

ADMINISTRATIVE AND CIVIL LAW DEPARTMENT



Government Information Practices Deskbook 2015

The Judge Advocate General's School
United States Army

ADMINISTRATIVE AND CIVIL LAW DEPARTMENT
GOVERNMENT INFORMATION PRACTICES DESKBOOK

2015

TABLE OF CONTENTS

Chapter	Topic
A	Freedom of Information Act
B	Privacy Act
C	Health Insurance Portability and Accountability Act (HIPAA)
	Part I: Military Command Exception
	Part II: HIPAA/Privacy Act Comparison
	Part III: HIPAA Guide for Law Enforcement

CHAPTER A

FREEDOM OF INFORMATION ACT

5 USC §552

Outline

I. REFERENCES.....	2
II. INTRODUCTION.....	3
III. RELEASING AGENCY RECORDS.....	4
IV. KEYS TO UNDERSTANDING THE FOIA.....	5
V. PROCESSING REQUESTS FOR RELEASE.....	10
A. REQUIREMENT FOR A PROPER REQUEST.....	10
B. REQUIRED AGENCY RESPONSE.....	11
C. REQUIREMENT TO MEET STATUTORY TIME LIMITS.....	13
D. DOCUMENTING AGENCY ACTION ON REQUESTS.....	14
E. CALCULATING FEES & PROCESSING FEE WAIVER REQUESTS.....	14
F. LITIGATING DENIED AND CONSTRUCTIVELY DENIED FOIA REQUESTS.....	16
VI. NINE EXEMPTIONS PERMIT WITHHOLDING.....	20
A. EXEMPTION 1: CLASSIFIED RECORDS.....	20
B. EXEMPTION 2: INTERNAL PERSONNEL RULES AND PRACTICES.....	22
C. EXEMPTION 3: OTHER FEDERAL WITHHOLDING STATUTES.....	23
D. EXEMPTION 4: TRADE SECRETS, AND COMMERCIAL AND FINANCIAL RECORDS.....	25
E. EXEMPTION 5: PRIVILEGED MEMORANDA & INTERNAL AGENCY COMMUNICATIONS.....	30
F. EXEMPTION 6: PROTECTION OF PERSONAL PRIVACY.....	33
G. EXEMPTION 7: LAW ENFORCEMENT RECORDS.....	36
H. EXEMPTION 8: FINANCIAL INSTITUTIONS INFORMATION.....	41
I. EXEMPTION 9: GEOLOGICAL AND GEOPHYSICAL INFORMATION.....	41
VII. EXCLUSIONS.....	42
VIII. CONCLUSION.....	43

I. REFERENCES.

A. Primary Sources.

1. Freedom of Information Act, 5 U.S.C. § 552, as amended [most recently by the “Openness Promotes Effectiveness in Our National Government Act of 2007” (OPEN Government Act of 2007) signed 31 December 2007].
2. Department of Defense Directive No. 5400.7, DOD Freedom of Information Act Program (2 January 2008).
3. Department of Defense Regulation No. 5400.7-R, DOD Freedom of Information Act Program (11 April 2006, Change 1).
4. Army Regulation No. 25-55, The Department of the Army Freedom of Information Act Program (1 November 1997) (does not include 1996 amendments to the Freedom of Information Act).
5. Air Force Manual, DOD 5400.7-R_AFMAN 33-302, Freedom of Information Act Program (21 October 2010).
6. Secretary of the Navy Instruction 5720.42F, Department of the Navy Freedom of Information Act Program (6 January 1999).
7. Marine Corps Order 5720.63, Publication in the Federal Register, Indexing, and Public Inspection of Marine Corps Directives (2 August 1991, Change 1).
8. Commandant's Instruction M5260.3 - The Coast Guard Freedom of Information and Privacy Acts Manual (6 April 2005, Change 5).

B. Secondary Sources.

1. DoJ Guide to the Freedom of Information Act, a Department of Justice publication (available on the World Wide Web at <http://www.justice.gov/oip/doj-guide-freedom-information-act-0>) [hereinafter DOJ FOIA Guide].
2. Freedom of Information Case List and updates, a Department of Justice publication (available at <http://www.usdoj.gov/oip/cl-tofc.html> (pre-May 2002)). Additional case list updates available at <http://www.justice.gov/oip/court-decisions.html>.
3. FOIA UPDATE, a newsletter issued quarterly by the Justice Department's Office of Information and Privacy (OIP), from 1979-2000. Available on the DoJ FOIA Web site at www.usdoj.gov/oip/foi-upd.htm.
4. FOIA Post, a Web-based successor to the FOIA UPDATE, is electronically published by the DoJ and is available at:

www.usdoj.gov/oip/foiapost/mainpage.htm.

5. “Summaries of New Decisions” a feature of FOIA Post, a monthly compilation of all FOIA decisions received by the DoJ Office of Information and Privacy, is available at www.usdoj.gov/oip/foiapost/mainpage.htm.

6. Military Resources Available On-Line.

a. Department of Defense – <http://www.dod.mil/pubs/foi/>

b. Army – <https://www.rmda.army.mil/organization/foia.shtml>

c. Navy – <http://foia.navy.mil/toolkit.asp>

d. Marine Corps –
<http://www.marines.mil/unit/hqmc/foia/Pages/USMCFOIARESOURCE%20MAT%20ERIALS.aspx>

e. Air Force – <http://www.foia.af.mil/>

f. Coast Guard – <http://www.uscg.mil/foia>

II. INTRODUCTION.

A. History/Purpose.

1. Freedom of Information Act (FOIA) was enacted in 1966, and took effect 5 July 1967. It revised the public disclosure section of the Administrative Procedure Act. 5 U.S.C. § 1002 (1964) (enacted in 1946, amended in 1966, and now codified at 5 U.S.C. § 552.)

2. “The basic purpose of the FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.” NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978). The FOIA firmly established an effective statutory right of public access to executive branch information in the federal government.

B. Key Concepts.

1. Applies to any and all agency records within the government’s possession and control.

2. Disclosure is the rule, not the exception.

3. Generally, the status of the requester and purpose of a request are irrelevant with respect to what records are disclosed. [Requester status is relevant regarding expedited access, fees, and attorney fees].

4. The government has the burden to justify withholding of information.
5. The requester may seek administrative and judicial relief if access to government information is improperly denied.

III. RELEASING AGENCY RECORDS.

A. Publication. § 552(a)(1) (Requires disclosure of agency procedures, substantive rules, functions, organization and general policy through Federal Register publication).

1. How to obtain information from the agency: DOD Reg. 5400.7-R, AR 25-55, DOD 5400.7-R/AFSUP1, SECNAVINST 5720.42F, and MCO 5720.63.
2. Rules of procedure and how to make submissions to the agency: Federal Acquisition Regulation (FAR), DOD FAR Supp., and Army FAR Supp. (AFARS)(contract submissions).
3. Substantive rules of general applicability. NI Industries v. United States, 841 F.2d 1104 (Fed. Cir. 1988); Vigil v. Andrus, 667 F.2d 931 (10th Cir. 1982); United States v. Mowat, 582 F.2d 1194 (9th Cir. 1978); Pruner v. Department of the Army, 755 F. Supp. 362 (D. Kan. 1991).

B. "Reading Room" Materials. § 552(a)(2) (Requires agency to make "available for public inspection and copying" records of final opinions, policy statements, administrative staff manuals, and frequently requested material.) Stanley v. Department of Defense, et al., No. 98-CV-4116 (S.D. Ill. June 22, 1999) (military hospital operational manuals are "internal housekeeping rules" as opposed to the kind of material of interest to the general public.)

1. Final opinions rendered in the adjudication of cases, specific policy statements, and certain administrative staff manuals. Vietnam Veterans of America v. Department of the Navy, 876 F.2d 164 (D.C. 1989).
2. The agency does not need to make available materials "related solely to the [agency's] internal personnel rules and practices." Hamlet v. United States, 63 F.3d 1097 (Fed. Cir. 1995), see, DOJ FOIA Guide.
3. Copies of disclosed records, frequently requested under FOIA (generally, three approved requests).
4. Reading Room records created after 1 November 1996 must be available on an agency's website.
5. Index for Public Inspection- final opinions of adjudicated cases; policies statements and interpretations not published in Federal Register; administrative staff manuals and instructions that affect a member of the public; frequently requested records that have been previously released.

C. Release Upon Request. § 552(a)(3). This is the most common means by which the public accesses Government records (and the subject of the remainder of this outline.)

IV. KEYS TO UNDERSTANDING THE FOIA.

A. Key Definitions.

1. What is an “agency?” § 552(f). “Agency” means “any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.”

a. However, the Office of the President and those organizations within the Executive Office of the President whose function is limited to advising and assisting the President are excluded from the definition of agency.

b. Subdivisions of an agency are not treated as independent agencies. Judicial Watch, Inc. v. FBI, 190 F.Supp.2d 29, 30 n.1 (D.D.C. 2002) (stating that proper defendant is the Department of Justice “rather than the FBI, which is a component of DOJ and therefore not an “agency” within the statutory definition”).

c. The Department of Defense is our agency.

(1) The Departments of the Army, Air Force, and Navy are components of an agency. Schwartz v. General Accounting Office, No. 00-369, (D.D.C., Nov.13, 2001) (subdivisions of an agency and individual employees are not proper party defendants under the FOIA).

(2) Federally recognized Army National Guard units are considered part of the Army, therefore, they fall within the definition of an “agency” for FOIA and Privacy Act purposes. In Re: Sealed Case, 551 F.3d 1047 (D.C. Cir. 2009)(holding that as long as the Secretary of the Army has not withdrawn a National Guard’s federal recognition, it is part of an agency for purposes of the Privacy Act [and thus the FOIA’s] whether or not federally activated). The Privacy Act adopts the Freedom of Information Act’s definition of agency (5 USC § 552a(a)(1)).

d. Under the FOIA, the term agency does not include:

(1) Congress, Judiciary, Office of the President (including Advisors), or state agencies. Wright v. Curry, 122 F.App'x 724, (5th Cir. 2004) (state agencies are “expressly exclude[d]” from scope of FOIA); Armstrong v. Executive Office of the President, 90 F.3d 553 (D.C. Cir. 1996) (offices within the Executive Office of the President whose functions are limited to advising and assisting the President do not fall within the definition of “agency”), cert. denied, 117 S.Ct. 1842 (1997); Dow Jones & Co., Inc. v. Department of Justice, 917 F.2d 571 (D.C. Cir. 1990) (Congress is not an agency for FOIA); Dong v. Smithsonian Inst., 125 F.3d 877 (D.C. Cir. 1997) (holding that Smithsonian lacks both the “authority” necessary for it to qualify as an “authority of the government of the United States” under § 551(1) and the executive Department status necessary under § 552(f)), cert. denied, 524 U.S. 922 (1998)).

(2) Private organizations, unless the government engages in “extensive, detailed, and virtually day-to-day supervision.” Burka v. HHS, 87 F.3d 508 (D.C.Cir. 1996) (finding data tapes created and possessed by contractor to be agency records because of extensive supervision exercised by agency which “evidenced” constructive control”).

(3) Private citizens. See Allnut v. Department of Justice, 99 F.Supp. 2d 673 (D. Md. 2000) (records held by private trustee acting as agent for the federal government not subject to the FOIA).

2. What is a “record?” Information collected, produced or maintained by the government which is within the possession and control of the government and which is readily retrievable and reproducible.

a. “Readily Retrievable and Reproducible.” Examples include: Books, papers, maps, and photographs, and machine readable materials, regardless of physical form. DOD Reg. 5400.7-R, para. C1.4.3.1.

b. “Possession and Control.” An agency must both possess and control the record. Department of Justice v. Tax Analysts, 492 U.S. 136 (1989) (agency must create or obtain the records and must have them in possession because of the legitimate conduct of agency business). DOD Reg. 5400.7-R, para. C1.4.3.3.

(1) Possession of records created by another agency. McGehee v. CIA, 697 F.2d 1095 (D.C. Cir. 1983).

(2) Records generated from sources outside the Government. Records must be either government-owned or subject to substantial government control or use. Burka v. HHS, 87 F.3d 508 (D.C. Cir. 1996) (data tapes created and possessed by contractor are agency records because they are “constructively controlled” through agency’s excessive supervision); Hercules, Inc. v. Marsh, 839 F.2d 1027 (4th Cir. 1988) (contractor-prepared Army post telephone directory is government record because book was government-financed and bore “Property of U.S.” legend).

(3) Research Data. Amendment to the Fiscal Year 1999 Omnibus Appropriations Bill required modification of OMB Circular A-110 to allow private parties access to non-profit grantee-held research data through FOIA request [modifying Supreme Court decision in Forsham v. Harris, 445 U.S. 169 (1980) (which held records in possession of federal contractors not accessible under the FOIA even if records relate to contractor's contract with the agency)].

(4) Government contractors managing government records. OPEN Government Act of 2007 clarifies definition of "record" to include information "maintained for an agency by an entity under government contract, for the purpose of records management."

(5) Not agency records where records are not maintained under contract for records management. Historical records of calls maintained by Verizon Wireless, a government Blackberry service provider, do not qualify as "agency records" under 5 U.S. C. 552(f)(2)(B) because they are not "maintained for an agency by an entity under Government contract, for the purposes of records management." Amer. Small Bus. League v. SBA, 623 F.3d 1052 (9th Cir. 2010).

c. What is not a "record?"

(1) Personal records. Documents created or maintained without official requirement for the convenience of the creator as a memory refresher and not shared with others for agency use. See Bureau of Nat'l Affairs v. United States Department of Justice, 742 F.2d 1484 (D.C. Cir. 1984) (uncirculated appointment calendar and telephone message slips of agency official are not agency records); Fortson v. Harvey, 407 F.Supp. 2d 13 (D.D.C. 2005) (Army officer's notes of investigation were personal records because notes were used only to refresh officer's memory and were neither integrated into agency files nor relied on by other agency employees). DOD Reg. 5400.7-R, para. C1.4.3.2.

(2) Tangible, evidentiary objects. Nichols v. United States, 325 F.Supp 130 (D. Kan. 1971) (archival exhibits consisting of guns, bullets, and clothing pertaining to assassination of President Kennedy are not records); Matthews v. United States Postal Service, No. 92-1208, slip op. at 4, n. 3 (W.D. Mo. Apr. 14, 1994) (computer hardware is not a record).

(3) Documents generated by and under the control of "non-agency" Federal entities. United States v. Anderson, Crim. No. 95-0040, 2003 U.S. LEXIS 725 (E.D. La. Jan. 16, 2003) (grand jury transcripts are court records and, therefore, are not agency records under the FOIA).

(4) A request for uncompiled data (selective information) is not a request for records. Borom v. Crawford, 651 F.2d 500 (7th Cir. 1981) (affirming summary judgment order denying request for parole data compiled by race when no such compilation existed); Krohn v. DOJ, 628 F.2d 195 (D.C. Cir. 1980).

d. The FOIA does not require agencies to create or retain records. Flight Safety Services Corp. v. Department of Labor, 326 F.3d 607 (5th Cir. 2003) (requester's demand that the agency "simply insert new information in the place of the redacted information requires the creation of new agency records, a task the FOIA does not require the government to perform"); DOD Reg. 5400.7-R, para. C1.5.7.

(1) Agency does not have to respond to requester questions. Zemansky v. EPA, 767 F.2d 569 (9th Cir. 1985).

(2) DOD may create a new record when more useful to requester or less burdensome to agency. DOD Reg. 5400.7-R, para C1.5.7.

(3) While the FOIA does not require agencies to create or retain records, the Federal Records Act (now known as the National Archives Act), 44 U.S.C. § 2101 *et seq.*, does require record retention pursuant to National Archives and Records Administration schedules. The National Archivist is presently involved in litigation over his orders regarding the retention/destruction of electronic mail/messages.

B. Key Factors Affecting Release.

1. Rule of Segregability. § 552(b); DOD Reg. 5400.7-R, para. C5.2.4.

a. Must segregate and release portions of agency records not subject to a withholding exemption. Trans-Pacific Policing Agreement v. United States Customs Serv., 177 F.3d 1022 (D.C. Cir. 1999) (remanded for determination if 10- digit shipping code number could be segregated); Ogelsby v. Department of the Army, 79 F.3d 1172 (D.C. Cir. 1996); Army Times Publishing Co. v. Department of the Air Force, 998 F.2d 1067 (D.C. Cir. 1993).

b. Nonexempt material is not "reasonably segregable" when efforts to segregate amount to an inordinate burden on the agency. Lead Industries Association v. OSHA, 610 F.2d 70 (2d Cir. 1979).

2. Status and purpose of requester.

a. As a general rule, status and purpose of the requester are not considered by the agency except in deciding procedural matters such as expedited processing and fee issues. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

b. A foreign government is a person under the Act. DOD Reg. 5400.7-R, para. C5.1.3; Neal-Cooper Grain Co. v. Kissinger, 385 F. Supp. 769 (D.D.C. 1974). **However, there are exceptions:**

c. The Intelligence Authorization Act of 2003, Public Law No. 107-306, 116 Stat. 2383 (2002) amended the FOIA, at 5 U.S.C. § 552(a)(3)(E)(ii), to preclude elements of the intelligence community from disclosing any records in response to a FOIA request made by any foreign government or international governmental organization, either directly or through a representative. Elements of the intelligence community are identified in 50 U.S.C. § 401a.(4) (includes the Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; and other elements within various Federal agencies).

d. Fugitives are not “persons” for purposes of the FOIA. Doyle v. Department of Justice, 668 F.2d 1365 (D.C. Cir. 1981) (fugitive is not entitled to enforcement of FOIA’s access provisions because he cannot expect judicial aid in obtaining government records related to sentence that he was evading); *but see* O’Rourke v. Department of Justice, 684 F.Supp. 716 (D.D.C. 1988) (convicted criminal, fugitive from his home country and undergoing U.S. deportation proceedings, qualified as “any person” for FOIA purposes).

3. Previous releases

a. “Release to one equals release to all.”

b. Waiver issues. Students Against Genocide v. Department of State, 257 F.3d 828 (D.C. Cir. 2001) (exemptions were not waived when withheld photographs were displayed, but not distributed, by then-UN Ambassador Madeline Albright during presentation to U.N. Security Council).

4. Discretionary releases. Even if a FOIA exemption applies to information, agencies may decide to release the information unless prohibited by another statute.

a. Department of Justice posture: The Reasonably Forseeable Harm” Standard. The FOIA’s exemptions do not require the withholding of information. Agencies have great discretion in determining whether to release requested information.

(1) On 21 January 2009, President Obama issued guidance emphasizing that the FOIA “should be administered with a clear presumption: In the face of doubt, openness prevails” and that, “[a]ll agencies should adopt a presumption in favor of full disclosure.” Under this guidance, agencies are strongly encouraged to make discretionary releases when appropriate. On 19 March 2009, AG Holder published guidance implementing the President’s policy. This guidance states that the DOJ will defend a denial of records only if **(1) the agency**

reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions, or (2) disclosure is prohibited by law.

