October 26, 2010

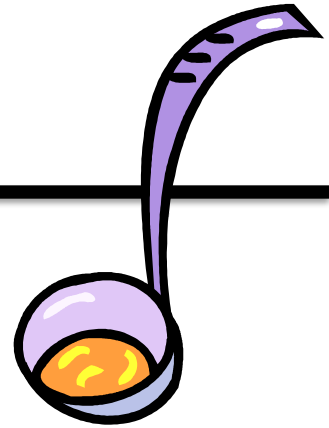


DLA FOIA Process Ingredients





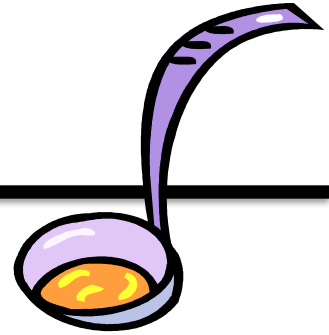
Receipt of a FOIA Request



- **Determine the Proper FOIA Office**
 - 10 days to route
- **Create a Tracking Number (FOIA Xpress)**
- **Create a File Folder**



Perfecting the Request



- **Scope of the request**
 - Reasonable
 - Overly Broad
 - Fee Declaration
 - Postal Mailing Information
- **Privacy Act Request**
 - Declaration



Privacy Act Request



- Identity Declaration Statement

"I declare under penalty of perjury that I am, in fact, [insert name and SSN] and that I currently reside at [insert complete mailing address] and that the documents requested in my FOIA/Privacy Act request of [insert date] filed with the Defense Logistics Agency pertain to me. Executed on [date] [signature]."



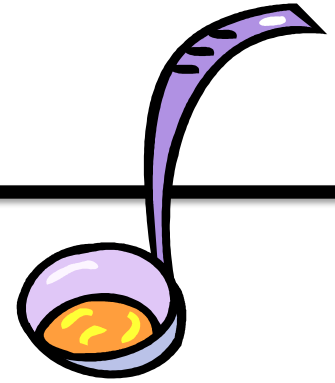
Multi-track Processing



- **Simple**
 - 20 days or less
- **Complex**
 - 20 days + 10 additional days
 - Unusual Circumstances
- **Expedited**
 - Compelling Need



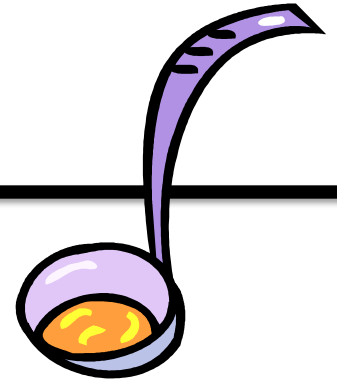
Acknowledgement



- **Acknowledgement Letter**
 - Perfected
 - Clarification Needed



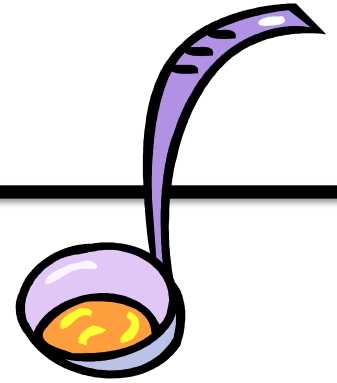
Request for Documents



- **Task the Action Office**
 - DLA Form 1471
 - DD 2086 (Fees)
 - Document Search



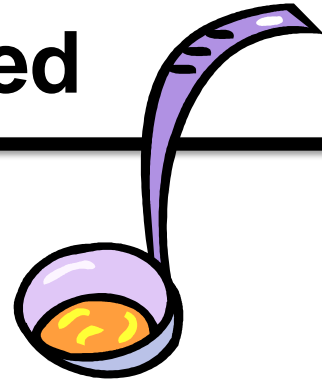
Detachments



- Records at Detachments
 - Processed by the responsible DLA PLFA
 - General Order determines record ownership cut-off
- Task the Detachment



Request for Documents Completed



- **Records found**
 - All aspects of request covered.
- **No Records found**
 - Justification for no records.
- **Upload documents into FOIA Xpress**
- **Review**
 - Apply Exemptions
 - Consider reasonable segregation
 - Clearly display exemption codes for redacted documents.



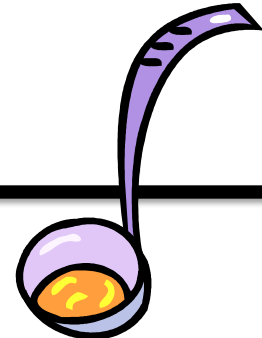
Final Response

- **Preparing the Final Response**
 - Components of the letter
 - Introduction
 - Records





Final Response

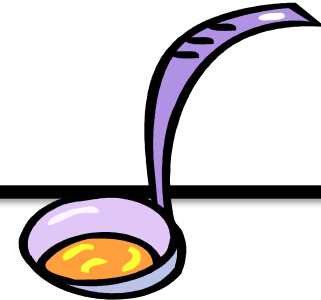


- **Preparing the Final Response Cont.**
 - **Determination/Exemptions claimed**

“The enclosed records are being released to you in part as portions were found to be exempt from disclosure pursuant to 5 U.S.C. § 552 (b)(6), personal privacy. Exemption 6 protects information about individuals when disclosure of such information would constitute a clearly unwarranted invasion of personal privacy. We have withheld personal identifying information of the selectee. Also, due to the increase in security awareness DoD provides greater protection of information identifying DoD personnel to the general public; therefore, we have withheld supervisor names and phone numbers.”



Final Response

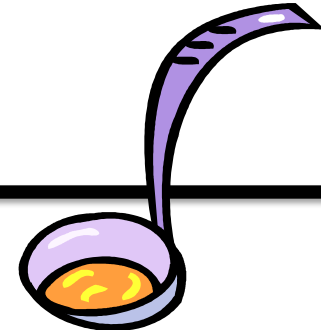


- **Preparing the Final Response Cont.**
 - **Appeal information**

“You have the right to appeal this (full/partial denial or no records response). An appeal must be made in writing to the General Counsel and reach the General Counsel’s office within 60 calendar days from the date of this letter. The appeal should include your reasons for reconsideration and enclose a copy of this letter. An appeal may be mailed, emailed to hq-foia@dla.mil, or faxed to 703-767-6091. Appeals are addressed to the General Counsel, Defense Logistics Agency, ATTN: DGA, Suite 1644, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6221. “



Final Response

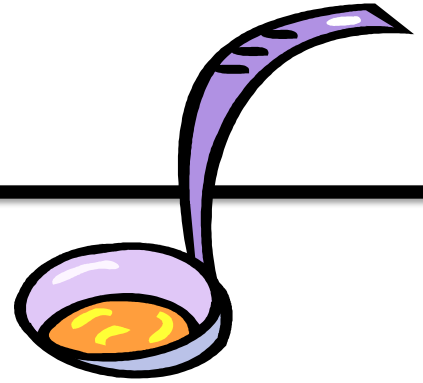


- **Preparing the Final Response Cont.**
 - **Fees assessed**
 - **Contact information**

“As a commercial requester, you may be charged search, review, and duplication fees. The total fees for processing your request are \$110 which includes one half hour of search at \$22.00 per hour, and two hours of review at \$44.00 per hour. Please send your check or money order payable to the Department of Treasury to the above letterhead address, ATTN: DGA (FOIA), Room 1644. Include our case number, DLA-10-HFOI-00133, on the face of the check and attach a copy of this letter.”