(2) Implementing the “Reasonably Foreseeable Harm” Standard. Most exemptions already require the identification of some harm to an interest protected by the exemption before the exemption even applies. Therefore, those exemptions are not impacted by the new policy and discretionary releases would not be appropriate. In those situations, agencies must reasonably segregate any non-exempt information and make as much disclosure as possible. Exemptions least affected by the Least affected by the new policy are: Exemption 1, 3, 4, 6, and 7.

5. Department of Defense Posture, **pending new guidance:**

a. **DOD employees must “exercise great caution” in the release of information related to DOD work.** [See Memorandum, Deputy Secretary of Defense, Subject: Operations Security Throughout the Department of Defense, dated 18 Oct 2001, at http://www.dod.gov/pubs/foi/dfoipo/docs/names_removal.pdf.]

b. DOD is statutorily authorized to withhold personal identifying information related to personnel stationed overseas or with sensitive or routinely deploying units. [See 10 U.S.C. § 130(b).] Current policy requires a much greater protection of information post 9/11 and any information “that personally identifies DoD personnel [is to] be more carefully scrutinized and limited. Under this policy, personally identifying information may be inappropriate for inclusion in any medium available to the general public.” [See Memorandum, Office of the Secretary of Defense, Subject: Withholding Information that Identifies DoD Personnel, dated 1 Sep 2005, at http://www.dod.gov/pubs/foi/dfoipo/docs/1sep2005memo_PII.pdf.]

6. Format of Records. The 1996 amendments to the Freedom of Information Act (the Electronic Freedom of Information Act Amendments, or “EFOIA”) give the requester choice of format, where readily reproducible. Dayton Newspapers, Inc. v. Department of the Air Force, 35 F. Supp.2d 1033 (S.D. Ohio 1998); *but see* Students Against Genocide v. Department of State, 257 F.3d 828 (D.C. Cir. 2001) (agency is not required to produce new photographs at a different resolution in order to mask the capabilities of the reconnaissance systems that produced them; such a step is not merely a matter of requester’s choice of “format”).

V. PROCESSING REQUESTS FOR RELEASE.

A. Requirement for a Proper Request. DOD Reg. 5400.7-R, para. C1.4.2.

1. Must request an “agency record.” DOD Reg. 5400.7-R, para., C1.4.3.

2. Must reasonably describe the record. DOD Reg. 5400.7-R, para., C1.5.8. See Ruotolo v. Department of Justice, 53 F.3d 4 (2d Cir. 1995); AFGE v. Department of Commerce, 907 F.2d 203 (D.C. Cir. 1990); Mason v. Calloway, 554 F.2d 129 (4th Cir. 1977).

3. Must comply with agency rules. DOD Reg. 5400.7-R, para. C1.4.2.

a. Written request required. (“written requests may be received by postal service or other commercial delivery means, by facsimile, or electronically”).

b. Must express willingness to pay fees or, in the alternative, explain why a waiver of fees is appropriate.

c. Must direct request to the proper DOD component. DOD Reg. 5400.7-R, para. AP 2.2.

d. Must expressly or impliedly invoke FOIA or an implementing regulation.

B. Required Agency Response. **Note:** Each service has established release and processing procedures. DOD Reg. 5400.7-R, para. C1.4.2; AR 25-55, ch. V; DOD 5400.7-R/AFSUP1; SECNAVINST 5720.42F, para. 8.

1. Agency must advise requester of agency’s receipt of the request and, if necessary, forward request to the proper agency records custodian.

2. Agency should liberally construe FOIA requests. See LaCedra v. Exec. Office for U.S. Attorneys, 317 F.3rd 345 (D.C. Cir. 2003) (in view of obligation “to construe a FOIA request liberally,” reading of plaintiff’s FOIA request -- for “all documents pertaining to my case . . . [and] specifically” for rewards and fingerprints -- to include only those specific items was “simply implausible” and “also wrong”).

3. Agency must evaluate the request for processing priority. The Electronic FOIA amendments modified the court-sanctioned rule of “first-in, first-out” FOIA processing. Open America v. Watergate Special Prosecution Force, 547 F.2d 606 (D.C. Cir. 1976).

a. Agencies may establish “multi-track” processing in which requests are sorted in accordance with the complexity of the request or potential volume of responsive document. See FOIA Update, Vol. XVIII, No. 1, at 6.

b. Agencies must have procedures to for expedited processing when exceptional circumstances surround a request, such as an imminent threat to life or personal safety or if the requester is a “person primarily engaged in disseminating information” and there is an “urgency to inform the public of actual or alleged Federal Government activity.” Al-Fayed v CIA, 254 F.3d 300 (D.C. Cir. 2001) (no expedited processing because there is no evidence that events connected to the deaths of Princess Diana and Dodi Al-Fayed

are matters of “current exigency” to the American public); Tripp v. DoD, 193 F. Supp. 2d 229 (D.D.C. 2002) (expedited processing denied because requester is not “primarily engaged in the activity of disseminating information,” even though “she has been the object of media attention, and has at times provided information to the media”; requester’s “job application to the Marshall Center and the resulting alleged Privacy Act violations by DoD are not the subject of any breaking news story.”)

c. Agency must make “reasonable efforts” to locate records and court may require agency to demonstrate adequacy of search. Dayton Newspapers, Inc. v. VA, 257 F.Supp. 2d 988 (S.D. Ohio 2003) (pursuant to its FOIA regulations, the VA was obligated to search only its headquarters, absent a clear indication that plaintiff sought records maintained in a VA regional office), *sustaining defendant’s motion for summary judgment and ordering final judgment*, 510 F.Supp. 2d 441 (S.D. Ohio 2007); Blackman v. Department of Justice, No. 00-3004 (D.D.C. Oct. 9, 2001) (agency’s search for deposition transcripts of one expert witness using “pay records” index was adequate; manual search that would involve 3,000 aviation cases and as many as 37 million pages would be “overly burdensome”), *summary affirmance denied*, No. 01- 5431 (D.C. Cir. Mar. 29, 2002) (*per curiam*)); Dayton Newspapers, Inc. v. Department of the Air Force, 35 F.Supp. 2d 1033 (S.D. Ohio 1998) (holding that 51 hours of electronic searching and assembly is “small price to pay”).

4. Agency must **segregate and release** nonexempt information. Trans-Pacific Policing Agreement v. United States Customs Serv., 177 F.3d 1022 (D.C. Cir. 1999) (remanded for determination if 10 digit shipping code number could be segregated); Dynalectron Corp. v. Department of the Air Force, 1984 WL 3289 (D.D.C. Oct. 30, 1984). In accordance with the OPEN Government Act of 2007, the requester must be informed of the amount of redacted exempt material withheld and the specific exemption relied upon to withhold the information. See also DOD Reg. 5400.7-R, para. C5.2.4.

5. IAW the 1996 EFOIA amendments, the agency must provide responsive records to the requester in the requester’s selected format, when possible and reasonable. Dayton Newspapers, Inc. v. Department of the Air Force, 35 F. Supp.2d 1033 (S.D. Ohio 1998).

6. Proper agency officials must act upon the request. Records custodians cannot deny a request; only Initial Denial Authority (IDA) may deny requested records. See Enviro Tech Int’l, Inc. v. EPA, 2003 U.S. LEXIS 25493 (N.D. Ill. Mar. 11, 2003) (EPA failed to comply with its regulations when a staff person, rather than a division director, signed EPA's denial of plaintiff's FOIA request) *aff’d* 371 F.3d 370 (7th Cir. 2004).

7. Agency must document any reasons for not releasing a record. DOD Reg. 5400.7-R, para. C5.2.2. The reasons may include:

- a. No responsive records after a “reasonable” search. Gaines v. EEOC, 36 F.App’x 640 (9th Cir. 2002) (“no records” response appropriate where agency had no responsive records).
- b. Agency neither controls nor otherwise possesses record.
- c. Insufficient description of record.
- d. Failure to comply with agency's procedural requirements.
- e. Request is withdrawn.
- f. Fee dispute.
- g. Duplicate Request.
- h. The information is not, by definition, a “record.” Oglesby v. U.S. Department of the Army, 920 F.2d 57 (D.C. Cir. 1990).
- i. The request is denied in whole or part IAW with FOIA.

C. Requirement to Meet Statutory Time Limits. 5 U.S.C. §§ 552(a)(6)(A) & (B).

1. Initial agency response - 20 working days.

- a. Agencies have 20 days (excepting Saturdays, Sundays, and legal public holidays) after receipt of a request to comply with or deny the request.
- b. In “unusual circumstances,” (i.e., voluminous amount of records, consultation with another agency, or retrieval of records from archival storage,) an agency may have an additional ten (10) day extension if the agency tells the requester in writing why it needs the extension and when it will make a determination on the request.
- c. Agency’s 20 day period to respond to a request commences on the date on which the request is first received by the “appropriate component of the agency, but in any event not later than ten days after the request is received by any component of the agency” designated by the agency to receive requests.
- d. Agency is allowed to make one request to the requester for information and toll the 20-day period while it awaits the information. Also, agency may toll the 20- day period as often as necessary to clarify with the requester an issue regarding fees. Either tolling period ends upon receipt of the information or clarification sought.
- e. Requester dissatisfied with agency response - shall be advised to file an

appeal so that it reaches the agency appellate authority no later than 60 calendar days from the date of receipt of the agency response. DOD Reg. 5400.7-R, para. C5.3.3.1.

f. Failure to process timely; fee waiver; ruling that where agency did not act on request by plaintiff (an “all other requester” category requester) for fee waiver, nor act on his administrative appeal, within 20 working days, it could not charge search fees; when requester responded to agency’s letter seeking more information concerning the fee waiver, that stopped the tolling of the 20-day period. Bensman v. Nat’l Park Serv., No. 10-1910, 2011 WL 3489507 (D.D.C. Aug. 10, 2011).

g. If agency shows failure to meet time limits was result of “exceptional circumstances” and it is applying due diligence in processing request, then court can allow additional time for administrative processing of request. §552(a)(6)(C). Open America v. Watergate Special Prosecution Force, 547 F.2d 605 (D.C. Cir. 1976).

h. “Exceptional circumstances” does not include delays that result from a predictable agency workload of requests unless “the agency demonstrates reasonable progress in reducing its backlog of pending requests.” 5 U.S.C. § 552(a)(6)(C)(ii).

2. Agency response to Appeals - 20 working days.

3. Denial and “constructive denial” of requests.

a. Custodian cannot deny a request. See Enviro Tech Int’l, Inc. v. EPA, No. 02 C4650 (N.D. Ill. Mar. 11, 2003) (EPA failed to comply with its regulations when a staff person, rather than a division director, signed EPA’s denial of plaintiff’s FOIA request).

b. Records withheld by custodians must be forwarded to the Initial Denial Authority (IDA) for decision on denials.

c. An agency’s failure to comply with the time limits for either the initial request or the administrative appeal may be treated as a “constructive exhaustion” of administrative remedies, and a requester may immediately seek judicial review. § 552(a)(6). See, Spannaus v. United States Department of Justice, 824 F. 2d 52 (D.C. Cir. 1987).

D. Documenting Agency Action on Requests.

1. Congress requires an annual FOIA processing report to be compiled by each agency. 5 U.S.C. § 552(e)(1). The OPEN Government Act of 2007 added additional requirements that must be reported beginning in 2008. Generally, reporting requirements include: the number of requests for records pending at end of the fiscal year; the average and median number of days that such requests had been pending; the number of requests for records received by the

agency; the number of requests that the agency processed; the average and median number of days taken by the agency to process different types of requests; the number of determinations made by the agency not to comply with requests for records made to the agency, and the reasons for each such determination, etc.

2. DoD components capture data related to FOIA processing on DD Form 2086, Record of Freedom of Information (FOI) Processing Cost (May 2002). In 2008, the Army implemented the Freedom of Information and Privacy Acts Case Tracking System (FACTS). FACTS is a web-based program designed to provide uniform data collection, reporting, and tracking of Army FOIA requests. Its use is mandatory by Army organizations.

3. Each agency is required to make its annual report available on its web site and the Department of Justice is required to link all such reports at one site.

E. Calculating Fees & Processing Fee Waiver Requests. DOD Reg. 5400.7-R, ch. 6.

1. Agencies can require requesters to defray certain costs of agency response.

a. The 1966 FOIA permitted agencies to charge fees for services.

b. The 1974 amendments permitted collection of fees for direct expenses only (i.e., duplication and search).

c. In 1986, Congress distinguished between various classes of requesters and established separate fee categories.

d. The OPEN Government Act of 2007 prohibits agencies from collecting search and duplication fees if the agency fails to comply with any time limit, unless an unusual or exceptional circumstance applies to the processing of the request.

2. FOIA Processing Fees. Charges are based on requester's status and purpose. There are three categories of requesters:

a. First - Most favored category: (1) educational, (2) noncommercial scientific institutions (whose purpose is scholarly or scientific research), and (2) representatives of the news media are charged only for duplication costs after the first 100 pages. See Elec. Privacy Info. Ctr. v. DOD, 241 F.Supp. 2d 5 (D.D.C. 2003) (plaintiff, a nonprofit, tax-exempt, educational organization, is a "representative of the news media" for purposes of the FOIA; the determinative question is the organization's "activities," not its corporate structure; plaintiff publishes a biweekly electronic newsletter and has compiled and published 7 books relating to privacy and civil rights; merely maintaining a Web site, by itself, is insufficient to qualify a FOIA requester as a representative of the news media); National Security Archive v. Department of Defense, 880 F.2d 1381 (D.C. Cir. 1989); Stanley v. Department of Defense, et al. No. 98-

CV-4117 (S.D. Ill. June 22, 1999).

b. Second - Least favored category: requesters of records for commercial use are charged for search, duplication, and review.

c. Third category: All other requesters are charged for search after the first 2 hours and duplication after the first 100 pages.

3. DOD FOIA Fee Rates. Effective 1 July 2002. 32 CFR Part 286; Federal Register, Vol. 67, No. 90, p. 31127 (May 9, 2002).

a. DOD Search and review costs.

(1) Rate for clerical work (E1–E9/GS1–GS8): \$20.00 per hour.

(2) Rate for professional work (O1–O6/GS9–GS15): \$44.00 per hour.

(3) Rate for executive review (ES1–ES6/O7–O10): \$75.00 per hour.

(4) Rate for contractor work: \$40.00 per hour.

b. Duplication costs. Flat rate for office copy reproduction is \$.15 per page. Flat rate for microfiche reproduction is \$.25 per page.

4. Fee limitations.

a. "\$15.00 Rule." No fee is charged if costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee. When assessable costs for a FOIA request total \$15.00 or less, no fee will be charged regardless of the requesters' category. DOD Reg. 5400.7-R, para. C6.1.4.2.

b. "\$250.00 Rule." When the agency estimates or determines that allowable charges are likely to exceed \$250.00, notify the requester and obtain satisfactory assurance of full payment, or for advance payment of up to full amount in the case of requester with no history of payment. DOD Reg. 5400.7-R, para. C6.1.5.2.6.

c. An agency may properly refuse to process FOIA requests if the requester does not pay previous FOIA fees. TPS, Inc. v. Department of the Air Force, 2003 U.S. LEXIS 10925 (N.D. Cal. Mar. 28, 2003) (Navy properly refused to produce requested records based upon requester's outstanding bill of \$300 for a 1995 search conducted for plaintiff).

5. Requests for Fee Waiver. Unlike the substantive FOIA analysis, waivers may be based on the requester's status and motive. See Schulz v. Hughes, 250 F.Supp. 2d 470 (E.D. Pa. 2003) (plaintiff not entitled to a waiver of fees;

the release of information concerning plaintiff's prosecution would not make a significant contribution to the public understanding of federal prosecutions or incarceration); McClellan Ecological Seepage Situation v. Carlucci, 835 F.2d 1282 (9th Cir. 1987) (applying and implicitly approving DOD's regulatory implementation of fee waiver provision).

F. Litigating Denied and Constructively Denied FOIA Requests.

1. Requester must exhaust administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

a. Once an agency has responded to a request, regardless of whether the response is timely, the requester can seek judicial review only after appealing to the agency first. See Ford v. U.S. Department of Justice, No. 02-7538 (4th Cir. Feb. 5, 2003) (*per curiam*) (affirms district court ruling that plaintiff has not exhausted his administrative remedies where the FBI did not timely respond to his FOIA request but responded before suit was filed, and where the agency denied as untimely plaintiff's appeal of the initial denial because he sent it nearly 10 years after the adverse decision); Hogan v. Huff, 2002 U.S. Dist. LEXIS 11092 (S.D.N.Y. June 21, 2002) (plaintiff failed to take legal action before the arrival of the first set of responsive records); Judicial Watch v. F.B.I., 190 F.Supp. 2d 29 (D.D.C. 2002).

b. A requester's failure to pay FOIA fees constitutes a failure to exhaust administrative remedies. See, Oglesby v. Department of the Army, 920 F.2d 57, 66 (D.C. Cir. 1990) (exhaustion does not occur until the required fees are paid or an appeal is taken from the refusal to waive fees).

c. Case is not ripe for adjudication when withholding of records was based upon requester's failure to pay fees associated with a FOIA request. Pietrangelo v. U.S. Department of the Army, 155 F.App'x 526 (2d Cir. 2005) (affirming dismissal for failure to exhaust, despite agency's untimely response, because plaintiff neither paid nor requested waiver of assessed fees).

2. The circumstances which would authorize a judicial stay were narrowed by E-FOIA amendments. Open America v. Watergate Special Prosecution Force, 547 F.2d 605 (D.C. Cir. 1976). Stays are granted for delays resulting from predictable agency workload of requests only if the agency "demonstrates reasonable progress in reducing its backlog of pending requests."

3. Judicial Review. 5 U.S.C. § 552(a)(4)(B); DOD Reg. 5400.7-R, para. C5.4.

a. Civil action challenging the denial of a request may only be brought by the person who filed the FOIA request. Three Forks Ranch Corp. v. Bureau of Land Mgmt, 358 F.Supp. 2d 1 (D.D.C. 2005) (holding that "a FOIA request made by an attorney must clearly indicate that it is being made 'on behalf of' the corporation to give that corporation standing to bring a FOIA challenge.")

b. Agency, not agency employee, is the proper party defendant. Petrus v. Bowen, 833 F.2d 581 (5th Cir. 1987) (“Neither the Freedom of Information Act nor the Privacy Act creates a cause of action against an individual employee of the agency.”)

c. Scope of review - *de novo*.

d. *In camera* inspection is “within the broad discretion of the court.” Quinon v. FBI, 86 F.3d 1222 (D.C. Cir. 1996).

e. Discovery is not typically part of a FOIA lawsuit. Heily v. U.S. Department of Commerce, 69 F.App’x 171 (4th Cir. 2003) (“It is well-established that discovery may be greatly restricted in FOIA cases.”)

(1) The decision to permit discovery in FOIA cases rests with the district court judge. Wood v. FBI, 432 F.3d 78 (2d Cir. 2005).

(2) When discovery is permitted it is to be sparingly granted. Most often, discovery is limited to investigating the scope of the agency search for responsive documents, the agency’s indexing procedures, and similar issues. Schiller v. INS, 205 F. Supp. 2d 648 (W.D. Tex. 2002).

(3) Note: Though not designed to be a federal “discovery tool,” the FOIA is frequently used as such by litigants in non-FOIA cases. See Pa. Department of Pub. Welfare v. United States, 2006 U.S. Dist. LEXIS 92807 (W.D. Pa. Dec. 21, 2006) (rejecting agency’s argument that simply because the requester has another non-FOIA lawsuit against the agency, its FOIA request is “abusing or misusing FOIA to obtain non-discoverable documents”).

(a) Discovery, particularly when a protective order is granted, generally provides greater access to all relevant records or records that could lead to relevant evidence than that provided by the FOIA.

(b) The FOIA is not a substitute for discovery in criminal cases. See Boyd v. DEA, 2002 U.S. Dist. LEXIS 27853 (D.D.C. Mar 8, 2002).

f. Vaughn index. A court may order an agency to submit a detailed index of the documents it seeks to withhold and the reasons justifying such withholding. Vaughn v. Rosen, 484 F.2d 820 (D.C. Cir. 1973); Compare, Wiener v. FBI, 943 F.2d 972 (9th Cir. 1991) with Maynard v. CIA, 986 F.2d 547 (1st Cir. 1993).

(1) The Vaughn index requires a correlation of the information that an agency decides to withhold with the particular FOIA exemption and the agency’s justification for withholding. The index includes a general description of each document sought by the FOIA requester and explains the agency’s justification for nondisclosure of each individual

document or portion of a document.

(2) The index compels the agency to scrutinize any material withheld in justification of its claimed exemption, assists the court in performing its duties, and gives the requester as much information as is legally permissible.

g. Burden of proof. Burden is on the government to establish that a document is exempt from disclosure. 5 U.S.C. § 552(a)(4)(B).

4. Attorney Fees and Costs. § 552(a)(4)(E).

a. Attorney fees are within the discretion of the court when a FOIA plaintiff “substantially prevails.” State of Texas v. Interstate Commerce Commission, 935 F.2d 728 (5th Cir. 1991); Education/Instruction, Inc. v. HUD, 649 F.2d 4 (1st Cir. 1981).

(1) Before 2002, the courts determined whether a plaintiff “substantially prevailed” by determining whether prosecution of the action was needed and that action had a causative effect on delivery of information (i.e., the “catalyst theory”). Weisberg v. Department of Justice, 848 F.2d 1265 (D.C. Cir. 1988).

(2) After 2002, the courts required that “in order for plaintiffs in FOIA to become eligible for an award of attorney’s fees, they must have been awarded some relief either in a judgment on the merits or in a court-ordered consent decree.” Oil, Chemical & Atomic Workers Int’l Union v. Department of Energy, 288 F.3d 452 (D.C. Cir. 2002).

(3) However, the OPEN Government Act of 2007 defines “substantially prevailed” as the obtaining of relief through a judicial order, or an enforceable written agreement, or by a voluntary or unilateral change in position by the agency, if the complainant’s claim is not insubstantial. This is a return to the “catalyst theory” of substantially prevailed as described in Weisberg.

(4) The OPEN Government Act of 2007 requires that all fees assessed in FOIA litigation must now be paid by the agency from its annual appropriations rather than from the Claims and Judgment Fund of the United States Treasury.

b. No attorney fees for *pro se* litigants, Burka v. HHS, 87 F.3d 508 (D.C. Cir. 1996), although a law firm representing itself is eligible to claim attorney fees. Baker & Hostetler LLP v. U.S. Department of Commerce, 473 F.3d 312 (D.C.Civ. 2006).

c. Four factors that courts will generally consider to determine whether an award of fees and costs is appropriate under FOIA after determining the requester’s eligibility:

- (1) Benefit to the public derived from the case;
- (2) Commercial benefit to the requester;
- (3) Nature of requester's interest in the records sought; and
- (4) Whether the agency's withholding of records had a reasonable basis in law. See Church of Scientology v. USPS, 700 F.2d 486 (9th Cir. 1983); LaSalle Extension University v. FTC, 627 F.2d 481 (D.C. Cir. 1980).

d. Commercial requesters and those requesters seeking information for commercial gain should be allowed attorney fees only where there is clear and positive benefit to the public and where the agency withheld information without a reasonable basis in law. Tax Analyst v. U.S. Department of Justice, 965 F.2d 1092 (D.C. Cir. 1992); cf. Aviation Data Service v. FAA, 687 F.2d 1319 (10th Cir. 1982).

5. Six year statute of limitations for filing FOIA lawsuits. 28 U.S.C. § 2401; Spannus v. DOJ, 824 F.2d 52 (D.C. Cir. 1987).

VI. NINE EXEMPTIONS PERMIT WITHHOLDING.

A. Exemption 1: Classified Records. This exemption protects matters that are "(A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order."

1. Threshold: To qualify for withholding under Exemption 1, a record must be substantively and procedurally **properly** classified.
2. Classifications are governed by Executive Order. On 29 December 2009, President Obama signed **Executive Order 13526**. This represents the current US Presidential executive order outlining how [classified information](#) should be handled. Effective 29 December 2009, this order revokes and replaces the previous Executive Orders in effect for this, which were [EO 12958](#) and [EO 13292](#). The EO is implemented by DOD 5200.1- R, AR 380-5; AFR 205-1, and OPNAVINST 5510.1.

a. There are three security classifications: Confidential, Secret, Top Secret. Classification is based upon the potential harm which could result from improper release of the protected documents, information, or materials.

b. For Official Use Only (FOUO). For FOUO information, see Appendix 3 to DoD 5200.1 -R. While not a proper classification under EO 13526, FOUO information may qualify for withholding under another FOIA

exemption.

c. "Controlled Unclassified Information" is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13526, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. President's Memorandum to the Heads of Executive Departments and Agencies, subject: Designation and Sharing of Controlled Unclassified Information (CUI), 44 WEEKLY COMP. PRES. DOC. 673 (May 7, 2008). This categorical designation, with accompanying document markings, is currently being implemented Government-wide and will replace markings currently used for sensitive but unclassified information within DoD (e.g., FOUO, FOUO-LES, LIMITED DISTRIBUTION). Memorandum from David M. Wennegren, DoD Deputy Chief Info. Officer, to Secretaries of the Military Departments, subject: Transition to New Markings for Controlled Unclassified Information (CUI) (Dec. 28, 2007).

3. Segregability applies even in Exemption 1 cases. Ogelsby v. Department of the Army, 79 F.3d 1172 (D.C. Cir. 1996); Oglesby v. Department of the Army, 920 F.2d 57 (D.C. Cir. 1990). [In 1974, following the Court's decision in EPA v. Mink, 410 U.S. 73 (1973), Congress amended the FOIA to require the segregation of nonexempt material in Exemption 1 cases and to permit *in camera* inspections.]

4. Proper classification of records does not obviate the introduction of classified information in litigation.

a. Court conducts *de novo* review of both procedural and substantive propriety of classification. Allen v. CIA, 636 F.2d 1287 (D.C. Cir. 1980).

b. Court may conduct *in camera* inspection, although the court should give substantial weight to agency affidavits. Young v. CIA, 972 F.2d 536 (4th Cir. 1993).

c. Courts will give great deference to agency's expertise and judgment on classification. James Madison Project v. National Archives and Records Administration, 2002 U.S. App. LEXIS 11184 (D.D.C. Mar 5, 2002) (deferring to CIA decision to retain classification of 80-year old records relating to invisible inks), aff'd 2002 U.S. App. LEXIS 21427 (D.C. Cir. Oct. 11, 2002); Weatherhead v. United States, 157 F.3d 735 (9th Cir. 1998), *cert. granted*, 120 S. Ct. 34 (1999), *cert. dismissed and vacated*, 120 S.Ct. 577 (1999) (Court dismisses for mootness, but vacates 9th Circuit's holding that classification decisions are not given deference unless agency first makes acceptable showing of harm); Goldberg v. Department of State, 818 F.2d 71 (D.C. Cir. 1987); Taylor v. Department of the Army, 684 F.2d 99

(D.C. Cir. 1982). See also Ctr. for Nat'l Sec. Studies v. United States Department of Justice, 331 F.3d 918 (D.C. Cir. 2003) (in this post 9/11 case, court declares that it could not “conceive of any reason to limit deference to the executive in its area of expertise to certain FOIA exemptions [i.e., Exemptions 1 and 3] so long as the government's declarations raise legitimate concerns that disclosure would impair national security.”); Am. Civil Liberties Union v. Department of Justice, No. 02-2077, 2003 U.S. Dist. LEXIS 8363 (D.D.C. May 19, 2003) (disclosure of statistical information regarding the Justice Department's use of surveillance and investigatory tools authorized by the USA PATRIOT Act would reveal intelligence activities, sources, or methods and could be expected to damage national security).

5. Operational Security.

a. Post-request classification is authorized. E.O. 13526, section 1.7(d), DOD Reg. 5400.7-R, para. C3.2.1.1.

b. Compilation/Mosaic Theories of classification. The government may withhold apparently harmless bits and pieces of seemingly innocuous information, which when assembled together would reveal classified or exempt information. American Friends Serv. Comm. v DOD, 831 F.2d 441 (3d Cir. 1987); Taylor v. Department of the Army, 684 F.2d 99 (D.C. Cir. 1982); Halperin v. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980). Use of the mosaic theory is not limited to Exemption 1 situations.

c. Previous Release of Classified Records Does Not Prevent Subsequent Withholding of Similar Type of Information. Aftergood v. CIA, 1999 U.S. Dist. LEXIS 18135 (D.D.C. Nov. 15, 1999) (CIA properly withheld its fiscal year 1999 total budget request because it may damage national security and reveal “intelligence sources and methods” even though it released the previous two years' budgets).

d. In rare cases mere existence of particular records may be classified. Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir. 1976) (request for procurement records concerning Glomar Explorer submarine-retrieval ship; consequently “neither confirm nor deny” response known as “Glomar” response or “Glomarization”).

(1) Glomar Denials or Glomarization is the agency's refusal to confirm or deny the existence or nonexistence of requested information or an abstract fact in cases where the sensitive fact or sensitive information would be disclosed by any other response to a particular FOIA request. See Kelly v. CIA, No. 00-2498 (D.D.C. Aug. 8, 2002) (CIA properly refused to confirm or deny the existence of any records reflecting a covert relationship between the CIA and UCLA because disclosure of whether such records (and activity) exist in relation to any particular academic institution would reveal intelligence sources and methods and

would damage national security; exemption protection is not waived by 2 agency memoranda that are general discussions of the CIA's overt and covert relationships with academic institutions in general that have nothing to do with the any specific relationship with UCLA).

(2) Use of Glomar denial not limited to Exemption 1 cases. See DOD Reg. 5400.7-R, para. C3.2.1.1.1., C3.2.1.6.6., and C3.2.1.7.1.3.1; FOIA Update Vol.VII, No. 1 (1986).

B. Exemption 2: Internal Personnel Rules and Practices. This exemption authorizes withholding an agency's internal rules and regulations governing matters pertaining to personnel or human resources.

1. Threshold: The record must be related "solely to internal personnel rules and practices of an agency."

2. Until March of 2011, Exemption 2 was generally interpreted by courts to include two different bases for withholding records from release. These differing bases for withholding were commonly known as "Low 2" and "High 2." The Supreme Court decision in *Milner v. Dep't of the Navy*, 131 S. Ct. 1259 (March 7, 2011) The opinion essentially did away with "High 2" by narrowing the exemption to the "Low 2" version of the exemption.

a. The Court found the common understanding of the term "personnel rules and practices" when applied by other courts has resulted in little difficulty in determining what qualifies as one of those records. These records "share a critical feature: They concern the conditions of employment in federal agencies—such matters as hiring and firing, work rules and discipline, compensation and benefits." *Id.* at 1265. The court declared that its "construction of the statutory language simply makes clear that Low 2 is all of 2 (and that High 2 is not 2 at all...)." *Id.*

b. "Exemption 2, consistent with the plain meaning of the term 'personnel rules and practices,' encompasses only records pertaining to issues of employee relations and human resources." *Milner*, at 1271.

c. A New Three-Part Test: (1) The information must be related to "Personnel" Rules and Practices; *Id.* at 1265 (2) the information must "solely" relate to those personnel rules and policies; and (3) the information must be "internal" to the agency for their records and use. See *id.* at 1265 n.4.

3. Because of the of the *Milner* decision, it may be helpful to understand the distinction that used to be drawn between "Low 2" and "High 2."

a. The Court of Appeals for the District Court of Columbia Circuit was the leading case interpreting Exemption 2. In *Crooker v. ATF*, 670 F.2d 1051 (1981) the court interpreted the statutory language to create a two-part test for determining the meaning and application of Exemption 2. For records to

qualify, first they had to be “predominantly internal,” and secondly they had to be of no genuine public interest (Low 2) or of a nature that would risk circumvention of the law (High 2). See *id.* at 1073-74.

b. “Low 2” applied to trivial matters and information in which there is little or no public interest. Even this interpretation of the exemption has been narrowed by *Milner* to clarify that it applies only to internal personnel rules and practices.

c. “High 2” provided authority to withhold information which would provide a requester with the means to circumvent an agency regulation or frustrate an agency function or mission. Examples of withholding under High 2: information concerning the design, array, structure, and construction of ammunition storage facilities; unclassified rules of engagement even though the enemy may be aware of the ROE through experiences with U.S. forces in Iraq; blueprint of agency buildings where contents or infrastructure could be harmed by public disclosure.

C. Exemption 3: Other Federal Withholding Statutes. FOIA Exemption 3 permits withholding of information prohibited from disclosure by another statute. A complete listing of current statutes that have been found as qualifying Exemption 3 statutes is available at: <http://www.justice.gov/oip/exemption3.pdf>.

1. Threshold: One of two disjunctive requirements must be met to withhold under this exemption: the withholding statute must either “(A) [require] that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establish particular criteria for withholding or refer to particular types of matters to be withheld.” A statute falls within the exemption's coverage if it satisfies either one of its disjunctive requirements.

2. Examples of federal withholding statutes:

a. The Homeland Security Act of 2002, Public Law 107-296, includes a provision that operates as an Exemption 3 statute for “critical infrastructure” information that is obtained by DHS.

b. 42 U.S.C. § 290dd-3, Confidentiality of patient records in an alcohol and drug treatment program.

c. 10 U.S.C. § 1102, DOD Medical Quality Assurance Records.

d. 10 U.S.C. § 2305 and 41 U.S.C. § 253b, prohibiting release of certain contractual proposals.

e. 10 U.S.C. §130b, allows withholding of information on personnel of overseas, sensitive, or routinely deployable units. See Windel v. United States, 2005 U.S. Dist. LEXIS 44422 (D. Alaska Apr. 11, 2005), (applying protection to members of a routinely deployable unit of the Air National Guard). Pursuant to DoD guidance issued on 9 November 2001, all DOD components shall ordinarily withhold *lists* of names and other personally identifying information of currently or recently assigned personnel (citing privacy and security concerns). Names, other than lists, mentioned in other documents may be withheld if the release would raise substantial security or privacy concerns (utilize Exemption 6).

f. 10 U.S.C. §130e, allows withholding of information that is determined to be Department of Defense critical infrastructure security information and the public interest consideration in the disclosure does not outweigh preventing the disclosure of the information. Department of Defense critical infrastructure security information means sensitive but unclassified information that, if disclosed, would reveal vulnerabilities, result in significant disruption, destruction or damage of or to DoD operations, property or facilities. These facilities are those owned by or operated on behalf of the DoD. [This responds directly to the issues in *Milner*.]

g. See annual DoD FOIA Report for complete listing of Exemption 3 statutes relied upon by DoD during the reporting period.

3. Statutes **commonly mistaken** for Exemption 3 withholding statutes:

a. 18 U.S.C. § 1905; The Trade Secrets Act does not qualify because it prohibits only those disclosures “not authorized by law.” CNA Fin. Corp. v. Donovan, 830 F.2d 1132 (D.C. Cir. 1987).

b. 5 U.S.C. § 552a; The Privacy Act.

c. 41 U.S.C. § 423(a)(1); The Procurement Integrity Act does not qualify because it prohibits only those disclosures “other than as provided by law” and “does not . . . limit the applicability of any . . . remedies established under any other law or regulation.” Cf. Pikes Peak Family Housing, LLC v. United States, 40 Fed.Cl. 673 (1998) (provision does not prohibit disclosure in civil discovery because that is “provided by law”). *But see* Legal & Safety Employer Research, Inc. v. Department of the Army, 2001 U.S. Dist. LEXIS 26278 (E.D. Cal. May 7, 2001) (erroneously holding that the provision qualifies as an Exemption 3 statute).

4. Statutes may have retroactive application. See Sw. Ctr. for Biological Diversity v. USDA, 314 F.3d 1060 (9th Cir. 2002) (the court properly applied a recently enacted Exemption 3 statute in existence at the time of its decision [16 U.S.C. § 5937], rather than the law that was in existence at the time the

suit was filed; statute protects information identifying the location of northern goshawk nest sites).

5. Carefully worded appropriations acts may qualify under Exemption 3. See City of Chicago v. U.S. Department of Treasury, 423 F.3d 777 (7th Cir. 2005) (ruling that appropriation act prohibition on the use of federal funds “to disclose to the public” certain ATF database records “prevents the agency...from acting on a request for disclosure “and that the act’s provisions making such data “immune from legal process” prevents a court from utilizing a plaintiff-compensated special master to process such data).

D. Exemption 4: Trade Secrets, and Commercial and Financial Records. This exception balances and safeguards the interests of both the federal government and entities that submit commercial and financial information to the government.

1. Statutory language. The FOIA permits withholding records that are “trade secrets and commercial or financial information obtained from a person that are privileged or confidential.”

2. Trade Secrets. There is a difference between the Trade Secrets Act and the FOIA’s exemption for trade secrets.

a. For purposes of the FOIA, “Trade Secrets” has a narrow definition.

(1) “[A] secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort.” Public Citizen Health Research Group v. FDA, 704 F.2d 1280 (D.C. Cir. 1983).