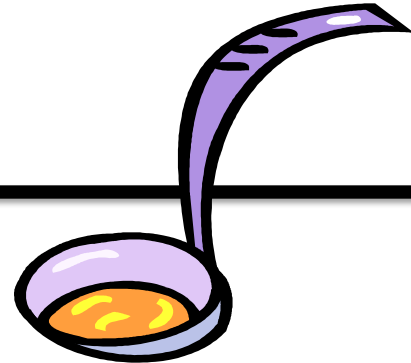
Coordination



- Who should review the initial determination?
 - FOIA Office
 - Subject Matter Expert/Action Office
 - General Counsel
 - Initial Denial Authority
 - Any others?



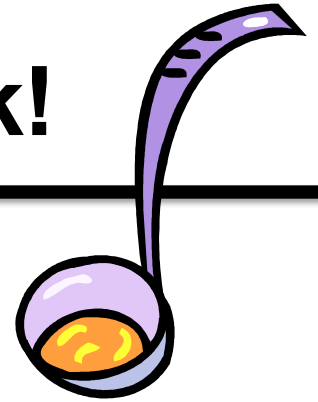
Closing the Request



- Acceptable Reasons for Closing
 - Granted in Full
 - Granted/Denied in Part
 - Denied in Full
 - Other
 - Other Other
- FOIAXpress



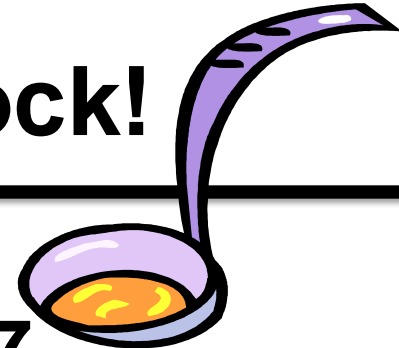
Tolling- Stopping the Clock!



- **The Open Government Act 2007**
 - Tolling Time Limits.
 - When/How often can you toll.
 - When does the toll period end.
 - Can't meet 20 day time limit.



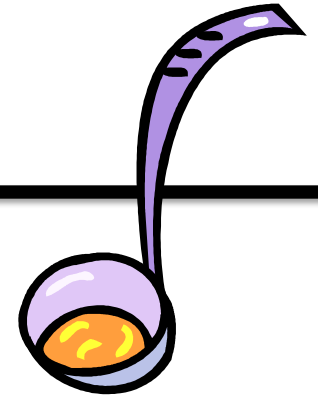
Tolling- Stopping the Clock!



- **The Open Government Act 2007**
 - The purpose of the Act is intended to ease the burden of the FOIA process by establishing:
 - Tracking numbering system
 - Methods to obtain status of request
 - Create a FOIA Liaison
 - Define agency records
 - **Establish time lines**
 - Routing misdirected requests
 - Assessment of fees



Tolling- Stopping the Clock!



- **Tolling Time Limits**

- Tolling is a legal principle which allows for the pausing or delaying of the period of time set by a statute of limitations
- Timelines begin on the date of receipt of a “proper” request; but not later than 10 days after it is received within a component of an agency
- The 10 days time limit applies to agency routing only



Tolling- Stopping the Clock!

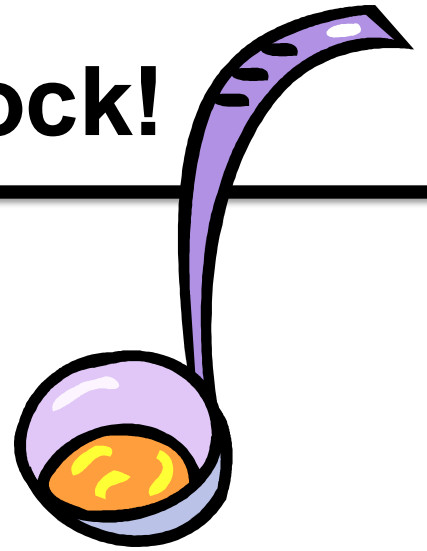


- When/How often can you toll?
 - There are only two circumstances for which you can toll:
 - To obtain information from the requester
 - Only once
 - To clarify fee related issues
 - No limit



Tolling- Stopping the Clock!

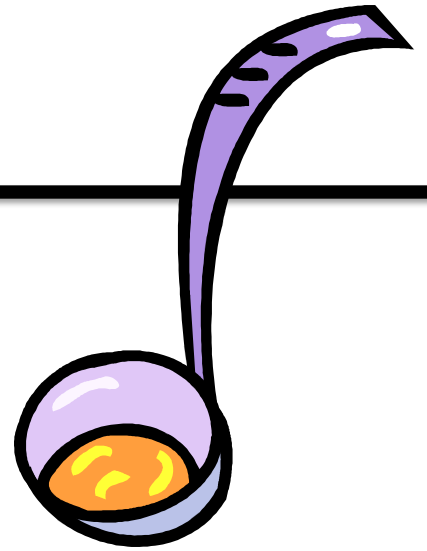
- When does the toll period end?
 - Answer received
 - Clock restarts
 - Perfect in FOIAXpress





The Case File

- What is the Case File?
- Organization of the Case File
- Retention
 - DLA Records Schedule Series 510.18 to 510.28





The Case File

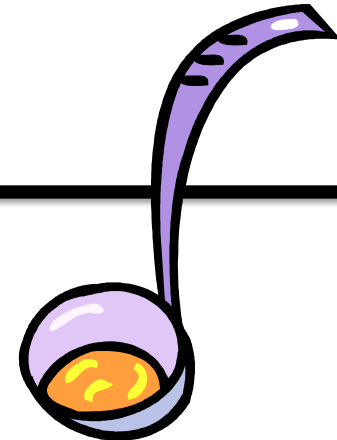
- **What is the Case File?**



The case file is the official file which contains all requests, records, correspondences, notes, etc., pertaining to the request and is maintained in accordance with the DLA Records Schedule.



The Case File



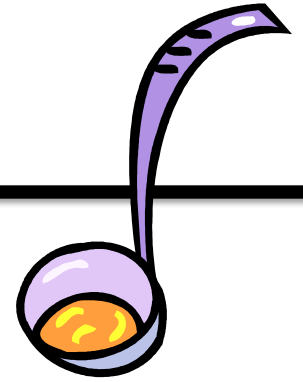
- Organization of the Case File

All case files are organized in accordance with the following format :

- Staff Summary Sheet
- Tab 1- Response Letter w/ attachment(s)
(a copy will be maintained in folder)
- Tab 2- FOIA Request
- Tab 3- Original document(s)
- Tab 4- Supplemental Information
(i.e., case notes, email, etc.)