(2) The passage of time may not make trade secrets any less secret. Herrick v. Garvey, 298 F.3d 1184 (10th Cir. 2002) (upholding district court ruling that technical drawings and specification documents for 1935 airplane still retain commercial value and are protected by Exemption 4).

b. The Trade Secrets Act, 18 U.S.C. § 1905, defines secrets far more loosely. This act criminalizes the unauthorized disclosure of any data protected by Exemption 4. CNA Financial Corp. v. Donovan, 830 F.2d 1132 (D.C. Cir. 1987).

(1) Trade Secrets Act applies broadly to virtually all business information and prohibits agency disclosure except as “authorized by law.”

(2) FOIA provides such “authority” to disclose business information only if it is nonexempt. CNA Fin. Corp., *supra*.

3. Commercial or financial information. Courts generally give these terms their “ordinary meanings” and reject more limiting definitions. See Public Citizen

Health Research Group v. Food and Drug Administration, 704 F.2d 1280 (D.C. Cir 1983); see also Baker & Hostetler LLP v. U.S. Department of Commerce, 473 F.3d 312 (D.C. Cir. 2006) (information about lumber industry’s “commercial strengths and challenges” even though they do not “reveal basic commercial operations...or relate to the income producing aspects of a business”).

4. From a person. Person is defined as any individual or entity other than the Federal Government or one of its activities. Nadler v. FDIC, 92 F.3d 93 (2d Cir. 1996) (person includes individuals, partnerships, corporations, associations or public and private organizations other than an agency); Stone v. Export-Import Bank of United States, 552 F.2d 132 (5th Cir. 1977) (foreign government agency).

5. Privileged. Generally related to common law privileges, but rarely used as a basis for withholding. Sharyland Water Supply Corp. v. Black, 755 F.2d 397 (5th Cir. 1985); Indian Law Resource Center v. Department of the Interior, 477 F. Supp. 144 (D.D.C.1979).

6. Confidential. The government can only withhold information that is confidential. The courts have developed two tests to determine whether information is confidential.

a. The “Confidential” test under National Parks & Conservation Association v. Morton, 498 F.2d 765 (D.C. Cir. 1974). Two main prongs have developed under case law; however, several courts have left open the possibility of a third prong.

(1) The “Impairment Prong.” Would disclosure likely “impair ability of agency to obtain necessary information in the future”? See Flight Safety Servs. Corp. v. Department of Labor, 326 F.3d 607 (5th Cir. 2003) (per curiam) (disclosure of salary and wage information in the form of surveys of business establishments would impair the agency's ability to collect such data in the future); Orion Research Inc. v. EPA, 615 F.2d 551 (1st Cir. 1980) (finding impairment for technical proposals because release “would induce potential buyers to submit proposals that do not include novel ideas”); *but see* McDonnell Douglas Corp. v. NASA, 981 F. Supp. 12 (D.D.C. 1997) (no impairment because “government contracting involves millions of dollars and it is unlikely that release of this information will cause [agency] difficulty in obtaining future bids), *rev'd on other grounds*, 180 F.3d 303 (D.D. Cir. 1999); Racal-Milgo Government Systems v. Small Business Administration, 559 F. Supp. 4 (D.D.C. 1981) (“It is unlikely that companies will stop competing for Government contracts if the prices contracted for are disclosed.”).

OR

(2) The “Competitive Harm” prong. Would disclosure likely cause

“substantial harm to the competitive position of the person from whom the information was obtained”?

(a) For examples of cases finding competitive harm, see McDonnell Douglas Corp. v. NASA, 180 F.3d 303 (D.C. Cir. 1999) (holding that release of unit price in rocket contract substantiates substantial competitive harm allowing customers to “ratchet down” prices); Gulf & Western Industries Inc. v. United States, 615 F.2d 527 (D.C. Cir. 1979) (actual costs, break even calculations, profits and profit rates); National Parks, *supra* (detailed financial information including company assets, liability and net worth); MCI Worldcom, Inc. v. GSA, 163 F. Supp. 2d 28 (D.D.C. 2001) (“Reverse FOIA”; protecting computer-based matrices used to calculate telecommunications services; finding that disclosure would cause competitive harm due competitors underbidding and customers “ratcheting down” their prices); RMS Industries v. Department of Defense, 1993 U.S. Dist. LEXIS 10995 (N.D. Cal. Nov. 24, 1992) (technical and commercial data, names of consultants and subcontractors, performance cost and equipment information).

(b) For examples of cases finding no competitive harm, see GC Micro Corporation v. Defense Logistics Agency, 33 F.3d 1109 (9th Cir. 1994) (“percentage and dollar amount of work contracted out to SDB [Small Disadvantaged Businesses] on each defense contract” is “made up of too many fluctuating variables”); Pacific Architects & Engineers v. Department of State, 906 F.2d 1345 (9th Cir. 1990) (reverse FOIA case) (unit prices); Hercules, Inc. v. Marsh, 839 F.2d 1027 (4th Cir. 1988) (holding no competition for Radford Army Ammunition Plant contract).

(3) [OR, thirdly, will disclosure negatively impact other government interests, such as compliance and program effectiveness? In National Parks, court hinted at this third “prong” but left the issue unresolved. In Critical Mass Energy Project v. National Regulatory Commission, 975 F.2d 871 (D.C. Cir. 1992), the court accepted a third basis for designating information confidential.]

(4) Unit prices are not [generally] confidential. See, e.g., Pacific Architects & Eng’rs, Inc. v. Department of State, 906 F.2d 1345 (9th Cir. 1990); Acumenics Research & Technology v. Department of Justice, 848 F.2d 800 (4th Cir. 1988). The disclosure of government contract unit prices is a contentious issue.

(a) Government policy formerly required “submitter notice” in response to requests for contract unit prices, IAW Executive Order 12,600. 52 Fed. Reg. 23,781 (Jul. 23, 1987); see *also* 3 C.F.R. 235 (1988) *reprinted in* 5 U.S.C. § 552 note (1994). Submitters would then file “reverse FOIA” lawsuits to prevent the disclosure of unit prices as confidential commercial or financial information.

(b) In 1997, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council announced the change to Part 15 of the Federal Acquisition Regulation. FAR, 48 C.F.R. §§ 15.503(b)(iv), 15.506(d)(2), required disclosure of unit prices, upon request, in government contracts solicited after 1 January 1998. As a result, government policy no longer required submitter notice under EO 12,600.

(c) Despite the best efforts of the Department of Justice and DoD, several courts have held that unit prices may be withheld under the FOIA. See Canadian Commer. Corp. v. Department of the Air Force, 514 F.3d 37 (D.C. Cir. 2008) (finding that line item pricing information involved in the option years of a maintenance contract must be protected); McDonnell Douglas Corp. v. Department of the Air Force, 375 F.3d 1182 (D.C. Cir. 2004) (finds that company has shown that disclosure of option prices and vendor pricing and handling factor, but not “over and above” prices, would likely cause substantial harm to its competitive position); McDonnell Douglas Corp. v. NASA, 180 F.3d 303 (D.C. Cir. 1999), *reh’g denied*, No. 98-5251 (D.C. Cir. Oct. 6, 1999) (finding line item price information from contract resulting from pre-1998 contract solicitation to be confidential under National Parks test); MCI Worldcom v. GSA, 163 F. Supp. 2d 28 (D.D.C. 2001) (FAR provisions cannot be read to authorize disclosure of information protected by Exemption 4 because authorizing statute, 41 U.S.C. § 253b(e)(3), prohibits disclosure of exempt info).

(d) Department of Justice policy again requires agencies to follow submitter notice procedures in response to requests for unit prices. On a case-by-case basis, agencies should determine the applicability of Exemption 4 to unit price requests. See U.S. Department of Justice, “Treatment of Unit Prices After McDonnell Douglas v. Air Force,” FOIA Post, <http://www.usdoj.gov/oip/foiapost/2005foiapost17.htm>. The DoD Freedom of Information and Security Review (DFOISR) is expected to issue specific guidance. See also R&W Flammann GmbH v. United States, 339 F.3d 1320 (Fed Cir. 2003) (holding, in a pre-award bid protest case concerning unit prices contained in sealed bids –as distinct from prices contained in proposals – which were subject to the public opening requirement contained in a different FAR provision, that such bid prices “entered the public domain upon bid opening, and therefore...did not fall within Exemption 4 of FOIA”).

(5) Unit prices and other items within an unsuccessful proposal are not releasable. 10 U.S.C. § 2305(g)(2) or 41 U.S.C. § 253b(m)(2).

b. The “Confidential” test under Critical Mass Energy Project v. NRC, 975

F.2d
871 (D.C. Cir. 1992).

(1) The Critical Mass test: Did the submitter voluntarily provide the information to the agency?

(a) Does the agency possess legal authority to require information submission: statute, executive order, regulation, or “less formal mandate”?

(b) Has the agency exercised such authority?

(c) Whether submitter’s participation in agency program was “voluntary” is **not** the test. Contract bids and proposals are considered “required submissions” and therefore releasability is analyzed under the National Parks analysis. See McDonnell Douglas Corp. v. NASA, 981 F. Supp 12 (D.D.C. 1997) (information provided in response to a Request for Proposals is a required submission); N.Y. Pub. Interest Research Group v. EPA, 249 F.Supp. 2d 327 (S.D.N.Y. 2003) (FOIA does not protect GE's submissions to EPA constituting recommendations as to how to clean up the Hudson River Superfund site; the submissions do not reveal anything about GE as a commercial entity; submitted records “are precisely the kind of information that would shed light on agency decision-making”; in *dicta*, declines to apply the D.C. Circuit's *Critical Mass* decision because no other circuit court has expressly adopted it, the Second Circuit has not commented on it); see also DFOISR Memorandum, SUBJECT: FIOA Policy on DOD application of Critical Mass (etc.), 93-CORR-014, 27 July 1993; DFOISR Memorandum, SUBJECT: Internal Guidance on DOD Application of Critical Mass (etc.), 93-CORR-094, 23 March 1993.

AND

(2) Is it information “of a kind that would customarily not be released to the public by the person from whom it was obtained?”

For a sample of the variety of Critical Mass case law in the procurement context, see Frazee v. United States Forest Serv., 97 F.3d 367 (9th Cir. 1996) (“proposed operating plan” submitted in response to solicitation for offers not “voluntarily” submitted under Critical Mass) (*dicta*); McDonnell Douglas Corp. v. NASA, 981 F.Supp 12 (D.D.C. 1997) (contractor line item prices not “voluntarily” submitted under Critical Mass), *reversed on other grounds*, 180 F.3d 303 (D.C. Cir. 1999); Comdisco, Inc. v. GSA, 864 F. Supp. 510 (E.D. Va. 1994) (reverse FOIA) (district court finds Critical Mass inapplicable in 4th Circuit) (*dicta*). See also Mallinckrodt Inc. v. West, 140 F.Supp. 2d 1 (D.D.C. 2000) (observing that “it is beyond dispute that unit pricing data

is required to be submitted,” but finding that rebate and incentive provisions do not constitute pricing data and ruling that they were voluntarily provided under Critical Mass because Blanket Purchase Agreement solicitation stated that they “should,” rather than “must,” be provided); Cortez III Serv. Corp. v. NASA, 921 F. Supp. 8 (D.D.C. 1996) (negotiated G&A rate ceilings, not required in solicitation but merely requested by contracting officer held “voluntarily submitted under Critical Mass), *appeal dismissed voluntarily*, No. 96-5163 (D.C. Cir. July 3, 1996).

7. How does agency determine what is confidential? See EO 12,600 (June 23, 1987) and DOD Reg. 5400.7-R, para. C3.2.1.4.8.

8. Determining whether business information is exempt--notice of proposed release to the submitter of information — “Reverse FOIA”

a. Notify the submitter of the FOIA request and solicit its views as to whether disclosure would cause substantial competitive harm.

b. After reviewing submitter’s comments, if the agency determines to disclose any information, it must advise the submitter of its rationale and inform it of the date it will make the disclosure. See NW. Coal. for Alternatives to Pesticides v. EPA, 254 F.Supp. 2d 125 (D.D.C. 2003) (upbraiding agency where submitter mailed redacted document to requester).

c. The agency rationale must be detailed and respond to each of the submitter’s claims as it will constitute the “administrative record” that will support the agency’s decision to release the requested information. Acumenics Research & Technology v. Department of Justice, 843 F.2d 800 (4th Cir. 1988) (“Reverse FOIA” case). See Federal Electric Corp. v. Carlucci, 866 F.2d 1530 (D.C. Cir. 1989) (agency failed to create an adequate agency administrative record).

d. Businesses that submit documents to the government may file suit under the Administrative Procedures Act (APA) to challenge an agency’s decision to release documents pursuant to a FOIA request. Chrysler Corp. v. Brown, 441 U.S. 281 (1979) (discretionary release permissible only if not protected by Exemption 4, thereby “authorized by law”); Gulf Oil Corp. v. Brock, 778 F.2d 834 (D.C. Cir. 1985).

e. Standard of review of agency action under APA -- review on the administrative record using the arbitrary and capricious standard. Acumenics Research & Technology v. Department of Justice, 843 F.2d 800 (4th Cir. 1988); General Electric Co. v. NRC, 750 F.2d 1394 (7th Cir. 1984).

E. Exemption 5: Privileged Memoranda & Internal Agency Communications. The FOIA permits withholding records that are “inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency.” Exemption 5 is limited to that information which would “routinely” or “normally” not be available to a party in litigation. FTC v. Grolier, 462

U.S. 19 (1983).

1. Threshold: Memoranda or communications must be “inter-agency or intra-agency.”
 - a. “Inter- or intra-agency memorandums” may include communications with parties outside the government. Nat’l Institute of Military Justice v. Department of Defense, 512 F.3d 677 (D.C. Cir. 2008) (cert. denied 08-125 (Dec. 15, 2008)) (2- to-1 decision) (memoranda provided to DoD by outside experts for consideration in establishing regulations for terrorist trial commissions qualify under the D.C. Circuit’s “consultant corollary”).
 - b. Competing or conflicting interests may require disclosure of records of communications with “outside consultant.” See Department of the Interior v. Klamath Water Users Protective Ass’n, 532 U.S. 1 (2001) (“intra-agency condition excludes, at the least, communications to or from an interested party seeking government benefit at the expense of other applicants”).
2. Scope. Exemption 5 incorporates most common law discovery privileges.
 - a. Deliberative Process Privilege. Purpose--to encourage open, frank discussions between subordinates and superiors; protect against premature disclosure of proposed policies before they are adopted; and protect against public confusion that might result from disclosure of reasons and rationales that were not ultimately the grounds for the agency's action. Russell v. Department of the Air Force, 682 F.2d 1045 (D.C. Cir. 1982); Judicial Watch, Inc. v. United States Department of Justice, 102 F.Supp.2d 6 (D.D.C. 2000) (deliberative process privilege protects handwritten notes by the Attorney General which reflect distillations of issues that she memorialized for later reference as part of her decision making process); Bilbrey v. Department of the Air Force, No. 00-0539 (W.D. Mo. Jan, 30, 2001) (protecting advice in two memoranda from wing commander to air force commander concerning nonjudicial punishment for requester charged with two counts of adultery and one of dereliction of duty; factual information in second memoranda used to rebut defense matters raised by requester ordered disclosed; that requester would have received the withheld information had he demanded a court-martial, and that he has a current need for the information, held irrelevant), *aff’d*, 20 Fed. Appx. 597 (8th Cir. 2001).
 - (1) Courts distinguish between “factual” and “deliberative” information. EPA v. Mink, 410 U.S. 73 (1973) (privilege does not generally protect purely factual matters).
 - (a) However, agency may withhold facts if they are “inextricably intertwined” with deliberative material. Ryan v. DOJ, 617 F.2d 781 (D.C. Cir. 1980); Jowett, Inc. v. Department of Navy, 729 F. Supp. 871 (D.D.C. 1989).
 - (b) Agency may also withhold facts if release would disclose the “deliberative process.” Mead Data Central, Inc. v. Department of

the Air Force, 566 F.2d 242 (D.C. Cir. 1977) (holding that “Exemption five is intended to protect the deliberative process of government and not just deliberative material . . . In some circumstances . . . the disclosure of even purely factual material may so expose the deliberative process within an agency that it must be deemed exempted by section 552(b)(5).”)

(c) Deliberative documents and communications do not always have to flow from subordinates to superiors. Nat'l Wildlife Fed'n v. U.S. Forest Serv., 861 F.2d 1114 (9th Cir. 1988).

(2) Courts also distinguish between “predecisional” and “postdecisional” records.

(a) Agency may withhold predecisional documents. NLRB v. Sears, 421 U.S. 132 (1975) (Deliberative process privilege can never apply to a final agency decision, but Exemption 5 incorporates the attorney-work privilege and documents setting strategy for the case); Lurie v. Department of the Army, 970 F. Supp. 19, 28 (D.D.C. 1997).

(b) Agency cannot withhold predecisional materials when final decision- maker “expressly adopts or incorporates them by reference.” NLRB v. Sears, 421 U.S. 132 (1975); Swisher v. Department of the Air Force, 660 F.2d 369 (8th Cir. 1981).

b. Attorney Work-Product Privilege.

(1) Exempts materials “prepared in anticipation of litigation or for trial by or for [a] party or by or for that . . . party’s representative (including the . . . party’s attorney, consultant, . . . or agent).” Fed.R.Civ.P. 26(b)(3); FTC v. Grolier, 462 U.S. 19 (1983); Safecard Services, Inc. v. SEC, 926 F.2d 1197 (D.C. Cir. 1991). See Coleman v. U.S. Department of Justice, No. 02-79-A (E.D. Va. Oct. 7, 2002) (the privilege protects investigatory documents that contain “mental impressions, conclusions, opinions or legal theories” of the attorneys involved).

(2) Courts have recognized that the privilege extends to records prepared in anticipation of litigation even when no specific claim is pending. Schiller v. NLRB, 964 F.2d 1205 (D.C. Cir. 1992) (holding that documents that provide tips on handling future litigation are covered by the work product privilege). See *also* Maine v. Department of the Interior, 298 F.3d 60 (1st Cir. 2002) (amended opinion) (concluding that court’s earlier opinion which required that litigation be primary factor in creation of documents for which attorney work- product privilege was claimed, was in error). *But cf.* Jongeling v. Army Corps of Eng'rs, No. 02-1020 (D.S.D. Jan. 2, 2003) (attorney work-product privilege cannot be claimed as defendant agency has not shown that the records at issue were prepared “in anticipation of litigation” or “because of” the

prospect of litigation; on in camera inspection).

c. Attorney-Client Privilege. The confidential communications from clients to the counsel made for the purpose of securing legal advice or services; and the communications from attorneys to their clients if the communications rest “on confidential information obtained from the client.” In re Sealed Cases, 737 F.2d 94, 98-99 (D.C. Cir. 1984). Mead Data Central, Inc. v. Department of the Air Force, 566 F.2d 242 (D.C. Cir. 1977). See also Citizens Progressive Alliance v. United States Bureau of Indian Affairs, 241 F. Supp. 2d 1342 (D.N.M. 2002) (privileges not waived when DOJ attorney confidentially disclosed documents to the attorney for interveners because the “common interest privilege,” an exception to the inherent confidentiality requirement of the attorney-client privilege or the attorney work-product privilege, allows attorneys facing a common litigation opponent to exchange privileged communications and attorney work-product in order to adequately prepare a defense).

d. Government’s Commercial Information Privilege. Federal Open Market Committee v. Merrill, 443 U.S. 340 (1979) (Exemption 5 incorporates privilege for commercially sensitive documents generated by the government); Morrison- Knudsen Co. v. Department of the Army, 595 F. Supp. 352 (D.D.C. 1984), *aff’d* 762 F.2d 138 (D.C. Cir. 1985) (table cite); Hack v. Department of Energy, 538 F. Supp. 1098 (D.D.C. 1992) (inter-agency cost estimates prepared by government for use in evaluating construction proposals submitted by private contractors).

e. Protection of Certain Confidential Witness Statements. United States v. Weber Aircraft Corp., 465 U.S. 792 (1984) (protecting witness statements given to military personnel in course of military air crash safety investigation); Ahearn v. Department of the Army, 583 F. Supp. 1123 (D. Mass. 1984) (protecting statements made in Inspector General investigations).

f. Presidential Communications Privilege. Loving v. Department of Defense, 550 F.3d 32 (D.C. Cir. 2008) (TJAG’s analysis and recommendation to the Secretary of the Army for transmittal to the president for him to determine whether to approve requester’s death sentence; ruling this privilege, unlike deliberative process privilege, protects facts; holding that privilege’s requirement that the communication must be reviewed by the president or solicited by his immediate advisors is satisfied by the “solicitation” for the TJAG opinion in R.C.M. 1204(c)(2)).

F. Exemption 6: Protection of Personal Privacy. FOIA permits withholding records that are “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;”

1. Threshold: Record must be from a “personnel and medical files and **similar files.**”

a. "Personal and medical files" are normally easy to identify. Includes military members' OMPF, local unit personnel files, and military medical records.

b. What are "similar files?" Department of State v. Washington Post, 456 U.S. 595 (1986) ("similar files" provision extends to any information of a "personal" nature, such as ones citizenship); Perlman v. U.S. Department of Justice, 312 F.3d 100 (2d Cir. 2002) (report of investigation is a "similar file" because it is a "detailed Government record"); New York Times Co. v. NASA, 920 F.2d 1002 (D.C. Cir. 1990) (holding that voice recording of the Challenger astronauts is a "similar file" for purposes of FOIA Exemption 6).

c. Information must identify a specific individual; records which identify a group of individuals do not qualify for Exemption 6 withholding unless the information is attributable to all members of the group. Arieff v. Department of the Navy, 712 F.2d 1462 (D.C. Cir. 1983) (list of drugs used by some within a 600-member group); Na Iwi O Na Kupuna v. Dalton, 894 F. Supp. 1397 (D. Haw. 1995) (records pertaining to large group of ancient human remains subject to FOIA, Congress intended Exemption 6 to only "protect the privacy of living members of contemporary society").

2. The balancing test: whether disclosure "would constitute a clearly unwarranted invasion of privacy." Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989). See also Bibles v. Oregon Natural Desert Association, 519 U.S. 355 (1997).

a. Identifying the privacy interest to be balanced.

(1) The privacy rights of the deceased is a settled issue.

(a) Deceased persons have no privacy rights. National Archives & Records Administration v. Favish, 541 U.S. 197 (2004) (unanimous ruling that death-scene photographs can be withheld from the public, and from media exploitation, "to protect...the personal privacy of family members against the uncontrolled release of information"; See also; Na Iwi O Na Kupuna v. Dalton, *supra*. (Reverse FOIA suit).

(b) Next-of-kin of deceased persons may have, in certain situations, a colorable privacy interest in "time-of-death" records. New York Times Co. v. NASA, 920 F.2d 1002 (D.C. Cir. 1990) (*en banc*) (voice recordings of space shuttle Challenger astronauts; next-of-kin may have, in rare situations, a colorable privacy interest). *But cf.* Outlaw v. Department of the Army, 815 F.Supp. 505 (D.D.C. 1993) (agency unable to determine, in connection with murderer's request for death scene photographs, whether murdered First Sergeant had any surviving next of kin 25 years after his death).

(2) Corporations and business associations do not generally have

protectable privacy interests. See Sims v. CIA, 642 F.2d 562, 572 n.47 (D.C. Cir. 1980). However, persons associated with small businesses, partnerships, and closely held corporations may have protectable interests in their entrepreneurial information. Doe v. Veneman, 230 F.Supp. 2d 739 (W.D. Tex. 2002) (“reverse” FOIA action brought by “incorporated” ranchers who entered into agreements with the government on the use of “anti-wolf livestock protection collar” who seek protection of their own identities, court protects the identities of entrepreneurial entities who have signed the agreements because the agency was making an “overly technical distinction” between individual and business), *aff’d in pertinent part on other grounds*, 380 F.3d 807 (5th Cir. 2004).

(3) “Something, even a modest privacy interest, outweighs nothing every time.” Nat’l Association of Retired Federal Employees v. Horner, 879 F.2d 873 879 (D.C. Cir. 1989).

(4) Associated Press v. DOD (2nd Cir. Jan. 5, 2009) (holding that identifying information of Guantanamo Bay detainees in records documenting allegations of abuse and identifying information of detainees’ family members in letters submitted to the government are exempt from FOIA disclosure under Exemptions 7(C) and 6 respectively).

b. Identifying the public interest in disclosure. The Reporters Committee decision has limited the concept of public interest under the FOIA to the “core purpose” for which Congress enacted it: to “[shed] light on an agency's performance of its statutory duties.” Information that does not directly reveal the operations or activities of the federal

government “falls outside the ambit of the public interest that the FOIA was enacted to serve.” If records are not informative on the operations and activities of the government, there is no public interest in their release. For an example of a court finding a qualifying public interest see Cochran v. United States, 770 F.2d 949 (11th Cir. 1985) (disclosure of nonjudicial findings and discipline imposed on Army major general for misuse of government personnel and facilities held proper) (Privacy Act wrongful disclosure suit).

3. Application of the balancing test.

a. Articulate the privacy interest involved. [Note the “**heightened interest in the personal privacy of DoD personnel**” resulting from terrorist activity likely to weigh heavily in favor or protection. See 9 November 2001, DoD guidance, at Appendix B]; see also Kimmel v DOD, 2006 U.S. Dist. LEXIS 14904 (D.D.C. Mar. 31, 2006) (protecting “names of civilian personnel below the level of office director and military personnel below the rank of colonel” in documents relating to congressional request that the President advance Rear Admiral Kimmel to the rank of Admiral; finding disclosure of those names would not shed light on the operations and activities of DOD;

ruling that the court “has no reason to question” the DOD policy expressing “concern that employees of DOD could become targets of terrorist assaults”). Long v. OPM, No. 05-1522, 2007 U.S. Dist. LEXIS 72887 (N.D.N.Y. Sept. 30, 2007) (An employee’s name and duty station are personal in nature and do not relate to the employee’s performance of public duties. Disclosure of lists of names does not, by itself, shed light on agency activities.)

b. Articulate the public interest involved.

c. Strike the balance.

d. Examples. FLRA v. DOD, 510 U.S. 487 (1994) (a leading case delineating the “core interests” of FOIA; thorough balancing of interests analysis); Department of State v. Ray, 502 U.S. 164 (1991) (privacy interest of Haitian deportees in their names and addresses outweighs any public interest that might be served by disclosure); Judicial Watch, Inc. v. United States, 84 F.App’x 335 (4th Cir. 2004) (protecting the names of lower-level IRS employees because disclosure would not shed light on the activities of the IRS); Sherman v. Department of the Army, 244 F.3d 357 (5th Cir. 2001) (protecting Social Security numbers in post-1968 award orders; though Army in past released some SSNs of service members, such disclosures do not waive privacy interests because only individuals can waive their privacy interests); Sheet Metal Workers Int’l Ass’n. v. United States Air Force, 63 F.3d 994 (10th Cir. 1995) (Sheet Metal Workers union engaged in “Davis-Bacon” monitoring--release of payroll records with names and addresses of workers employed on government contracts constitutes a clearly unwarranted invasion of personal privacy); McCutchen v. HHS, 30 F.3d 183 (D.C. Cir. 1994) (names of persons exonerated by investigation protected from disclosure); Providence Journal Co. v. Department of the Army, 981 F.2d 552 (1st Cir. 1992) (the higher the rank, the greater the public interest might be in release of agency record concerning disciplinary action); Homer J. Olsen, Inc. v. U.S. Department of Transp., 2002 U.S. Dist. LEXIS 23292 (N.D. Cal. Dec. 2, 2002) (disclosure of names of contractor and subcontractor employees “would constitute a clearly unwarranted invasion of personal privacy”); Chin v. Department of the Air Force, No. 97-2176 (W.D. LA June 24, 1999) (privacy outweighed the public interest in withholding of identities in general request for fraternization investigations); Mueller v. Department of the Air Force, 63 F. Supp. 2d 738 (E.D. Va. 1999) (denial of request for dismissed non-judicial punishment proceeding documents because public interest was minimal and would shed little light on Air Force's overall conduct).

4. “Categorical Balancing” and Privacy Glomarization. Agency can refuse to confirm or deny categories of records; however, application must be consistent. See Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989); Beck v. Department of Justice, 997 F.2d 1489 (D.C. Cir. 1993); DOD Reg. 5400.7-R, para. C3.2.1.6.5.1-2.

G. Exemption 7: Law Enforcement Records. Exempts from disclosure any

record or information compiled for law enforcement purposes, the disclosure of which could reasonably be expected to result in any of six specified harms.

1. Threshold. Record must be compiled for a law enforcement purpose.

a. Courts have distinguished between agencies whose primary purpose is law enforcement and agencies with both law enforcement and administrative functions. See Jefferson v. Department of Justice, 284 F.3d 172 (D.C. Cir. 2002) (ruling agencies must distinguish between records based on “allegations that could lead to civil and criminal sanctions” and records “maintained in the course of general oversight of government employees”).

(1) Agency whose primary function is not law enforcement (e.g., DoD’s primary function is war-fighting, not law enforcement) must establish that particular records at issue involved the enforcement of a statute or regulation within its authority. Jefferson v Department of Justice, *supra* (DoJ’s Office of Professional Responsibility has mixed functions, function related to collection of evidence for potential prosecution of attorney sufficiently related to a law enforcement function); Tax Analysts v. IRS, 294 F.3d 71 (D.C. Cir. 2002) (district court erred when it ruled that IRS does not compile information for law enforcement purpose).

(2) The exemption covers all law enforcement records, both “investigatory and non-investigatory materials. Tax Analysts v. IRS, *supra*.

b. Record must have a law enforcement purpose.

(1) Information that was originally compiled for law enforcement purposes, but later summarized in a new document not prepared for law enforcement purposes, is protected under the exemption. Abramson v. FBI, 456 U.S. 615 (1982).

(2) Exemption will protect non-law enforcement records that are “recompiled” for law enforcement purposes. John Doe Agency v. John Doe Corporation, 493 U.S. 146 (1989).

2. An agency *may* withhold law enforcement records under this exemption, but only to the extent disclosure:

“(A) could reasonably be expected to interfere with enforcement proceedings,

“(B) would deprive a person of a right to a fair trial or an impartial adjudication,

“(C) could reasonably be expected to constitute an unwarranted invasion

of personal privacy,

“(D) could reasonably be expected to disclose the identity of a confidential source. . . in a criminal or national security investigation . . . or information furnished by a confidential source,

“(E) would disclose techniques and procedures or would disclose guidelines for law enforcement investigations or prosecutions if disclosure could reasonably be expected to risk circumvention of the law, or

“(F) could reasonably be expected to endanger the life or physical safety of any person.”

3. Exception 7(A) does not require an agency to make a specific showing within the context of a particular case.

a. Agency may demonstrate that the disclosure of certain classes of documents would have the effect of interfering with agency enforcement. NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978).

b. Agency may rely upon Exemption 7(A) to exempt records only while a law enforcement proceeding [includes prosecution] is pending. See Maydak v. Department of Justice, 218 F.3d 760 (D.C. Cir. 2000) (refusing to allow agency to rely on exemptions not previously “substantiated” after it withdrew reliance upon Exemption 7(A) due to change in underlying circumstances; ordering disclosure of grand jury records, attorney work-product, and law enforcement records without redaction), *reh’g en banc denied*, No. 98-5492 (D.C. Cir. Oct. 30, 2000), *stay granted* (D.C. Cir. Nov. 29, 2000), *cert. denied*, 121 S. Ct. 2591 (2001). See also Ctr. for Nat’l Sec. Studies v. United States Department of Justice, 331 F.3d 918 (D.C. Cir. 2003) (upholding withholding of the identities of detainees held during the post-9/11 terrorist investigation, because disclosure “would give terrorist organizations a composite picture of the government investigation” and thus enable them to impede it through “counter-efforts.”).

4. Use of Exemption 7(B) is designed to prevent pre-trial publicity that would deprive a person of a fair trial.

a. Use of this exemption dependent upon a two-part test: a pending or imminent proceeding and determination that disclosure more probably than not would interfere with fairness.

b. There are few cases in this area. See Dow Jones Co., Inc. v. FERC, 219 F.R.D. 167 (C.D. Cal. 2002) (agency has not shown that any trial or adjudication is “pending or truly imminent” or that disclosure would generate pretrial publicity that could deprive the companies or their employees of their right to a fair trial).

5. Exemption 7(C) protects the personal privacy of individuals named in law enforcement files. See SafeCard Serv. V. SEC, 926 F.2d 1197 (D.C.

Cir. 1991).

- a. Privacy protections standards are greater under 7(C) than Exemption 6 (“reasonably be expected to constitute an unwarranted invasion of personal privacy” versus “clearly unwarranted invasion”). Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).
- b. Protects the names of both witnesses and investigators. See Palacio v. Department of Justice, No. 02-5247, 2003 U.S. App. LEXIS 1804 (D.C. Cir. Jan. 31, 2002) (*per curiam*) (identities of suspects, witnesses, and investigators properly withheld under Exemption 7(C)); Rugiero v. U.S. Department of Justice, 257 F.3d 534 (6th Cir. 2001) (protects the identities of government employees and investigators contained in DEA's investigatory files); Davis v. United States Department of Justice, No. 00-2457 (D.D.C. Mar. 21, 2003) (protects information that would identify FBI Special Agents and support personnel, other federal employees, third parties, informants, subjects of investigative interest, bank personnel, and state, local, federal, and foreign law enforcement personnel). See also Billington v. United States Department of Justice, 11 F.Supp. 2d 45 (D.D.C. 1998) (individual who admitted that he was an FBI informant possesses a diminished privacy interest under Exemption 7(C), but has not waived its protection) *aff'd in pertinent part*, 233 F.3d 581 (D.C. Cir. 2000).
- c. Glomar responses to targeted requests are appropriate. U.S. Department of Justice v. Reporters Comm. For Freedom of the Press, 489 U.S. 749 (1989) (ruling that FBI properly refused to confirm or deny whether it had a “rap sheet” on an alleged member of organized crime); Oguaju v. United States, 288 F.3d 448 (D.C. Cir. 2002) (Marshall Service properly refused to confirm or deny the existence of records regarding an escapee-turned-informant/ witness at the requester’s trial); Pusa v. FBI, 31 F.App’x 567 (9th Cir. 2002) (FBI properly refused to confirm or deny existence of records pertaining to communications between FBI and certain named third parties); Taylor v. Department of Justice, 257 F.Supp. 2d 101 (D.D.C. 2003) (holding there is no public interest in disclosure of third-party information that might assist a convict in challenging his conviction; FBI properly refused to confirm or deny the existence of records on living persons). See also, DOD Reg. 5400.7-R, para. C3.2.1.7.1.3.1-3.
- d. Exemption 7(C) may protect privacy of the close survivors of the deceased from disclosure of facts concerning his death. NARA v. Favish, 541 U.S. 157 (2004) (protecting privacy interests of close family members from the pain that would flow from the death scene photographs of Deputy White House Counsel Vincent Foster); Badhwar v. U.S. Department of the Air Force, 829 F.2d 182 (D.C. Cir. 1987) (disclosure of autopsy reports “might shock the sensibilities of surviving kin”); NY Times v. NASA, 782 F.Supp. 628 (D.D.C. 1991) (withholding audiotope of voices of Space Shuttle *Challenger* astronauts recorded immediately before their deaths, to

protect family members from pain of hearing final words of loved ones).

e. In a reverse FOIA case, the Supreme Court ruled that a corporation has no personal privacy interest in agency's investigation of its overcharging of schools for telecommunication services; observing that "[a]djectives typically reflect the meaning of corresponding nouns, but not always. Sometimes they acquire distinct meanings of their own" and in this case the "it" would not be reasonable to interpret the adjective "personal" to reflect the meaning of "person." The Supreme Court rejected the argument that the term "person" included a corporation in the phrase "personal privacy" and closed by saying "[w]e trust that AT&T will not take it personally." FCC v. AT&T, Inc., 131 S. Ct. 1177 (2011).

f. Exemption 7(C) may protect privacy by protecting identities of agency supervisors at levels equivalent to GS-14 and GS-15 disciplined for viewing pornography during work hours; "disclosure in this case is not limited to the reputational embarrassment of having misused government property on official time but rather extends to the embarrassment resulting from public knowledge that the conduct was of a sexual nature" and ruling that the disclosure of the names is not necessary to show the agency's "operations and activities" in light of the extensive release of the IG's report. Steese, Evans & Frankel v. SEC, No. 10-1071, Dist. LEXIS 129401 (D. Col. Dec. 7, 2010).

6. The purpose of Exemption 7(D) is to ensure that "confidential sources are not lost through retaliation against the source for past disclosure or because of source's fear of future disclosure." Brandt Construction v. Environmental Protection Agency, 778 F.2d 1258 (7th Cir. 1985).

a. Protects source's identity whenever he provides information under either an express promise of confidentiality or "under circumstances from which such an assurance could reasonably be inferred." See U.S. Department of Justice v. Landano, 508 U.S. 165 (1993); Rosenfeld v. Department of Justice, 57 F.3d 803 (9th Cir. 1995). *But see* Cooper Cameron Corp. v. U.S. Department of Labor, 280 F.3d 539 (5th Cir. Tex. 2002) (ordering disclosure of OSHA witness statements; finding no express promises of confidentiality despite declarant's statement that agency manual requires express promises to be given; implicitly and aberrationally ruling that circumstances giving rise to an implied promise of confidentiality can occur in a criminal investigation only).

b. The term "confidential source" is provided wider definition than limited meaning within criminal matters. This exemption is not limited to criminal witnesses and victims, rather protections are afforded to broad spectrum of individuals and institutions, excluding federal employees acting in their official capacity. See Retail Credit Company v. Federal Trade Commission, No. 75-0895, 1976 WL 1206 (D.D.C. 1976).