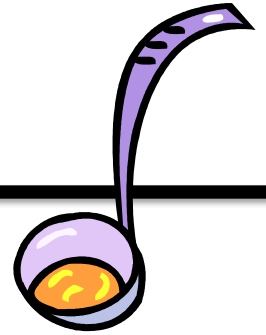
The Case File



- Retention
 - DLA Records Schedule Series 510.18 to 510.28
- **510.18 Freedom of Information Act (FOIA) Request Files-** Destroy 2 years after date of reply
- **510.20 FOIA Request Denial Files-** Destroy after 6 years if not appealed
- **510.22 FOIA Appeal Files-** Destroy 6 years after final denial by agency, or 6 years after the time at which a requester could file suit, or 3 years after adjudication by courts, whichever is later
- **510.24 FOIA Control Files-** Destroy 6 years after date of last entry
- **510.28 FOIA Report Files-** Destroy when 2 years old



Administrative Appeals



- Requester Rights.
- Reasons to Appeal.
- How are Appeals Processed.
- Last of the Administrative Remedies.



FOIA Tools

- Reference materials:
 - DOJ Guide, FOIA Post & Update, Hotline
http://www.justice.gov/oip/04_7.html
202-514-3642
 - DoD Regulation and Hotline
<http://www.dod.mil/pubs/foi/dfoipo/>
703-696-3329
 - DLA Regulation
 - DLA FOIA Staff
 - Other agencies

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



WARFIGHTER SUPPORT ENHANCEMENT

STEWARDSHIP EXCELLENCE

WORKFORCE DEVELOPMENT

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

FOIA/Privacy Act Recent Decisions

**Ms. Caroline Smith, Attorney-Advisor
Office of Information Policy, DOJ**

October 26, 2010

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The logo of the Defense Logistics Agency (DLA) is centered in the background. It features a globe with a yellow banner arched over the top that says "LOGISTICS". A bald eagle with spread wings is perched on a shield. The shield has a grey top section and red and white vertical stripes. Two yellow banners hang vertically on either side of the shield, with "DEFENSE" on the left and "AGENCY" on the right.

DLA FOIA/PRIVACY WORKSHOP

Privacy Act Overview

October 26, 2010



Privacy Act Overview

The Privacy Act of 1974 (5 U.S.C. 552a), Public Law 93-579, was created in response to concerns about how the use of computerized databases / records impact an individuals' privacy rights.



Implementing Documents

- The Privacy Act of 1974 (5 U.S.C. 552a), Public Law 93-579
- OMB Circular A-130, Management of Federal Information Resources; and other OMB Memos
- Department of Defense Privacy Program (DoD Directive 5400.11 & DoD 5400.11-R)
- DLA Privacy Program



Definitions

- **Personal Information.** Information about an individual that identifies, links, relates, or is unique to, or describes him or her. Such information is also known as *personally identifiable information*.
- **Individual.** A *living* person who is a U.S. citizen or an alien lawfully admitted for permanent residence.



Definitions

- **System Manager.** The DLA official responsible for the operation and management of a system of records.
- **Record.** Any item, collection, or grouping of information about an individual maintained by DLA, whatever the storage media (paper, electronic, etc.).



Definitions

- **System of Records.** A group of records under the control of DLA from which personal information about an individual is retrieved by the name of the individual.
- **Routine Use.** The disclosure of a record ***OUTSIDE*** the DoD for a use that is compatible with the purpose for which the information was collected and maintained.



Conditions of Disclosure

No agency shall disclose any record in a system of records except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, . . .



Conditions of Disclosure

- . . . unless disclosure of the record would be**
- 5 U.S.C. § 552a(b)(1) ("need to know" within agency)
- 5 U.S.C. § 552a(b)(2) (required FOIA disclosure)
- 5 U.S.C. § 552a(b)(3) (routine uses)



Conditions of Disclosure

- 5 U.S.C. § 552a(b)(4) (Bureau of the Census)
- 5 U.S.C. § 552a(b)(5) (statistical research)
- 5 U.S.C. § 552a(b)(6) (N A R A)



Conditions of Disclosure

- 5 U.S.C. § 552a(b)(7) (law enforcement request)
- 5 U.S.C. § 552a(b)(8) (health or safety of an individual)
- 5 U.S.C. § 552a(b)(9) (Congress)



Conditions of Disclosure

- 5 U.S.C. § 552a(b)(10) (G A O)
- 5 U.S.C. § 552a(b)(11) (court order)
- 5 U.S.C. § 552a(b)(12) (Debt Collection Act)



Accounting of Disclosures

- An agency must keep accurate accounts of when and to whom it has disclosed personal records, including
 - Name and address of the person or agency to whom the disclosure is made, and
 - Date, nature and purpose of each disclosure.

GSA FORM 3363 (6-76)



Individual's Right of Access

- **DLA must, upon request, unless the record is exempt from disclosure:**
 - Permit an individual to access any record pertaining to him or her which is contained in the system of records (section (d)(1)).
 - Permit the individual to be accompanied by a person of their choosing (section (d)(1)).
 - Permit the individual to obtain a copy of any such record in a comprehensible form at a reasonable cost (section (d)(1)).



Individual's Right of Access

- **DLA must, upon request, unless the record is exempt from disclosure:**
 - Permit the individual to request amendment of a record contained in the system of records (section (d)(2)).
 - Permit the individual to seek review of the denial to amend (section (d)(3)).
 - Permit the individual to file a statement of disagreement in the file regarding the refusal to amend (section (d)(4)).
 - An individual is not permitted access to any information compelled in reasonable anticipation of a civil action or proceeding (section (d)(5)).



Agency Requirements

- Maintain only information about an individual that is relevant and necessary to accomplish a legal purpose of the agency (section (e)(1)).
- Collect information to the greatest extent practicable directly from the subject individual if that information may have an adverse effect upon that individual (section (e)(2)).



Agency Requirements

- Privacy Act Statements; required when collecting information from the individual to be maintained in a “system of records.” (section (e)(3)).
 - Authority
 - Principal purpose(s)
 - Routine uses *(to include DoD Blanket Routine Uses)*
 - Disclosure (voluntary or mandatory); and the effects on the individual of not providing the information.
 - *DLA identifies the applicable SORN.*
- Publish the existence and character of the system of records (section (e)(4)) .



Agency Requirements

- Maintain all records about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual when making any determination (section (e)(5)).
- Except for FOIA releases, make reasonable efforts to assure that records are accurate, complete, timely, and relevant for agency purposes prior to disseminating any record OUTSIDE of DoD (section (e)(6)).



Agency Requirements

- Maintain no record describing how any individual exercises rights guaranteed by the First Amendment (section (e)(7)).
- Make reasonable efforts to serve notice on an individual when any record is made available to any person under court order when such process becomes a matter of public record (section (e)(8)).



Agency Requirements

- Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records (section (e)(9)).



Agency Requirements

- **DoD Rules of Conduct for DoD Personnel Shall:**
 - Take such actions, as considered appropriate, to ensure that any personal information contained in a system of records, of which they have access to and are using to conduct official business, shall be protected so that the security and confidentiality of the information shall be preserved.
 - Not disclose any personal information contained in any system of records, except as authorized. *Personnel willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.*
 - Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized to the applicable Privacy POC for his or her DoD Component.



Agency Requirements

- **DoD Rules of Conduct for Privacy System Managers:**
 - Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities and are properly trained to safeguard personal information being collected and maintained.
 - Prepare any required new, amended, or altered system notices for and submit them to DGA for publication in the Federal Register.
 - Not maintain any official files on individuals, which are retrieved by name or other personal identifier, without first ensuring that a SORN has been published in the Federal Register. *Any official who willfully maintains a system of records without meeting the publication requirements is subject to possible criminal penalties and/or administrative sanctions.*



Agency Requirements

- Establish appropriate ***administrative, technical,*** and ***physical*** safeguards to insure the security, confidentiality, and integrity of the records (section (e)(10)).
- Publish any new routine uses and/or new uses of the data in a SORN in the Federal Register for public comment (section (e)(11)).
- Same as above except for Computer Matching Agreements (section (e)(12)).



Agency Rules

- Agency must promulgate rules to carry out the requirements of the Privacy Act (section (f)).
 - Rules must describe how an agency is complying with the Act; and how an individual can exercise their rights under the Act.



Penalties for Non-compliance

- **Civil Remedies** (section (g))
 - The cost of actual damages suffered (\$1000 minimum)
 - Costs and reasonable attorney's fees



Penalties for Non-compliance

- **Criminal Penalties** (section (i))
 - Charge of a misdemeanor
 - Maximum fine of \$5,000



Privacy Act Exemptions

- Agency head may exempt a system of records from specific requirements of the Act.
- Two “self executing”; while the General and Specific exemptions must be published in the Federal Register.
 - (c)(3); self executing
 - (d)(5); self executing
 - General Exemptions: (j)(1) and (j)(2)
 - Specific Exemptions: (k)(1) through (k)(7)



Privacy Act Exemptions

- **(j)(1) Exemption:** Records maintained by the C I A.
- **(j)(2) Exemption:** Records maintained by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws.
 - OSI, Air Force
 - CID, Army
 - NCIS, Navy
 - DoD Inspector General



Privacy Act Exemptions

- **(k)(1) Exemption:** Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1-R.
- **(k)(2) Exemption:** Investigatory material compiled for law enforcement purposes, other than material within the scope of (j)(2).
- **(k)(3) Exemption:** Pertain to the protective services to the President or other individuals pursuant to section 3056 of Title 18.



Privacy Act Exemptions

- **(k)(4) Exemption:** Required by statute to be maintained and used solely as statistical records.
- **(k)(5) Exemption:** Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information.



Privacy Act Exemptions

- **(k)(6) Exemption:** Testing and examination material.
- **(k)(7) Exemption:** Evaluation material used to determine potential for promotion in the Armed Services.



Government Contractors

- When a DLA contract requires the operation or maintenance of a system of records or requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records, the record system or the portion of the record system affected are considered to be maintained by DLA and are subject to the DoD Privacy Program (section (m)).



Government Contractors

- DLA applies the requirements of the Privacy Act to the contractor by placing the Federal Acquisition Regulation (FAR) clauses (Part 24, Protection of Privacy and Freedom of Information) in the contract.
- The contractor and its employees are to be considered employees of DLA for purposes of the criminal provisions during the performance of the contract.



Disclosure of the SSN

Section 7 (not codified as part of the Act)

- It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN.
- Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.



Other DoD Requirements

- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information; Reduce the Use of Social Security Numbers.
 - Eliminate Unnecessary Use.
 - Explore Alternatives.
- OUSD(P&R) Directive-Type Memorandum 07-015-USD(P&R) – “DoD Social Security Number (SSN) Reduction Plan” dated March 28, 2008



Other DoD Requirements

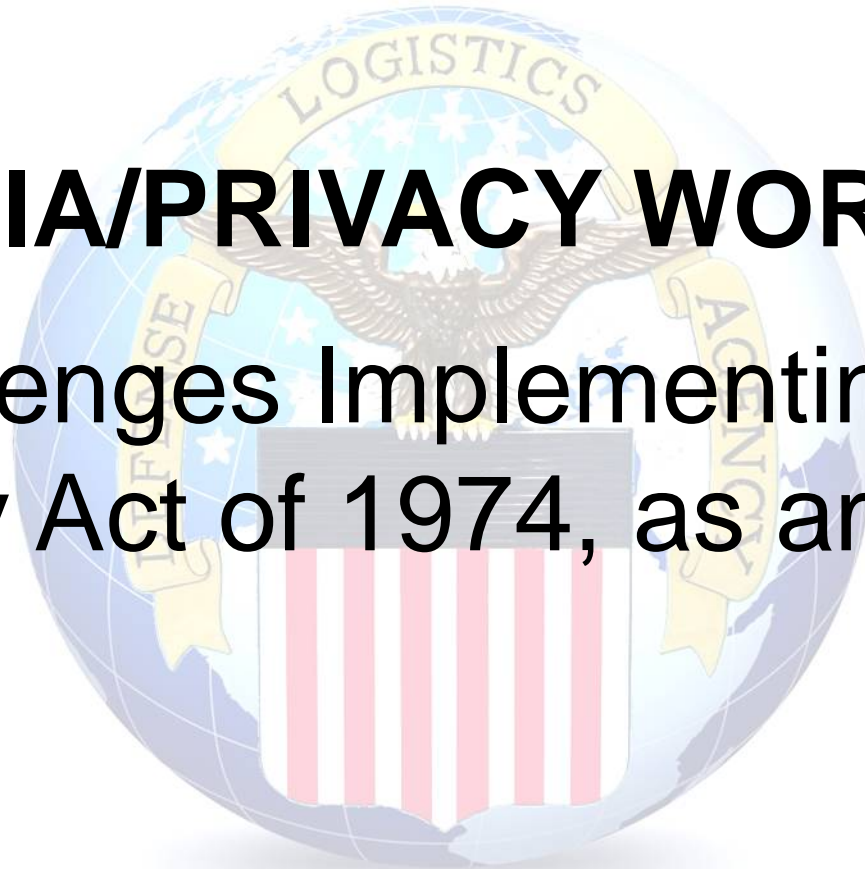
- OSD(DA&M) memo “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” dated June 5, 2009.
 - Privacy training is a prerequisite before an employee or contractor is permitted access to DoD information / systems.
 - Privacy training required annually.
 - Employees / contractors annually sign a document describing their responsibilities acknowledging their understanding.

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

DLA FOIA/PRIVACY WORKSHOP

Challenges Implementing the
Privacy Act of 1974, as amended





Privacy Implementation Challenges

1. Technologies' Rapid Pace of Change
 2. Timeliness of Guidance and Legislation
 3. System Dependence on Unique Identifiers
 4. Increased Demands for Appropriate Sharing of PII
 5. Ensuring Contractor Compliance
-
- I. Background Slides
 - A. ISPAB



Technologies' Rapid Pace of Change

- PII can be found anywhere:
 - Portable mass storage
 - *thumb drives, portable HD's, CDs*
 - Ubiquitous storage in common work appliances
 - copiers, faxes, B-berries
- Internet behavior is easily tracked:
 - Web browser tracking
 - cookies, zero pixel gifs, flash cookies
- Social Media is complex -- Web 2.0
 - Facebook, Twitter, YouTube
- Cloud Computing presents new issues
 - Gov't Cloud vs. Commercial Cloud
 - Geolocation and Jurisdiction



Timeliness of Guidance and Legislation

- Is OMB Guidance too old?
 - Privacy Act – published 1975 (40 FR 28948)
 - Computer Matching Act – published 1989 (54 FR 25818)
- Is Privacy Act still current? (Sep. 29, 1975)
 - Passed in response to:
 - abuse of Executive power, surveillance, wrongful disclosures
 - Amended by Computer Matching Act of 1988
 - Do definitions still have currency?
 - “System of Records”
 - Routine Use