7. Exemption 7(E) provides protections similar to what was previously "High 2."

See Coastal Delivery Corp. v. United States Customs Serv., 272 F.Supp.2d 958 (C.D. Cal. 2003) (holding agency properly withheld records of Customs Service examinations conducted at the Los Angeles/Long Beach seaport “because terrorists . . . could use the information to discover the rate of inspection and then direct their containers to vulnerable ports.”); *reconsideration denied* id. at 966-68 (C.D. Cal. 2003); *appeal dismissed voluntarily*, No. 03-55833 (9th Cir. Aug. 26, 2003).

8. Exemption 7(F) permits the withholding of records necessary to protect the physical safety of a wide range of individuals.

a. No balancing test is required. See Living Rivers, Inc. v. United States Bureau of Reclamation, 272 F.Supp.2d 1313 (D. Utah 2003) (withholding of “inundation maps” of potential flood zones beneath Hoover and Glen Canyon Dams because disclosure “could aid in carrying out a terrorist attack” that “could reasonably place at risk the li[ves] or physical safety” of area residents; court held maps were compiled “in direct relation to” a governmental law enforcement function). *But see* ACLU v. DOD, 06-3140, 2008 WL 4287823 (2d Cir. Sept. 22, 2008) (affirming disclosure order of 21 photographs with identity redacted under Exemption 7(c), showing mistreatment of detainees, even though court accepted that their release “could reasonably be expected to incite violence against United States troops, other Coalition forces, and civilians in Iraq and Afghanistan”; ruling that government’s contention that “any individual” encompasses a person identified as belonging to of [sic] a population of national size would, if accepted, circumvent the limitation imposed by the phrase “could reasonably be expected to endanger.”)

b. The agency must only show a reasonable likelihood of physical danger to withhold information. L.A. Times Common’s, LLC v. Department of the Army, 442 F.Supp.2d 880 (C.D. Cal. 2006) (applying Exemption 7(F) where disclosure of private security contractor company names could endanger the life or safety of many individuals). Ctr. for Nat’l Sec. Studies v. U.S. Department of Justice, 215 F.Supp.2d 94 (D.D.C. 2002) (disclosure of the dates and locations of arrest, detention, and release of post-September 11th detainees would make detention facilities and their occupants vulnerable to retaliatory attacks), *rev’d in other part, aff’d in part on other grounds and remanded*, 331 F.3d 918 (D.C. Cir. 2003).

H. Exemptions 8: Financial Institutions Information.

I. Exemption 9: Geological and Geophysical Information.

VII. EXCLUSIONS.

The FOIA amendment of 1986 provided a new mechanism by which the government could protect limited sensitive law enforcement records. These exclusions permit law

enforcement officials to treat agency records as if they were not subject to the FOIA. Unlike normal FOIA responses in which the agency was required to either acknowledge the existence of records or provide a Glomar response, in cases involving exclusions, the agency merely responds that there are no records responsive to the request.

A. Exclusion 1. Investigation or proceedings involving possible criminal law violation, **and** subject unaware of pendency of investigation or proceedings, **and** disclosure of existence of records could reasonably be expected to interfere with enforcement proceedings.

B. Exclusion 2. Informant records maintained under informant's name or identifier, **and** maintained by a criminal law enforcement agency, unless informant's status as an informant has been officially confirmed.

C. Exclusion 3. Records maintained by FBI, **and** pertaining to foreign intelligence or counterintelligence, or international terrorism, **and** existence of records is classified.

VIII. CONCLUSION.

"A popular government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or, perhaps, both." - Pres. James Madison, August 4, 1822

"We seek a free flow of information...we are not afraid to entrust the American people with unpleasant facts, foreign ideas, alien philosophies, and competitive values." - Pres. John F. Kennedy, February 1962

"With the passage of the FOIA, the burden of proof shifted from the individual to the government. Those seeking information are no longer required to show a need for information.

Instead, the 'need to know' standard has been replaced by a 'right to know' doctrine. The government now has to justify the need for secrecy." - Introduction to the Citizens Guide on Using the Freedom of Information Act, published by the House Committee on Government Reform, September 2005.

CHAPTER B

THE PRIVACY ACT

5 USC § 552a

Outline of Instruction

I. REFERENCES..... 2

II. INTRODUCTION..... 3

III. SCOPE OF THE ACT. 4

IV. PUBLIC NOTICE OF SYSTEMS OF RECORDS. 8

V. COLLECTION AND MAINTENANCE OF INFORMATION 9

VI. DISCLOSURE OF INFORMATION FROM SYSTEMS OF RECORDS..... 13
EXCEPTIONS TO THE "NO DISCLOSURE WITHOUT CONSENT" RULE 14

VII. ACCESS TO AND AMENDMENT OF RECORDS 18
EXEMPTIONS THAT DENY ACCESS AND AMENDMENT..... 22

VIII. CRIMINAL PENALTIES. 24

IX. CIVIL REMEDIES. 25

X. SOCIAL SECURITY NUMBERS. 27

XI. CONCLUSION..... 28

I. REFERENCES.

A. Primary.

1. The Privacy Act of 1974, 5 U.S.C. § 552a, *as amended*.
2. Privacy Act Implementation, Office of Management and Budget, 40 Fed. Reg. 28948 (9 July 1975) *as amended* 40 Fed. Reg. 56741 (4 December 1975).
3. OMB Guidelines, 51 Fed. Reg. 18,982, 18,985 (1986).
4. Dep't of Defense Directive No. 5400.11, Department of Defense Privacy Program (8 May 2007, *Incorporating Change 1, September 1, 2011*).
5. Dep't of Defense Regulation No. 5400.11-R, Privacy Program (14 May 2007).
6. Army Regulation No. 340-21, The Army Privacy Program (5 July 1985).
7. Dep't of Army Pamphlet 25-51, The Army Privacy Program -- System Notices and Exemption Rules (30 April 1999).
8. Air Force Instruction 33-332, The Air Force Privacy Program (16 May 2011).
9. Secretary of the Navy Instruction 5211.5E, Department of the Navy Privacy Program (28 December 2005).
10. Marine Corps Order P5211.2B, The Privacy Act of 1974 (4 September 1997).

B. Secondary.

1. Overview of the Privacy Act of 1974 (February 2010), a Department of Justice publication; available at <http://www.justice.gov/opcl/1974privacyact-overview.htm>
2. Defense Privacy and Civil Liberties Office Web Page, provides current Privacy Act System of Records Notices and other Privacy Act guidance and information; available at <http://dpclo.defense.gov/privacy>.
3. Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1 (18 April 1992); available at [http://dpclo.defense.gov/privacy/About The Office/policy_guidance.html](http://dpclo.defense.gov/privacy/About%20The%20Office/policy_guidance.html) Electronic Privacy Information Center, Litigation Under the Federal Open Government Laws (2008).

4. Service specific resources available on-line.
 - a. Army: <https://www.rmda.army.mil/organization/pa.shtml>
 - b. Navy/Marine Corps:
<http://www.doncio.navy.mil/TagResults.aspx?ID=36>
 - c. Air Force: <http://www.privacy.af.mil/>
 - d. Coast Guard, <http://www.uscg.mil/foia/>

II. INTRODUCTION.

A. History of the Act. The Privacy Act of 1974 provides safeguards for the protection of records the Federal government collects on United States citizens or lawfully admitted permanent residents. It was passed in great haste during the final week of the Ninety-Third Congress after the illegal surveillance and investigation of individuals were exposed during the Watergate scandal. Due in part to its hasty enactment, no conference committee was convened to reconcile differences in the bills passed by the House and Senate. Instead, staffs of the respective committees--led by senators Ervin and Percy, and congressmen Moorhead and Erlenborn--prepared a final version of the bill that was ultimately enacted. The original reports are thus of limited utility in interpreting the final statute. The more reliable legislative history consists of a brief analysis of the compromise amendments--entitled "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act"--prepared by the staffs of the counterpart Senate and House committees and submitted in both the House and Senate in lieu of a conference report. See 120 Cong. Rec. 40,405-09, 40,881-83 (1974), *reprinted in* Source Book on Privacy (1976) at 858-68, 987-94.

B. Congressional Concerns.

C. Policy Objectives. "Broadly stated, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them." Privacy Act Overview (May 2004), 891. The Act addresses four major policy objectives:

1. Restrict disclosure of personal information maintained by agencies;
2. Allow individuals access to records about themselves;
3. Allow individuals to amend records about themselves; and,
4. Establish fair collection, maintenance and dissemination practices.

III. SCOPE OF THE ACT.

A. Generally applicable to agency records within a “System of Records.” Manuel v. Veterans Administration Hospital, 857 F.2d 1112 (6th Cir. 1988).

B. Key Definitions.

1. “Agency” means “any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President[*]), or any independent regulatory agency.”

a. Privacy Act adopts the FOIA definition. 5 U.S.C. § 552a(a)(1) incorporates 5 U.S.C. § 552(f).

b. * The Office of the President and those organizations within the Executive Office of the President whose function is limited to advising and assisting the President are excluded from the definition of agency.

c. Government contractors and their employees are covered by the civil and criminal penalties of the Act, if provided for by the contract. 5 U.S.C. § 552a(m).

2. “Individual” means “any citizen of the United States or an alien lawfully admitted for permanent residence” in the U.S. 5 U.S.C. § 552a(a)(2).

a. Definition is far more restrictive than the FOIA’s definition of “any person.”

b. Does not include deceased individuals. Crompton v. U.S., 843 F. Supp. 751 (D.D.C. 1994), *aff’d on other grounds*, 59 F. 3d 1400 (D.C. Cir. 1995). Likewise, neither surviving family members nor executors are specifically granted Privacy Act rights. See OMB Guidelines, 40 Fed. Reg. 28,948, 28,951 (11975). *But cf. NARA v. Favish*, 541 U.S. 157 (2004) (ruling that surviving relatives have a FOIA-recognized privacy interest in scene-of-death photos of their close relative).

c. Does not include corporations or business enterprises. Falwell v. Executive Office of the President, 158 F.Supp. 2d 734, 736 n.3 (W.D. Va. 2001) (plaintiff may make personal request under the Act, but Falwell’s corporate alter-egos are not individuals as defined under the law); St. Michael’s Convalescent Hospital v. California, 643 F.2d 1369 (9th Cir. 1981).

d. Privacy Act rights are personal to the individual and cannot be derivatively asserted by others. See Sirmans v. Caldera, 27 F. Supp. 2d 248 (D.D.C. 1998) (plaintiffs “may not object to the Army’s failure to correct the records of other officers”); Abramsky v. U.S. Consumer Products Safety Comm’n., 478 F. Supp. 1040 (S.D.N.Y. 1979) (union president cannot compel release of records pertaining to employee’s termination).

e. **Note:** parents of minor children and guardians of incompetents may act on behalf of that individual. 5 U.S.C. § 552a(h). The OMB Guidelines also note that minors are also authorized to independently exercise their Privacy Act rights.

f. Entrepreneurial information. Sole proprietors are not “individuals” under OMB’s view. OMB Guidelines 40 Fed. Reg. at 28,951. The cases are split 6-to-2 against OMB’s views. Compare, e.g., Scarborough v. Harvey, 493 F. Supp. 2d 1 (D.D.C., 2007) (rejecting distinction) with Shermco Indus. v. Sec’y of the U.S. Air Force, 452 F.Supp. 306 (N.D. Tex. 1978) (accepting distinction).

3. “Maintain” means to maintain, collect, use, or disseminate. § 552a(a)(3).

4. “Record” means “any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or other identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” 5 U.S.C. § 552a(a)(4).

a. As a general rule, the threshold requirement is that the information must contain his name or otherwise identify an individual. Pierce v. U.S. Dep’t of Air Force, 512 F. 3d 184 (5th Cir. 2007) (ruling that report of investigation summary, which refers to all personnel by job position rather than name, and contains no dates, is not a record). However, there are three jurisdictional differences in the manner in which courts determine whether a record is “about” an individual under the Act.

(1) Some jurisdictions require only that the record “**be about**” the subject of the record. See Unt v. Aerospace Corp., 765 F.2d 1440 (9th Cir. 1985) (letters written by appellant did not discuss appellant personally, therefore, they were not “records” subject to restrictive disclosure within the meaning of the Act).

(2) Some jurisdictions require the record **to both identify and be about** a subject. See Tobey v. NLRB, 40 F.3d 469 (D.C. Cir. 1994) (NLRB’s computerized unfair labor practice case tracking system was not a system of records about individuals of which notice was required in the Federal Register despite the presence of the identity of the field examiner within the records).

(3) Some jurisdictions have a very broad definition of a record that includes **any information that identifies a subject and any personal characteristic**. See Bechhoefer v. Dep't of Drug Enforcement, 209 F.3d 57 (2d Cir. 2000) (appellant's letter, on letterhead including both his name and address, satisfied statutory definition of record).

b. In unsettled jurisdictions, the safest course is to follow the Bechhoefer definition.

5. A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying particular assigned to the individual. § 552a(a)(5). Manuel v. VA, 857 F.2d 1112 (6th Cir. 1988); Crompton v. U.S., 843 F. Supp. 751 (D.D.C. 1994), *aff'd on other grounds*, 59 F. 3d 1400 (D.C. Cir. 1995).

a. The actual method of retrieval is the key to whether a record is within a system of records. Henke v. United States Dep't of Commerce, 83 F.3d 1453 (D.C. Cir. 1996) (holding that the test is whether the information is actually retrieved, not retrievable, by use of the individual's name or identifier); Yonemoto v. VA, No. 06-00378, 2007 WL 1310165 (D. Haw. May 2, 2007) (ruling that agency's e-mail archives are not a system of records; finding that "[j]ust because an agency is capable of retrieving the information, and just because it does so to comply with a FOIA request, does not mean that the information is maintained in a Privacy Act 'system of records'; such a manner of retrieval is not the 'actual practice of the VA'").

b. The technical definition of "system of records" makes coverage under the Act dependent upon the method of retrieval rather than the contents of the record. Consequently, there are critics who argue that this renders the Act subject to agency abuse. See U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society, (1977).

c. Personal notes – Treated the same as under the FOIA. Hudson v. Reno, 130 F.3d 1193 (6th Cir. 1997) (supervisor's notes about plaintiff's misconduct which were kept in a locked drawer and labeled the "First Assistant's" files do not fall within this definition). See also Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 38:

(1) "Personal notes of unit leaders or office supervisors concerning subordinates ordinarily are not records within a system of records governed by the Privacy Act. The Act defines 'system of records' as a 'group of any records under the control of any agency...from which information is retrieved by the ...[individual's] identifying particular...' [citation omitted]...Personal notes that are *merely an extension of the author's memory*, if maintained properly, will not come under the provisions of the Privacy Act or the Freedom of Information Act [citation omitted] (emphasis added)." *Id.*

(2) “To avoid being considered agency records, personal notes must meet certain requirements. *Keeping notes must be at the sole discretion of the author.* Any requirement by superior authority, whether by oral or written directive, regulation or command policy, likely would cause the notes to become official agency records. *Such notes must be restricted to the author’s personal use as memory aids. Passing them to a successor or showing them to other agency personnel would cause them to become agency records* (emphasis added). Chapman v. National Aeronautics and Space Administration, 682 F.2d 526 (5th Cir. 1982).”

(3) “Even if personal notes do become agency records, they will not be within a system of records and subject to the Privacy Act unless they are retrieved by the individual’s name or other personal particular. Thus if they are filed only under the matter in which the subordinate acted or in a chronological record of office activities, the Privacy Act would not apply to them. However, [they] would be subject to disclosure under the FOIA.” Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 38.

(4) “Individuals who maintain personal notes about agency personnel should ensure their notes do not become records within systems of records. Maintaining a system of records without complying with the Privacy Act system notice requirement could subject the individual to criminal charges and a \$5,000.00 fine. [citation omitted].” *Id.* See also Johnston v. Horne, 875 F.2d 1415 (9th Cir. 1989); Kalmin v. Dep’t of Navy, 605 F. Supp. 1492 (D.D.C. 1985).

(5) An agency may incorporate personal notes into agency records if it does so in a timely manner. Compare Chapman v. NASA, 682 F.2d 526 (5th Cir. 1982) (“Act did not prohibit taking and keeping private notes by a supervisor. However, when the notes were no longer kept private and were used to evaluate plaintiff, they had to be maintained consistent with the Act”) with Thompson v. Dep’t of Transportation, 547 F. Supp. 274 (D. Fla. 1982) (timeliness requirement met where materials upon which adverse disciplinary action is based are placed in the appropriate system of records contemporaneously with or within a reasonable time after an adverse disciplinary action is proposed).

(6) See Johnson v. Horne, 875 F.2d 1415 (9th Cir. 1989) (supervisor’s private notes about an employee not covered under Privacy Act because they are not agency records); Bowyer v. Dep’t of the Air Force, 804 F.2d 428, 431-31 (7th Cir. 1986) (same); Boyd v. Secretary of the Navy, 709 F.2d 684, 686-87 (11th Cir. 1983) (same), *cert. denied*, 104 S. Ct. 709 (1984).

6. "Disclosure." The general prohibition is quite broad. "No agency shall disclose any record which is within a system of records by any means of communication to any person . . ." 5 U.S.C. § 552a(b).

a. Consent may **not** be implied.

b. Verbal reports of information maintained within a system of records may constitute an improper disclosure.

IV. PUBLIC NOTICE OF SYSTEMS OF RECORDS.

A. Publication Requirement. Public notice must appear in the Federal Register. 5 U.S.C. § 552a(e)(4).

1. No longer an annual requirement. However, advance notice to Congress and OMB is required for any new or altered system of records. 5 U.S.C. § 552a(r).

2. Publication in the Federal Register of any new routine use is required at least 30 days prior to use under (e)(4)(D) to provide an opportunity for public comment. 5 U.S.C. § 552a(e)(11).

3. There are both agency-specific and government-wide system notices. As a general rule, DOD and DOD components publish military-specific system notices. For a complete list of the DOD's Privacy Act System of Records Notices, as well as links to all government wide systems notices, see <http://dpcl.o.defense.gov/privacy/SORNs/SORNs.html>.