System Dependence on Unique Identifiers

- IT Systems need unique ID's
 - SSN usage in DoD systems governed by SSN Reduction Plan
 - DoD Directive-Type Memorandum, 07-015-USD(P&R) “DoD Social Security Number Reduction Plan”
 - Several requirements for continued collection of SSNs
 - Truncated SSN's included
 - DLA Forms and J-6 Effort
- Biometrics seen as one option
 - ❖ DLA's involvement in Biometrics
 - DLA's Defense Standardization Program Office
 - The DoD Electronic Biometric Transmission Specification – Sept. 2008
 - Privacy Issues with Biometrics Include:
 - Statistical concerns
 - Due process for biometrics



Increased Demand for Sharing of PII

- **“Debt collection” drove demand in 1990’s**
- **“Terrorism Information” drives demand now.**
- **Information Sharing Environment (ISE) –**
 - **“Intelligence Reform and Terrorism Prevention Act of 2004,” Pub.L.108–458, Dec. 17, 2004**
 - **DoD is participant in ISE**
 - **Defense Privacy Office Director is DoD’s Privacy and Civil Liberties Officer (42 USC § 2000ee–1).**
 - **DoD’s ISE Privacy Framework is being developed.**
 - **Privacy Framework sets forth how ISE will function in compliance with Fair Information Practice Principles**



Sharing and the Labeling of PII

- **Labeling of PII when shared with others within the ISE must use new “Controlled Unclassified Information” labeling framework.**
 - **Presidential Memorandum (May 9, 2008)**
 - **DOJ & DHS Co-Chaired Task Force on Controlled Unclassified Information – Report to President (Aug. 25, 2009)**
 - **DoD Implementation:**
 - **DoD 5200. 1-R, “Information Security Program”**
 - **DTM 08-027 – “Security of Unclassified DoD Information on Non-DoD Information Systems,” September 16, 2010**



Contractor Compliance

- **For contracts involving operation of a “system of records,”**
 - **Contractors “shall be considered to be an employee of an agency.” -- 5 U.S.C. § 552a(m)(1)**
- **The FAR and DFARS refer to parts & clauses implementing requirement:**
 - FAR Part 24.1
 - Clauses 52.224-1, 52.224-2
 - FAR Part 39.1
 - Especially Part 39.105, “Privacy.”
 - DFARS Subparts 224.1 and 239.71



BACKGROUND



Information Security & Privacy Advisory Board

- **ISPAB reviewed Privacy Act and associated Gov't Privacy Policies/Practices – believes improvements need to be made. Recommends:**
 - Amendments to the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002.
 - Improvements to Government leadership on privacy.
 - Other necessary changes to privacy policy.

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



WARFIGHTER SUPPORT ENHANCEMENT

STEWARDSHIP EXCELLENCE

WORKFORCE DEVELOPMENT

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched atop a shield with vertical red and white stripes. The shield is set against a blue globe with white stars. A yellow banner arches over the eagle with the word "LOGISTICS" in black. Two other yellow banners, one on the left and one on the right, contain the words "DEFENSE" and "AGENCY" respectively.

Freedom of Information Act Exemption 4

Debbie Teer
October 26, 2010



Exemption 4

- Protects Release of:
 - Trade secrets
 - Commercial or Financial Information
 - Obtained from a person.
 - Privileged or confidential.



Voluntary or Required

- Critical Mass

(Critical Mass Energy Project v. NRC, 975 F.2d 871
(D.C. Cir. 1992))

- Voluntarily submitted

- Did agency exercise authority

- National Parks

(Nat'l Parks & Conservation Ass'n v. Morton, 498 F.2d 765
(D.C. Cir. 1974))

- Required

- Impairment prong
- Competitive harm prong
 - EO 12600



EO 12600

- Requires federal agencies to establish certain predisclosure notification procedures which will assist agencies in developing adequate administrative records.
 - Submitters of confidential commercial information.
 - Notify requester



Submitter Notice

- Letter includes:
 - Identifies requester and records requested
 - Factors to consider
 - National Parks
 - Reasonable period of time to respond
 - Contact information
 - FOIA case number
 - Copy of records
 - Submitter Notice Instructions



Submitter Notice

- Review the response
 - Has the submitter objected to release
 - Objection adequately supported
 - No response received
- Document your review and determination
 - Competitive harm analysis
 - Case-by-case
 - Reasonable segregation
 - Cannot withhold information created by the Federal Government



Intent to Release

- Submitter objections not sustained
 - Notify requester of intent to release
 - Provide reason for release
 - Use case law
 - Close letter with rights
 - Reverse FOIA



Unit Prices

- Definition:
Specified amounts to be paid by the government per item for goods or services
- Burden of Proof
 - Submitter
- Release of Unit Price



Unit Prices

- Federal Acquisition Regulation (FAR)
 - 15.506 Postaward debriefing of offerors.
 - Subpart 24.2—Freedom of Information Act



Unit Prices

– Reverse FOIAs

- Withheld

- McDonnell Douglas Corp. v. NASA , 180 F.3d 303 (D.C.C. 1999)
- McDonnell Douglas Corp v. USAF, 375 F.3d 1182 (D.C.C. 2004)

- Released

- Boeing Co. v. U.S. Department of the Air Force, 616 F Supp 2d 40, 2009 U.S. Dist.
- Pacific Architects and Engineers Inc., v. US Dept of State, 906 F.2d 1345 (1990)
- Martin Marietta Corp. v. John H. Dalton, 974 F. Supp. at 37 (1997)

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



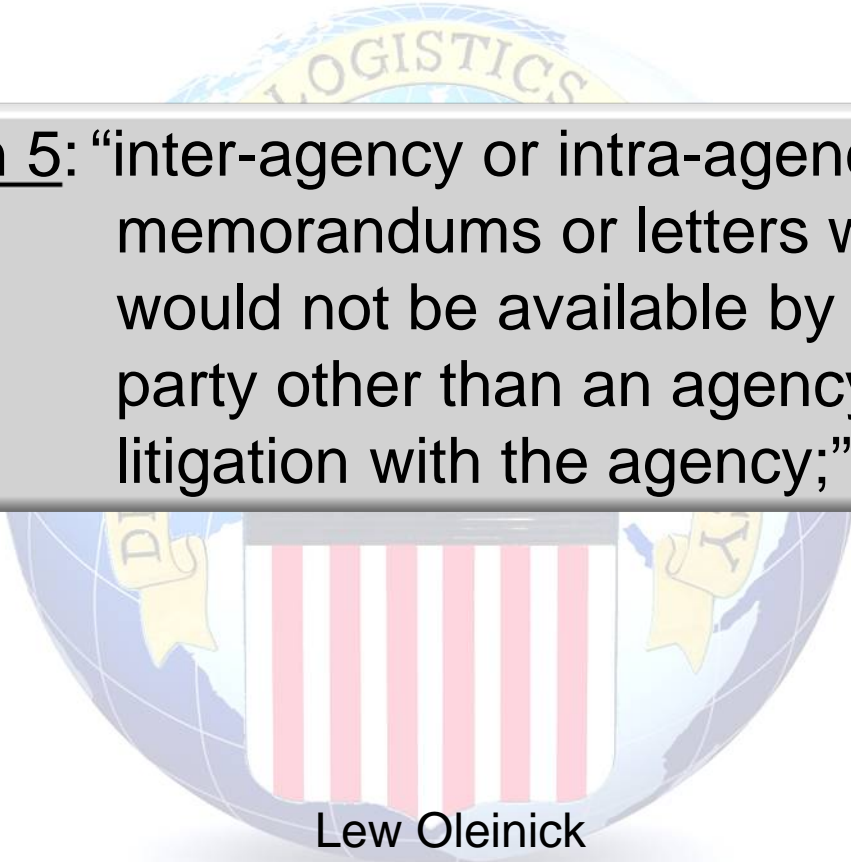
WARFIGHTER SUPPORT ENHANCEMENT

STEWARDSHIP EXCELLENCE

WORKFORCE DEVELOPMENT

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



Exemption 5: “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;”

Lew Oleinick

October 26, 2010



Outline

- What types of records are covered?
- What is Exemption 5 intended to protect?
- Purpose of Exemption 5
- Recognized privileges for Exemption 5
- Implications of President Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines and Proactive Disclosure



Exemption 5 Coverage

- Inter or intra agency records
- Records “normally privileged in the context of civil discovery”
- “To qualify, a document must thus satisfy two conditions:
 - its source must be a Government agency, and
 - it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it.¹”
 - Consultant Test

1. DOI v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 8-9 (U.S. 2001)



Purpose of Exemption 5

- to encourage open, frank discussions on matters of policy between subordinates and superiors;
- to protect against premature disclosure of proposed policies before they are finally adopted;
- protect against public confusion that might result from disclosure of reasons and rationales that were not in fact ultimately the grounds for an agency action.



Common privileges for Exemption 5

- Deliberative process
- Attorney work product
- Attorney-client



Deliberative Process

- Question to ask: What is the status of the record?
 - Two-part test: pre-decisional? deliberative?
 - Burden is upon agency to show record satisfies both parts of test.
- Deliberative portions protected:
 - analysis, evaluations, recommendations, advice
 - but see Tax Analysts v. IRS, 117 F. 3d 607, 617 (D.C. Cir. 1997).
- Factual portions generally not protected
- Incorporating into final agency decision may alter claim to privilege.



Attorney Work-Product

- “reasonable anticipation of litigation”
 - although specific claim need not be identified
- Covers: civil, administrative, and criminal proceedings.
 - Caveats
 - Documents not originally prepared in anticipation of litigation can’t assume work-product privilege
 - Documents prepared in “normal course of business” – not related to litigation – may not be protected.
- Prepared by: (1) attorney or (2) non-attorney supervised by attorney.
- Factual materials covered.
- No temporal limitation.



Attorney Client

- What is covered?
 - "confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice."
 - applies to facts divulged by a client to his attorney
 - any opinions given by an attorney to his client based upon, and thus reflecting, those facts
 - Not limited to litigation context
- Does the “client” have to be specified?
 - Maybe: see Elec. Privacy Info. Ctr. v. DOJ, 584 F. Supp. 2d 65, 80 (D.D.C. 2008)
- Special cases



Presidential and AG FOIA Policy

- President's January 21, 2009 and Attorney General's March 19, 2009 memoranda apply to Exemption 5.
 - President's on "presumption of openness"
 - "In face of doubt, openness prevails."
 - Do not withhold because of "speculative or abstract fears."
 - AG's Policy
 - Agency should not withhold information simply because it may do so legally.
 - If full release is not possible, agency "must consider whether it can make partial disclosure."
 - Recognizes FOIA disclosure requirement is not absolute and cites exemptions, nat'l security, & privileges.
 - Bottom Line: Return to "Foreseeable Harm" Standard



Foreseeable Harm Analysis

- Primary Factors to Guide Analysis
 - The nature of the decision
 - The nature of the decision-making
 - The status of the decision
 - The status of the personnel involved
 - The potential for process impairment
 - The significance of any process impairment
 - The age of the information
 - The sensitivity of individual record portions



Impact of FOIA Release on Privilege

- Discretionary disclosure under the FOIA does not waive privilege on similar records.
 - See
 - Nat'l Inst. of Military Justice v. United States DOD, 404 F. Supp. 2d 325, 2005 U.S. Dist. LEXIS 33154 (D.D.C. 2005)
 - Students Against Genocide v. Dep't of State, 257 F. 3d 828, 835-36 (D.C. Cir. 2001)
 - Salisbury v. United States, 690 F.2d 966, 971 (D.C. Cir. 1982)

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



Freedom of Information Act Exemptions 6 & 7(C)

Kathy R. Tennessee
October 26, 2010



Exemptions b(6) & 7(C)

The following analysis is used for both exemptions:

1. Is the exemption's threshold met?
2. Is there a privacy interest?
3. Is there a qualifying public interest?
4. Balance Public vs. Privacy Interest.



Exemption b(6)

Exemption b(6) threshold language:

“Personnel and medical files and similar files” when disclosure of such information “would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6).



Exemption b(7)(C)



- Exemption 7(C) threshold language:
 - Protects “records or information compiled for law enforcement purposes,” the disclosure of which “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”



Law Enforcement Records



According to the U.S. Department of Justice, “the mention of an individual's name in a law enforcement file will engender comment and speculation and carries a stigmatizing connotation.”

- Persons who are **NOT** targets of an investigation.