B. Contents of a system notice. 5 U.S.C. § 552a(e)(4).

1. Name and location of the system;

2. Categories of individuals on whom records are maintained;

3. Categories of records maintained in the system;

4. Each routine use of the records, including categories and purpose of users;

5. Policies and practices regarding storage, retrieval, access, retention, and disposal of records within the system;

6. Title and business address of the responsible agency official;

7. Procedures regarding individual's right to notification upon request;

8. Procedures whereby an individual can be notified at his request how he can gain access to any record retaining to him and how he can contest its contents; and,

9. Categories of sources of records in the system.

V. COLLECTION AND MAINTENANCE OF INFORMATION.

A. Collect only relevant and necessary information to accomplish an agency purpose as defined by statute or Executive Order. 5 U.S.C. § 552a(e)(1).

B. Collect information to greatest extent practicable directly from the individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. 5 U.S.C. §552a(e)(2).

1. Collect from the subject first when the information sought is "objective and unalterable." Dong v. Smithsonian, 943 F. Supp. 69 (D.D.C. 1996) (holding that concerns over Plaintiff's possible reaction to an "unpleasant rumor" does not excuse noncompliance with the Act), *rev'd on other grounds*, 125 F.3d 877 (D.C. Cir. 1997); Waters v. Thornburgh, 888 F.2d 870 (D.C. Cir. 1989) (finding that the issue of plaintiff's attendance at bar examination is inalterable and that agency violated Act by interviewing others first); Brune v. IRS, 861 F.2d 1284 (D.C. Cir. 1988) (holding as permissible the earlier interview of witnesses in an investigation involving potential "shake-down" of audited taxpayers).

2. Collect from third parties when:

a. Verifying information (security or employment);

b. Seeking opinion or evaluation;

c. Unable to contact subject;

d. Collecting is exceptionally difficult (unreasonable cost or delay); or,

e. Consent or subject asks for third party collection.

f. See, e.g., OMB Guidelines, 40 Fed. Reg. 28,948, 28,961 ("Practical considerations . . . may dictate that a third party source . . . be used as a source of information in some cases . . . It may well be that the kind of information needed can only be obtained from a third party").

C. Maintain no records regarding how an individual exercises First Amendment rights. 5 U.S.C. § 552a(e)(7).

1. Threshold. The record at issue must implicate the individual's First Amendment rights. See Cloud v. Heckler, 3 Gov't Disclosure Serv. (P-H) para 83,230, at 83,962 (W.D. Ark. Apr. 21, 1983) (filing of employee's letters criticizing agency, written while on duty, does not violate subsection (e)(7) because "[p]oor judgment is not protected by the First Amendment").

2. Exceptions.

a. Consent of the subject.

b. Authorized by statute. Hass v. United States Air Force, 848 F. Supp. 926 (D. Kan. 1994) (retaining copy of plaintiff's earlier FOIA requests is not the maintenance of information related to plaintiff's exercise of her First Amendment rights).

c. Pertinent to and within the scope of an authorized law enforcement activity. *Compare* Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982) (NSA's collection of international telegraphic communications and transfer of that data to the FBI properly within law enforcement exception of the Act, because FBI had reasonable cause to believe that Jabara was a foreign agent when it requested the summaries) *with* Clarkson v. IRS, 678 F.2d 1368 (11th Cir. 1982) (collection of appellant's political speeches in an IRS file labeled "Tax Protestors" constitutes violation of the Act).

3. Applies to all records, regardless of where maintained. Boyd v. Secretary of the Navy, 709 F.2d 684 (11th Cir. 1983) (holding that PA prohibition regarding collecting First Amendment information applied even when record not maintained in a system of records); Albright v. United States, 631 F. 2d 915 (D.C. Cir. 1980) ("desk drawer" storage of video of federal employees during a meeting explaining a denial of promotions held to be a record related to exercise of First Amendment rights).

D. Inform individuals asked to supply information of the authority for solicitation of the information and whether disclosure is mandatory or voluntary; the purpose for which the information is to be used; the routine uses applicable to the information; and the effects of not providing the information. This notice is general called a "**Privacy Act Advisement.**" 5 U.S.C. § 552a(e)(3).

1. When required.

a. Notice **must** be provided when agency collects from an individual any personal information which will be kept in a system of records.

b. Notice **should** be given to third party sources of information at the time of collection. See Gardner v. United States, No. 96-1467, 1999 U.S. Dist. LEXIS 2195 (D.D.C. Jan. 29, 1999) (noting that although Act mandates actual notice of routine uses, "information in the instant case was not gathered from Plaintiff, but from third-parties"). *But see* Saunders v. Schweiker, 508 F. Supp. 305 (W.D.N.Y. 1981) (plain language of Act "does not in any way distinguish between first-party and third-party contacts").

2. Content of the Privacy Act Advisement:

a. The authority for collection;

- b. The principal purpose for collection;
- c. Whether disclosure is voluntary or mandatory;
- d. The effect of not providing information; and,
- e. The routine uses which may be made of the information. See Covert v. Harrington, 876 F.2d 751 (9th Cir. 1989) (Dep't of Energy disclosure of employee security forms to the Dep't of Justice improper because agency failed to notify its employees that the information in the files would be used for law enforcement purposes).

3. Location. "Placement of the Privacy Act advisory statement in a form should be in the following order of preference:

- a. Below the title of the form and positioned so the individual will be advised of the requested information,
- b. Within the body of the form with a notation of its location below the title of the form,
- c. On the reverse of the form with a notation of its location below the title of the form,
- d. Attached to the form as a tear-off sheet, or
- e. Issued as a separate supplement to the form." See Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 18.

E. Accuracy requirements.

1. Maintain records used to make determinations about an individual with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness in the determination. 5 U.S.C. § 552a(e)(5). Perfect records are not required; reasonableness is the standard. Doe v. United States, 821 F.2d 694 (D.C. Cir. 1987) (*en banc*) (not inaccurate for agency to file ROI containing sharply conflicting accounts of unwitnessed interview between Dep't of State security agent and Doe, despite language that "there is no reason to doubt the statements made by [the] agent," since file also contain's Doe's rebuttal); Edison v. Dep't of the Army, 672 F.2d 840 (11th Cir. 1982) (finding that appellant failed to show any causal connection between his incorrect ORB and the decision to pass him over for promotion, finding that there were many other possible factors which may have gone into the board's decision).

2. Before disseminating the record to a person other than an agency, unless disseminated pursuant to FOIA, the agency will make reasonable efforts to ensure the records are accurate, complete, timely and relevant for agency purposes. 5 U.S.C. § 552a(e)(6). See Pontecorvo v. FBI, No. 00-1511, slip op. at 20 (D.D.C. Sept. 30, 2001) (finding that “if the information gathered and contained within an individual’s background records is the subjective opinion of witnesses, it is incapable of being verified as false and cannot constitute inaccurate statements under the Privacy Act”).

F. Accounting for disclosures. “Each agency, with respect to each system of records under its control, must keep a record of the date, nature, and purpose of each disclosure of a record to any person or to another agency under subsection (b) and the name and address of the person or agency to whom the disclosure is made.”

1. Disclosure accounting is required unless the record is disclosed within the agency (Exception 1) or pursuant to FOIA (Exception 2). 5 U.S.C. § 552a(c)(1).

2. Accounting of disclosures must be kept for five years or the life of the record, whichever is longer. See 5 U.S.C. § 552a(c)(2).

3. Except for disclosures made to law enforcement agencies, an individual is entitled, upon request, to access to accounting. See 5 U.S.C. § 552a(c)(3).

4. Agency must inform any person or other agency about any correction or notation of dispute made by the agency in accordance with a subject’s amendment rights. See 5 U.S.C. § 552a(c)(4).

5. DA Form 4410-R may be used to record disclosure for accounting purposes.

G. Agency must make reasonable efforts to notify an individual when any record is made available to any person under compulsory process when such process becomes a matter of public record. 5 U.S.C. § 552a(e)(8). See Moore v. United States Postal Serv., 609 F. Supp. 681 (E.D.N.Y. 1985) (“§552a(e)(8) does not speak of advance notice of release”).

H. Establish rules of conduct for persons dealing with Privacy Act records and instruct each person regarding the Act’s requirements. 5 U.S.C. § 552a(e)(9).

I. Establish safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. 5 U.S.C. § 552a(e)(10).

VI. DISCLOSURE OF INFORMATION FROM SYSTEMS OF RECORDS.

A. Disclosure prohibited. The “no disclosure without consent” rule: “No agency shall disclose any record . . . by any means of communication to any person, or to another agency, except pursuant to a written request by or with the prior written consent of the individual to whom the records pertains, unless an exception applies.” 5 U.S.C. § 552a(b).

1. Consent must be express. See Wiley v. Veterans Admin., 176 F.Supp 2d 747 (E.D. Mi. 2001) (prospective employees broadly worded “release,” executed concurrent with employment application in 1990, served as valid consent for purpose of disclosure to employer in 1999).
2. “Disclosures” can be made by written, oral, electronic, or mechanical means. See OMB Guidelines, 40 Fed. Reg. 28,948, 28,953 (1975).
3. Prohibition applies only if disclosure is from a system of records.
 - a. Pertains to information initially retrieved from a system of records. Boyd v. Secretary of the Navy, 709 F.2d 684 (11th Cir. 1983) (memorandum documenting meeting between appellant and Navy supervisors not a record because it was not maintained by appellee in a group of records keyed to appellant’s name); Henke v. Dep’t of Commerce, 83 F.3d 1453 (D.C. Cir. 1996) (computer database was not a system of records as there is no evidence that agency regularly or even frequently used the names of the contact persons to obtain information about those persons).
 - b. Excludes knowledge independently derived. An employee’s personal opinion or information drawn from personal memory is not equivalent to retrieval from a system of records. Kline v. HHS, 927 F.2d 522 (10th Cir. 1983) (holding that verbal information about employee derived from independent knowledge and not from an agency system of records are not subject to the Privacy Act). *But see* Bartel v. FAA, 725 F.2d 1403 (D.C. Cir. 1984) (holding “independent knowledge defense” is not available to employees personally involved in creation of record).
4. A later release of information previously known does not violate the Privacy Act. Hollis v. Department of the Army, 856 F.2d 1541 (D.C. Cir. 1988) (holding that when a release of service member’s child care allotments consisted “merely of information . . . which the recipient of the release already knew, the Privacy Act is not violated”); FDIC v. Dye, 642 F.2d 833 (5th Cir. 1981). *But see* Pilon v. Department of Justice, 73 F.3d 1111 (D.C. Cir. 1996) (holding that Act violated by faxing document to a former employee previously familiar with the document’s contents).

5. Privacy Act is not limited to extra-judicial disclosures; it applies even where a disclosure to a court during the course of litigation is undertaken. See Laningham v. Navy, 813 F.2d 1236 (D.C. Cir. 1987) (*per curiam*) (holding that Navy did not intentionally and willfully disclose disability board information in civil trial in violation of PA). If while in litigation, an agency receives a request for Privacy Act information, counsel must object on the ground that the Privacy Act prohibits disclosure, or obtain a court order, see Exception 11 *infra*, permitting such disclosure.

B. There are **12 Exceptions** to the “no disclosure without consent” rule that permit third-party access to information without prior written consent of the subject of the record. 5 U.S.C. § 552a(b)(1)-(12).

1. **Exception 1.** Disclosure to “officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1). The “Need to Know” exception.

a. This exception authorizes **intra**-agency disclosures only for necessary, official purposes. See OMB Guidelines, 40 Fed. Reg. 28,948, 28,950-01, 28,954 (1975).

(1) Improper uses are impermissible. See Parks v. IRS, 618 F.2d 677 (10th Cir. 1980) (disclosure of names of employees who did not purchase savings bonds, “for solicitation purposes,” held improper); Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 37.

(2) Examples of proper “need to know” disclosures. Bigelow v. DOD, 217 F.3d 875 (D.C. Cir. 2000) (approving supervisor’s review of appellant’s personnel file related to supervisor’s “continuing duty to make sure that [plaintiff] was worthy of trust”; supervisor “had a need to examine the file in view of the doubts that had been raised in his mind about [plaintiff] and [plaintiff’s] access to the country’s top secrets”); Britt v. Naval Investigative Serv., 886 F.2d 544 (3d Cir. 1989) (proper to disclose investigative report to commander “since the Reserves might need to reevaluate Britt’s access to sensitive information or the level of responsibility he was accorded”); Jones v. Dep’t of the Air Force, 947 F. Supp. 1507 (D. Colo. 1996) (no violation for Air Force investigator to review medical and mental health records and then comment on the contents in ROI compiled in preparation for plaintiff’s court-martial, which was distributed to certain Air Force personnel); Hass v. United States Air Force, 848 F. Supp. 926, 932 (D. Kan. 1994) (upholding disclosure of mental health evaluation to officers who ultimately made decision to revoke plaintiff’s security clearance and discharge her).

b. Are contractors who operate a system of records to accomplish an agency mission considered agency employees? Two cases have held yes. See Coakley v. Dep’t of Transportation, 1994 U.S. Dist. LEXIS 21402

(D.D.C. Apr. 7, 1994); Hulett v. Dep't of the Navy, No. TH 85-310-C, slip op. (S.D. Ind. Oct. 26, 1987) (medical and personnel records disclosed to contractor/psychiatrist for purpose of assisting him in performing "fitness for duty" examination), *aff'd*, 866 F.2d 432 (7th Cir. 1988) (unpublished table decision). See also Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 16. *But see Taylor v. Orr*, 1983 U.S. Dist. LEXIS 20334 (D.D.C. Dec. 5, 1983) (Sec'y of the Air Force violated the Act by providing plaintiff's examining physician a copy of her personnel records without her consent prior to a fitness-for-duty examination ordered by the secretary). OMB recommends use of a routine use to accomplish disclosures to contractors.

2. **Exception 2.** Disclosure **required** by the FOIA. 5 U.S.C. § 552a(b)(2). See Greentree v. United States Customs Serv., 674 F.2d 74, 79 (D.C. Cir. 1982) (subsection (b)(2) "represents a Congressional mandate that the Privacy Act not be used as a barrier to FOIA access").

a. The Privacy Act/FOIA interface typically involves FOIA Exemption 6, Protection of Personal Privacy, and FOIA Exemption 7(C), Records or Information Compiled for Law Enforcement Purpose the disclosure of which could reasonably be expected to result in an unwarranted invasion of privacy. Both exemptions require a balancing of the competing interests: Public Interests in Disclosure v. Invasion of Privacy. See Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

b. No discretionary release.

(1) No agency "discretionary disclosure" of information that is exempt under FOIA **and** subject to the Privacy Act. DOD v. FLRA, 510 U.S. 487 (1994).

(2) Agency must have an actual FOIA request to rely on exception 2. See Zeller v. United States, 467 F. Supp. 487, 503 (E.D.N.Y. 1979) (FOIA exception to Privacy Act does not apply because "nothing in the FOIA appears to require such information to be released in the absence of a request therefore"). See also OMB Memorandum for the Senior Agency Officials for Information Resources Management, SUBJECT: Privacy Act Guidance - Update, dated 24 May 1985. Compare Bartel v. FAA, 725 F.2d 1403 (D.C. Cir. 1984) (FOIA was meant to limit agency discretion to deny public access to information in its files, therefore, the Privacy Act must be read generally to preclude nonconsensual disclosure of Privacy Act material unless the agency acts pursuant to a FOIA request) with Cochran v. United States, 770 F.2d 949 (11th Cir. 1985) (absence of written FOIA request irrelevant because overwhelming balance favored the public's right to disclosure of the information which related to a violation of the public trust by a senior government official; requested records would not be withholdable under any FOIA exemption).

c. Applying both statutes to requests for Privacy Act covered records. Analysis of third-party requests: Does a FOIA exemption permit withholding? If the answer is “Yes,” (e.g., the Exemption 6 balancing test favors the subject’s personal privacy), the record must be withheld. If the answer is “No,” (e.g., the Exemption 6 balancing test favors the public interest), the record must be released.

3. **Exception 3.** Disclosure pursuant to published routine use. 5 U.S.C. § 552a(b)(3). Because it is potentially so broad, this is a controversial exception.

a. Threshold. The terms of this exception establish two requirements.

(1) First, the agency must provide constructive notice of the routine use through publication in the Federal Register.

(2) Second, the routine use must meet the compatibility requirement; that is, disclosure of record must be for a purpose that is compatible with the reason for which it was collected. 5 U.S.C. § 552a(a)(7). See Britt v. Naval Investigative Service, 886 F.2d 544 (3rd Cir. 1989) (holding that transfer of Marine Reservist’s military criminal investigation file to his civilian federal employer did not meet the Act’s compatibility requirement); Swenson v. United States Postal Service, 890 F.2d 1075 (9th Cir. 1989).

b. There are two types of routine uses: specific and general.

(1) Specific routine uses are strictly construed to cover only those uses listed within published systems notices. See Pontecorvo v. FBI, No. 00-1511, slip op. at 13-15 (D.D.C. Sept. 30, 2001) (ordering discovery to determine whether the agency “overstepped [the] explicit restrictions” contained in its routine use).

(a) Each service has published lists of systems notices. See DA Pam 25-51, AFP 12-36, OPNAVNOTE 5211, MCBUL 5211.

(b) CAUTION: Many printed collections of systems notices are out of date. Use on-line sources, such as <http://www.defenselink.mil/privacy/notices/> for most current systems notices.

(c) An agency’s construction of its routine use is entitled to deference. See Dep’t of the Air Force, Scott Air Force Base, Ill. v. FLRA, 104 F.3d 1396, 1402 (D.C. Cir. 1997).

(2) General routine uses cover all of the agency’s systems notices and provide broad disclosure guidance that may be interpreted to cover a range of activities, such as:

- (a) To law enforcement agencies when record indicates a violation or potential violation of law.
- (b) To other federal agencies on request for hiring, retention, security clearance, or licensing decisions by those agencies.
- (c) In response to Congressional inquiries and private relief legislation. Pellerin v. VA, 790 F.2d 1553 (11th Cir. 1986). *But see Swenson v. United States Postal Service*, 890 F.2d 1075 (9th Cir. 1989) (disclosure beyond scope of inquiry).
- (d) As required by international agreement.
- (e) To the Department of Justice for litigation.
- (f) For counter-intelligence purposes or enforcing laws which protect the national security.

4. **Exception 4.** Disclosure to the Bureau of Census. 5 U.S.C. § 552a(b)(4).

5. **Exception 5.** Disclosure for statistical research. 5 U.S.C. § 552a(b)(5).

6. **Exception 6.** Disclosure to the National Archives and Records Administration as a record having sufficient historical or other value to warrant its continued preservation, or for evaluation by the Archivist to determine whether the record has such value. 5 U.S.C. § 552a(b)(6).

7. **Exception 7.** Disclosure “to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought. 5 U.S.C. § 552a(b)(7). See Doe v. Naval Air Station, 768 F.2d 1229 (11th Cir. 1985) (oral request from detective insufficient).

8. **Exception 8.** Disclosure “to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.” 5 U.S.C. § 552a(b)(8).