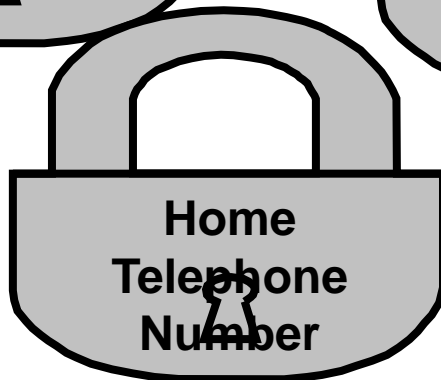
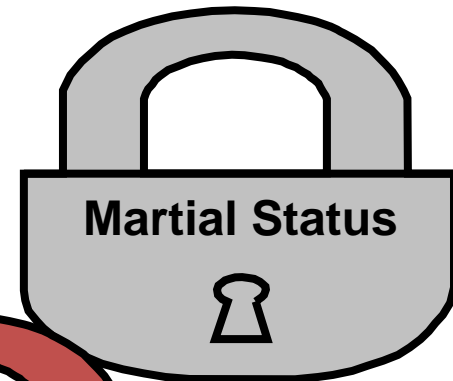
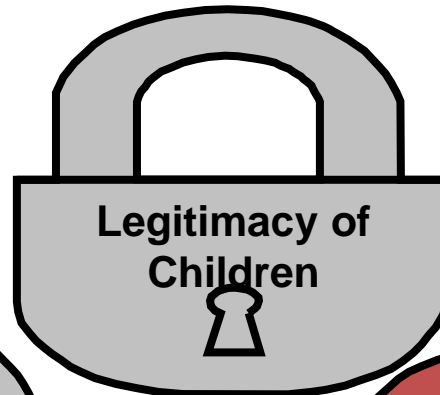
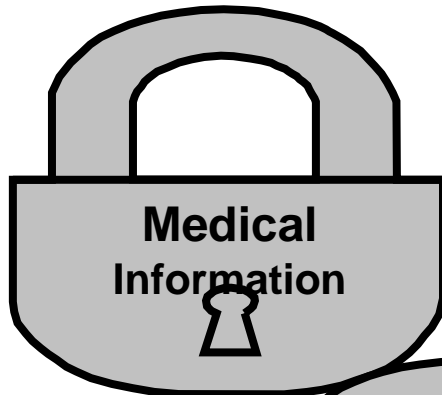
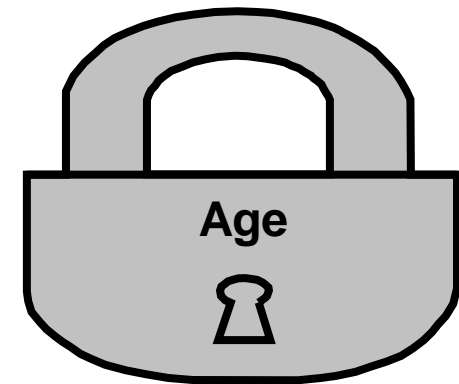
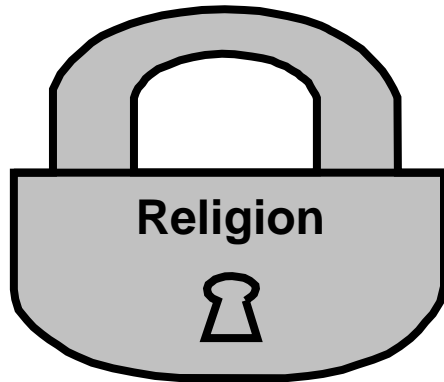


Is There a Privacy Interest?

- Consider the Sensitivity of Information
- Consider Adverse Consequences
- The passage of time does **not** diminish a privacy interest.



Identifying a Privacy Interest





Where There is No Privacy Interest

- **Corporations** – except small companies
- **Deceased Individuals** (except in extreme cases)
- **Public Records** – unless they are practically obscure.
- **Federal Employees** – OPM regulation, 5 C.F.R. 293.311
- **Identities of FOIA Requesters** – except personal information.



Balance the Privacy and the Public Interests

- If there is NO privacy interest, disclose the information.
- If there is a privacy interest, and no qualifying public interest, withhold the information.
- If there is a privacy interest and a public interest, balance them to determine which is greater.





Is There a Qualifying Public Interest?

The Supreme Court ruled in Reporters Committee that the public interest must fall within the FOIA's "core purpose" of shedding light on an agency's performance of its duties.



Is There a Qualifying Public Interest

Is the public interest directly served by the disclosure.





References

- U.S. Department of Justice(2009) *Guide to the Freedom of Information Act.*
- Office of Secretary of Defense Memo (2005) *Withholding of Information that Personally Identifies DoD Personnel.*

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

DLA FOIA/Privacy Training Workshop

Day 3

WELCOME

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched atop a shield with vertical red and white stripes. The shield is set against a blue globe with white stars. A yellow banner arches over the eagle with the word "LOGISTICS" in blue. Two vertical yellow banners on either side of the eagle contain the words "DEFENSE" and "AGENCY" respectively.

Fees and Fee Waivers

Judith Mansfield, DLA Disposition Services

Peggy Pasquinely, DLA Land & Maritime

October 28, 2010



Fees

- Fee Schedule
 - OMB Uniform FOIA Fee Schedule and Guideline
(http://www.dod.gov/pubs/foi/dfoipo/docs/OMB_Guidelines_FOIAFees.pdf)
 - DoD Rates



Fees

- Direct Costs
 - Search, Review, and Duplication
- Fee Declaration
 - Must be Adequate
 - Based on Requester Category



Fees

- Direct Costs
 - Search
 - Review
 - Duplication



Fees

- Requester Categories

Type of Requester	Direct Costs		
	Search	Review	Duplication
Commercial	Yes*	Yes	Yes
Educational Inst/ Scientific Inst/Media	No	No	Yes* (100 pgs free)
All Others	Yes * (2 hrs free)	No	Yes (100 pgs free)

*If answered in more than 20 days, cannot charge.



Fees

- Examples of Fee Declarations:
 1. I will pay all reasonable fees.
 2. I agree to pay reasonable duplication fees up to \$50.
 3. I agree to pay fees up to \$100.



Fees

- Exceptions to Charging Fees
 - Beyond 20 days
 - Less than \$15
 - Fee waiver requested



Fees

- Aggregating FOIA Request
 - Multiple Requests for Portions of a record or similar records
 - Believe Attempt to Circumvent Fees



Fees

- Fee Waiver
 - Considerations
 - Public interest
 - Contribution to public understanding
 - Commercial interest of requester
 - Made on a Case-By-Case Basis
 - Record in FOIAXpress



Fees

- Advance Payment
 - Fees over \$250
 - Past Delinquency



Fees

- DLA Best Practices
 - Aggregating Requests
 - Determining Media Category
 - Recording Fees Not Charged
 - Use FOIAXpress



Fees

- FAQs
 1. In addition to the per page copying charge, may costs be assessed for the time spent copying responsive documents?
 2. Who pays for the cost of mailing records to the requester?
 3. Why are FOIA fees deposited in the U.S. Treasury?



Fees

- FAQs
- 4. Into which fee category should a request submitted by an attorney be placed?
- 5. When should a fee waiver request be resolved?
- 6. May interest be charged on an overdue FOIA debt?

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



WARFIGHTER SUPPORT ENHANCEMENT

STEWARDSHIP EXCELLENCE

WORKFORCE DEVELOPMENT

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

The seal of the Defense Logistics Agency is centered in the background. It features a bald eagle with wings spread, perched on a shield with vertical red and white stripes. Above the eagle is a banner with the word "LOGISTICS". The entire seal is set against a light blue globe with white stars.

Referrals, Consultations, and Misdirected Requests

Debbie Teer & Kathy Tennessee
October 28, 2010



Definitions

- Referral
 - Responsive documents originated with another DoD Component or Federal agency.
- Consultation
 - Responsive records are sent to another DoD Component or Federal agency for review, provide a release recommendation, and respond back to the requesting agency.
- Misdirected Request
 - The entire request is routed to another DoD Component.



Referrals

- General Rule: Originating Agency is the Most Appropriate Agency to Make a FOIA Disclosure Determination.
- Contact Originating Agency.
- Notify Requester.



Consultations

- When to Consult:
 - Record contains information provided by other DoD Component or Federal Agency.
 - Other DoD Component or Federal Agency has an interest in the record.
 - Sensitivity of record.



Misdirected Requests

- Requested records are not under your cognizance.
 - No or minimal search is done.
 - Records are within the agency.
 - Do not perfect request.
 - Notify requester.



Routing Requirement

- Open Government Act 2007
 - 20-day time period begins on the date the request is first received by the appropriate component of the agency, but in any event not later than 10 business days after the request is first received by any component of the agency this is designated to receive requests.



Considerations

- Are these agency records.
- Who can best respond.
- Is the originator subject to the FOIA.
- Placement in queue.
- Always refer, route, and consult with the FOIA Office.

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



E-FOIA, Electronic Reading Rooms,
the OPEN Government Act of 2007,
and
Proactive Disclosure



Agenda

- Statutory Authority
- Policy Basis
 - E-FOIA
 - Open Government
 - “Foreseeable Harm” Standard
- DOJ’s Two-Part Test
- DOJ Implementing Guidance
- DoD Requirements
- DLA Implementation



Statutory Authority

- Electronic FOIA Amendments of 1996 (Pub.L. 104–231)
 - Reading Rooms – per 5 USC § 552 (a)(2)
 - Agency “shall make” available by “computer telecommunications”:
 - Index describing – per 5 USC § 552 (a)(2)(e), and
 - Copies of all Records – per 5 USC § 552 (a)(2)(d)
 - which have been released to any person under FOIA
 - have become, or are likely to become, the subject of subsequent requests for substantially the same records



Statutory Authority

- Freedom of Information Act (5 USC § 552)
 - Without any requests, the following shall be posted proactively:
 - Agency Rules of Procedure →
per (a)(1)(c)
 - Agency Substantive Rules →
per (a)(1)(d)
 - Administrative Staff Manuals and Instructions that
affect a member of the public → per
(a)(2)(c)



Policy Basis – E-FOIA

- Executive Order 13392, “Improving Agency Disclosure of Information,” Dec. 19, 2005
- Presidential Memorandum on FOIA – Jan. 21, 2009
 - Among first acts of President’s first day in office
 - Presumption of disclosure for all FOIA requests.
 - Agencies should take affirmative steps to make information public.
 - Use modern technology to inform citizens – don’t wait for requests.
- White House COS/GC Memo on FOIA – Mar. 16, 2010
 - Asks Agency Heads to revise FOIA regulations to incorporate President’s policies of 1/21/2009
 - Asks Agency Heads to review resources for FOIA to ensure they are “responding to FOIA requests promptly and cooperatively, consistent with the requirements for addressing this Presidential priority.”



Policy Basis – Open Gov't

- Presidential Memorandum on Open Government and Transparency – Jan. 21, 2009
 - “disclose information rapidly in forms that the public can readily find and use”
 - “harness new technologies to put information about their operations and decisions online”
- OMB Memorandum M-10-06, “Open Government Directive.”
 - Don’t wait for FOIA requests to put useful information onto your website
 - Agency annual FOIA report must be posted in XML format on DLA’s Open Gov’t website



Policy Basis – “Foreseeable Harm”

- Presidential Memorandum on FOIA – Jan. 21, 2009
 - “The Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails.”
 - “presumption of disclosure should be applied to all decisions involving FOIA.”
- Attorney General Memorandum on FOIA – March 19, 2009
 - Warning
 - Agency should not withhold “simply because it may do so legally.”
 - Agency should not withhold merely because records technically fall within scope of FOIA exemption
 - Partial Disclosure
 - If you can’t make a full disclosure, review for partial. FOIA already requires this.
 - Rescinded Oct. 12, 2001 AG FOIA Memorandum
 - Creates two-part test for when DOJ will defend an Agency denial of a FOIA request.



DOJ's Two-Part Test

- DOJ will defend a denial of a FOIA request only if:
 1. agency reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions, or
 2. disclosure is prohibited by law.
- Returns to “foreseeable harm” standard established by DOJ in 1993



DOJ's Implementing Guidance

- DOJ on discretionary disclosures:
 - “There is no doubt that records protected by Exemption 5 hold the greatest promise for increased discretionary releases under the Attorney General's Guidelines.”
 - Impact of discretionary disclosures on the ability of an agency to protect other, similar documents?
 - Courts have found discretionary disclosure waives FOIA exemption only for those specific documents released.
 - Courts recognize general rule of non-waiver through discretionary disclosure, i.e., releasing a document does not waive ability to assert FOIA exemption for all documents of that type.



DOJ Implementing Guidance

- FOIA Reading Rooms
 - U.S. Department of Justice Guide to the FOIA, 2009 Edition
 - FOIA Reading Room Requirements
 - Definition of “frequently requested”
 - Which records should be posted?
 - Agency personnel should use →
 - Knowledge of requester community, plus
 - prior FOIA request history to determine which records are:
 - “frequently requested,” and would likely be of
 - “subsequent interest”



DoD Requirements

- D(A&M) Memo's on DoD FOIA Web Sites:
 - Sep. 26, 2006
 - “each FOIA Requester Service Center must have a dedicated web site containing information that will assist FOIA requesters in obtaining information from the government.”
 - Field Activities must link to the primary FOIA Requester Service Center (FRSC) web site
 - Oct. 11, 2007
 - DoD Components' main FOIA web site must have Electronic Reading Room
 - Components with multiple FRSCs must maintain E-Reading Room -- maintain link on main FOIA web site to Field FRSC's reading room.
 - Either way, Electronic Reading Room must be easily accessible by the public.
 - Jun. 24, 2008
 - DoD FOIA Program Office requires DoD Component certification of compliance with FOIA for E-Reading Room.



DLA's Reading Room

5 U.S.C. § 552(a)(2)(A) Records – Final opinions and orders made in the adjudication of cases that may be cited, used, or relied upon as precedents in future adjudications.

DLA does not possess this type of record. Refer to DOD [Requester Service Center Reading Room](#).

5 U.S.C. § 552 (a)(2)(B) Records – Statements of policy and interpretations that have been adopted by the agency and are not published in the Federal Register.

HQ DLA

- [DLA General Orders](#).

Defense Supply Center Richmond

- [Critical Item Source Approval Guidance](#).

5 U.S.C. § 552 (a)(2)(C) Records – Administrative staff manuals and instructions, or portions thereof, that establish DoD policy or interpretations of policy that affect the public.

- [DoD Publications](#)
- [DOD Handbook for Requesters](#)
- [Defense Freedom of Information Policy Office](#)
- [DLA FOIA Regulations](#)
- [DLA Privacy Regulations](#)
- [DLA Publishing System \(DLAPS\)](#)
- [Defense Logistics Acquisition Directive \(DLAD\), Procedures, Guidance and Information \(PGI\) Web page](#)
- [DSCR Acquisition Reference List](#)
- [DESC Publications](#)



DLA's Reading Room

5 U.S.C. § 552 (a)(2)(D) Records – Records released to the public, under the FOIA, that are or will likely become the subject of subsequent requests. (e.g., FOIA Logs, annual reports)

HQ DLA

- [Defense Logistics Agency Procurement Data](#)
- [DLA Internet Bid Board Data System](#)
- [Top 100 DLA Contractors](#)
- [DLA Procurement Gateway](#) (Retired - contains legacy procurement info)

Defense Supply Center Columbus

- [DSCC Specification Finder](#)
- [Index of DSCC Mil Specs & Drawings](#)
- [Business Opportunities](#)

Defense Supply Center Richmond

- [DSCR Corporate Contracting](#)

Defense Energy Support Center

- [Frequently Requested DESC Records](#)

Conventional Reading Rooms

Public reading rooms are located at the HQ DLA facility and at the DLA Field Activities. Contact the appropriate DLA FOIA / Privacy Contact to make an appointment to gain access to their FOIA reading room.



Break time!