- a. Case law emphasizes emergency nature of exception.
- b. Disclosure notification must be sent to last known address.

c. Individual about whom records are disclosed need not necessarily be the individual whose health or safety is at peril; *e.g.*, release of records on several individuals in order to identify an individual who was injured in an accident. See OMB's Privacy Act Guidelines, 40 Fed. Reg. 28,955 (1975); DePlanche v. Califano, 549 F. Supp. 685 (W.D. Mich. 1982).

9. **Exception 9.** Disclosure "to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee." 5 U.S.C. § 552a(b)(9).

a. Disclosure need not be based upon Congressional request. Devine v. United States, 202 F.3d 547 (2d Cir. 2000).

b. Disclosure must be to Congressional body, rather than member. Swenson v. U.S. Postal Service, 890 F.2d 1075 (9th Cir. 1989).

10. **Exception 10.** Disclosure to the Comptroller General in the course of the performance of the duties of the General Accounting Office. 5 U.S.C. § 552a(b)(10).

11. **Exception 11.** Disclosure "pursuant to the order of a court of competent jurisdiction." 5 U.S.C. § 552a(b)(11).

a. Excludes grand jury subpoenas. Doe v. DiGenova, 779 F.2d 74 (D.C. Cir. 1985).

b. Unclear whether exception covers orders from states courts, though there are no court cases on point and OMB has not issued formal guidance.

12. **Exception 12.** Disclosure to a consumer reporting agency in accordance with the Debt Collection Act. 5 U.S.C. § 552a(b)(12).

VII. ACCESS TO AND AMENDMENT OF RECORDS.

A. Each agency that maintains a system of records **shall**:

1. Access: "upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him . . . to review the record and have a copy made . . ." 5 U.S.C. § 552a (d)(1); subject to ten exemptions discussed below.

2. Amendment: "permit the individual to request amendment of a record pertaining to him . . ." 5 U.S.C. § 552a(d)(2).

B. Access Issues.

1. Third party information in the subject/requester's file.
 - a. Remember the definition of a "record." If the information identifies requestor and pertains to requestor, the agency should release/permit access.
 - b. If the information does not identify the requestor or is not "about" the requestor, the agency may deny access. See Voelker v. IRS, 646 F.2d 332 (8th Cir. 1981); compare DePlanche v. Califano, 549 F. Supp 685 (W.D. Mich. 1982).
2. Medical records of minors. DOD Reg. 5400.11-R, para. C3.1.6.5.
 - a. The Privacy Act applies to "[citizens] of the United States or [aliens] lawfully admitted for permanent residence." Minors are protected by the Act because minority is not a disqualifier. 5 U.S.C. § 552a(a)(2), see also Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 9.
 - b. The Privacy Act provides that "the parent of any minor...may act on behalf of the individual." 5 U.S.C. § 552a(h).
 - c. Stateside.
 - (1) Definition of minor? State law.
 - (2) If a minor, may release records to parents unless prohibited by state law.
 - (3) Look to the law of the state in which the records are located as state laws differ on the issue of access to a minor's medical records based, in part, on the subject matter of the record (e.g., psychiatric records, treatment records for drug and alcohol abuse, sexual hygiene/reproductive records).
 - d. Overseas.
 - (1) Definition of minor? The Department of Defense deems the age of majority to be 18 years.
 - (2) Parental access. Parents have a general right of access to medical records of minors.
 - (3) Parents may be denied access only if **all** of the following four conditions are met:
 - (a) Minor was between ages 15 and 17 at the time of treatment.

(b) Treatment sought in program that promised to keep treatment records confidential.

(c) Minor specifically requested confidentiality.

(d) Parent did not have the minor's written authorization or a court order.

3. Access denied under Privacy Act, but accessible under FOIA.

a. The Privacy Act is not a FOIA Exemption 3 withholding statute. Provenzano v. DOJ, 717 F.2d 799 (3d Cir. 1983), *vacated as moot*, 469 U.S. 14 (1984).

b. Congress clarified the Privacy Act's status in the CIA Information Act, Pub. L. No. 98-477, § 2(c), 98 Stat. 2211, 2212 (1984) (codified at 5 U.S.C. § 552a(t)(2)).

C. Amendment Issues.

1. A subject may seek correction of facts but has no authority to demand the amendment of an agency employee's opinion or judgment.

a. Corrections are limited to facts, not judgments, under the Act. Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 4; Hewitt v. Grabicki, 794 F.2d 1373 (9th Cir. 1986).

b. A requestor may seek the amendment of agency judgments only if all underlying facts are discredited. Mueller v. Winter, 485 F.3d 1191 (D.C. Cir. 2007); RR v. Dep't of Army, 482 F. Supp. 770 (D.D.C. 1980) (*dictum*).

2. A subject may not use the Privacy Act to collaterally attack an agency decision, if that issue was already the subject of judicial or quasi-judicial action. Sugrue v. Derwinski, 26 F. 3d 8 (2d Cir. 1994).

a. Issues for which adequate judicial review is available. Henderson v. Social Security Administration, 908 F.2d 559 (10th Cir. 1990).

b. A subject must exhaust administrative remedies before filing suit for an agency's refusal to permit amendment. Cargill v. Marsh, 902 F.2d 1006 (D.C. Cir. 1990).

3. If, after an appeal, the agency refuses to amend the record, the agency must permit the individual to file a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and must notify the individual of the provisions for judicial review of the agency's action. 5 U.S.C. § 552a(d)(3).

4. In any subsequent disclosure of information about an individual who has filed a statement of disagreement, the agency must clearly note the portion of the record which is disputed and provide copies of the statement, and, if the agency deems it appropriate, a concise statement of the reasons for the agency's refusal to amend the record. 5 U.S.C. § 552a(d)(4).

a. Individual agency determines what "concise" means, but should be lenient.

b. Statements of disagreements often prove damaging to the requestor.

5. Where the agency has made prior disclosures of a disputed record and an accounting was made, the agency must inform prior recipients of any correction or notation of dispute that concerns the disclosed record. 5 U.S.C. § 552a(c)(4). See "Accounting for Disclosures," at para V.F, *supra*.

D. Burdens of Proof.

1. Access. 5 U.S.C. § 552a(g)(3)(A). Burden of proof is upon agency. Courts have authority to conduct a *de novo* review.

2. Amendment. 5 U.S.C. § 552a(d)(2)(B)(i). Burden of proof is upon the plaintiff to prove that record is not accurate, relevant, timely or complete. Mervin v. FTC, 591 F.2d 821 (D.C. Cir. 1978).

E. Processing an Access or Amendment Request.

1. Time Limits.

a. Access. The agency has 10 working days to acknowledge the request and must release/provide access within 30 working days.

b. Amendment.

(1) Custodian/System Manager has 10 working days to acknowledge request and 20 additional working days (30 total working days) to provide a final response. 5 U.S.C. § 552a(d).

(2) Denial/Refusal Authority.

(a) Army. There is no specified time limit on action by the Access and Amendment Refusal Authority (AARA). AR 340-21, para 1-7.

(b) Air Force. The "Denial Authority" does not have a specified time limit. AFI 33-332, para 5.3.

(c) Navy/Marines. "Denial Authority" SECNAVINST 5211.5E, para 7.I.

2. Appeal.

- a. The requestor must appeal the agency action within 60 calendar days.
- b. The Review Authority will decide the requestor's appeal within 30 working days, unless for "good cause" the head of the agency extends the decision for 30 more days. 5 U.S.C. § 552a(d)(3).

F. There are ten exemptions that deny access and amendment rights to the subject of a Privacy Act record. 5 U.S.C. § 552A (j) and (k).

1. Agencies may claim exemptions to deny a subject access to his own records.
 - a. Exemptions are not generally automatic; agency head must have previously published a regulation explaining why the exemption (other than (d)(5)) is applicable to that particular system.
 - b. Agencies are not entitled to improperly claimed exemptions. Ryan v. Dep't of Justice, 595 F.2d 954 (4th Cir. 1979).
 - c. Exemptions are strictly construed. Agencies have the burden of proof to deny a subject access to his or her own file.
2. One Special Exemption. 5 U.S.C. § 552a(d)(5).
 - a. "Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding."
 - b. This is the only self-executing exemption.
 - c. Applies to administrative proceedings. Martin v. Office of Special Counsel, 819 F.2d 1181 (D.C. Cir. 1987); Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 27.
3. Two General Exemptions. 5 U.S.C. § 552a(j)(1)-(2).
 - a. The general exemptions cover records:
 - (1) Maintained by the CIA (5 U.S.C. § 552a (j)(1)); or,
 - (2) Maintained by an agency/component thereof which performs as its principal function any activity pertaining to law enforcement (5 U.S.C. § 552a (j)(2)).
 - b. According to the Defense Privacy Board, the exemption does not follow a record transferred from an exempt system to a nonexempt system. Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 31. *But see Doe v. FBI*, 936 F.2d 1346 (D.C. Cir. 1991).
 - c. There is no temporal limitation to these exemptions.

4. Seven Specific Exemptions. 5 U.S.C. § 552a(k)(1)-(7).

a. The special exemptions cover records that are:

(1) Classified (simply incorporates FOIA exemption 1 protections in the Privacy Act context). 5 U.S.C. § 552a(k)(1).

(2) Investigatory material compiled for law enforcement purposes not covered by 5 U.S.C. § 552a(j)(2) [the second general exemption]. 5 U.S.C. § 552a(k)(2).

(a) This exemption protects all information in the system of records unless the subject has been deprived of a federal right, privilege, or benefit as a result of the maintenance of the records.

(b) If so, the subject would be entitled to access to all material except that which would identify a confidential source who provided information under an express promise of confidentiality.

(3) Maintained in connection with providing protective services to the President of the United States or other individuals. 5 U.S.C. § 552a(k)(3).

(4) Required by statute to be maintained and used solely as statistical records. 5 U.S.C. § 552a(k)(4).

(5) 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 material. 5 U.S.C. § 552a(k)(5).

(a) This is a narrow exemption which is limited to the protection of a confidential source who provided the information pursuant to an **express** promise of confidentiality.

(b) Applicable even though the source of the confidential information is known to the requester. Volz v. Dep't of Justice, 619 F.2d 49 (10th Cir. 1980).

(c) There is no temporal limit to the protection.

(d) Also includes material compiled to determine whether a federal grant will be awarded. Henke v. United States Dep't of Commerce, 83 F.3d 1445 (D.C. Cir. 1996).

(6) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process. 5 U.S.C. § 552a(k)(6).

(a) Release of material that implicates the applicant evaluation system “would give future applicants an unfair advantage and would impair the usefulness and value of the system.” Patton v. Federal Bureau of Investigations, 626 F. Supp. 445 (M.D. Pa. 1985).

(b) Robinett v. U.S. Postal Service, Civil Action No.: 02-1094, 2002 U.S. Dist. LEXIS 13779 (E.D. La. Jul. 24, 2002) (scoring evaluation information on employment application fell within the parameters of an exemption statute under the FOIA and 5 U.S.C. § 552a(k)(6) of the Privacy Act).

(7) Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source who was granted an express promise of confidentiality. 5 U.S.C. § 552a(k)(7). See also, May v. Dep’t of Air Force, 777 F.2d 1012 (5th Cir. 1985).

5. Summary: Analysis of first person access requests:

a. Does a Privacy Act exemption apply (e.g., the document is a law enforcement record or prepared in anticipation of litigation)? If the answer is “No,” the agency must grant access to the document. If the answer is “Yes,” the agency may withhold.

b. Does a FOIA exemption apply (e.g., on-going LEA investigation under 7(C))? If the answer is “Yes,” the agency may withhold the document. If the answer is “No,” the agency must release.

c. An agency may only withhold a record from a subject ONLY when Exemptions apply under both the FOIA and Privacy Act.

VIII. CRIMINAL PENALTIES.

A. “Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than **\$5,000.**” 5 U.S.C. § 552a(i). See, e.g., United States v. Trabert, 978 F.Supp 1368 (D.Colo. 1997)

B. “Any officer or employee of an agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.” 5 U.S.C. § 552a(2).

C. "Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000." 5 U.S.C. § 552a(3).

D. Criminal action is against the individual, not the agency.

IX. CIVIL REMEDIES.

A. Statutory. 5 U.S.C. § 552a(g).

1. Violations and remedies.

a. Wrongful refusal to amend. 5 U.S.C. § 552a(g)(1)(A); 5 U.S.C. § 552a(g)(2). Remedy: Enjoin/order amendment; attorney fees/costs.

b. Wrongful denial of access. 5 U.S.C. § 552a(g)(1)(B); 5 U.S.C. § 552a(g)(3). Remedy: Enjoin from withholding; provide in camera inspection; attorney fees/costs.

c. Failure to maintain accurate, timely, complete, and relevant records resulting in an adverse determination. 5 U.S.C. § 552a(g)(1)(C); 5 U.S.C. § 552a(g)(4). Remedy: If agency acted in an intentional/willful manner, U.S. is liable for: Actual damages but not less than \$1,000; attorney fees/costs.

d. Failure to comply with another provision causing an adverse effect. 5 U.S.C. § 552a(g)(1)(D); 5 U.S.C. § 552a(g)(4). Remedy: If agency acted in an intentional/willful manner, U.S. liable for: Actual damages but not less than \$1,000; attorney fees/costs.

2. Civil remedies are solely against the agency.

3. Courts are not free to create remedies greater than those granted by the statute. Edison v. Dep't of Army, 672 F.2d 840 (11th Cir. 1982).

4. Intentional or willful refers to the intentional or willful failure to abide by the Act. Andrews v. VA, 838 F.2d 418 (10th Cir. 1988); Tijerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987); Albright v. U.S., 732 F.2d 181 (D.C. Cir. 1984).

5. Privacy Act does not mandate agency to create and maintain files, and destruction of an official record does not give right to a Privacy Act cause of action. Tufts v. Dep't of Air Force, 793 F.2d 259 (10th Cir. 1986).

6. Damages.

a. Doe v. Chao, 540 U.S. 614 (2004) (ruling that “actual damages” must be proved to recover the statutory minimum of \$1,000 or damages beyond the minimum; out-of-pocket damages will suffice but it is not clear if solely nonpecuniary damages for mental injuries are sufficient). See also Jacobs v. Nat’l Drug Intelligence Ctr, 548 F. 3d 375 (5th Cir. 2008) (upholding \$100,000 award for emotional distress, noting that Doe v. Chao did not authoritatively rule on this issue).

b. Cummings v. Dep’t of the Navy, 279 F. 3d 1051 (D.C. Cir. 2002) (holding Feres v. United States, 340 U.S. 135 (1950), inapplicable to Service members Privacy Act lawsuit, whether seeking injunctive relief or damages).

7. Attorney’s Fees. The Privacy Act includes “fee shifting” provisions. Anderson v. Dep’t of Treasury, 648 F.2d 1 (D.C. Cir. 1979).

a. Threshold requirement: plaintiff must substantially prevail. Sweatt v. U.S. Navy, 683 F.2d 420 (D.C. Cir. 1982).

b. Not paid to a *pro se* litigant even if plaintiff is an attorney. Manos v. Department of the Air Force, 829 F. Supp. 1191 (N.D. Cal. 1993).

c. Only permitted for litigation; not administrative actions. Kennedy v. Andrus, 459 F. Supp. 240 (D.D.C. 1978), *aff’d*, 612 F. 2d 586 (D.C. Cir. 1980)(table cite).

8. Two-year statute of limitations governs Privacy Act actions. 5 U.S.C. § 552a(g)(5). Bowyer v. Department of Air Force, 875 F.2d 632 (7th Cir. 1989); Tijerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987).

B. Tort Actions.

1. One court has held that the Privacy Act “does not limit the remedial rights of persons to pursue whatever remedies they may have under the [Federal Tort Claims Act] for privacy violations consisting of record disclosures.” O’Donnell v. United States, 891 F. 2d 1079 (3^d Cir. 1989).

2. It now appears settled that the Privacy Act consists of a “comprehensive legislative scheme” that precludes Bivens constitutional tort remedies. See Wilson v. Libby, 535 F. 3d 697 (D.C. Cir. 2008); Downie v. City of Middleburg Heights, 301 F. 3d 688 (6th Cir. 2002).

3. Note also that the statutory scheme established under “FOIA precludes the creation of a Bivins remedy.” Johnson v. Executive Office for U.S. Attorneys, 310 F.3d 771 (D.C. Cir. 2002).

X. SOCIAL SECURITY NUMBERS.

A. Section 7(a)(1). (Enacted as part of the Privacy Act, but not codified.) “It shall be unlawful for any Federal, State, or local governmental agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number.” By its terms, Section 7 does not apply to:

1. Any disclosure required by Federal statute, or,
2. Any disclosure required under any Federal, State, or local statute or regulation in existence and operating before 1 January 1975 to verify the identity of the individual.

B. “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 authority such number is solicited, and what uses will be made of it.” Section 7(b).

C. DOD Regulations

1. DOD 5400.11-R, Chapter 2, para C2.1.2. - Collecting Social Security Numbers.
2. Army Regulation 340-21, para 4-3 – “If the individual refuses to disclose the SSN [other than for purposes of establishing personnel, financial, or medical records], the Army activity must be prepared to identify the individual by alternate means.”
3. SECNAVINST 5211.5E, para 9.c.(7) – A DON activity may request a SSN even if not required or pre-1975 system of record, but must notify voluntary and if refused, must identify by alternate means.
4. AFI 33-332, para 3.3 – “Do not deny people legal right, benefit, or privilege for refusing to give their SSNs unless the law requires disclosure, or law or regulation adopted before January 1, 1975 required the SSN ...” (no alternate means identification provision).

D. DODI 1000.30, August 1, 2012 , incorporates and cancels (DTM) 2007-015-USD(P&R)—“DoD Social Security Number (SSN) Reduction Plan.”

1. This instruction establishes the policy and assigns responsibility for reduction of SSN in DoD. It is the DoD policy to reduce or eliminate the use of SSNs wherever possible.
2. The use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted or disguised. SSNs shall be used in approved form when they meet the criteria established in the instruction.

3. The identified acceptable uses include:
 - a. Law Enforcement, National Security, Credentialing
 - b. Security Clearance Investigation or Verification
 - c. Interactions With Financial Institutions
 - d. Confirmation of Employment Eligibility
 - e. Administration of Federal Worker's Compensation
 - f. Federal Taxpayer Identification Number
 - g. Computer Matching
 - h. Foreign Travel
 - i. Geneva Conventions Serial Number
 - j. Noncombatant Evacuation Operations
 - k. Legacy System Interface
 - l. Operational Necessity
 - m. Other Cases (with specified documentation)

E. Section 7 applies to state and local agencies as well.

XI. CONCLUSION.

The underlying purpose of the Privacy Act is to give citizens more control over personal information collected by the Federal Government and how that information is used. The act accomplishes this in four basic ways. It seeks to establish sound information practices in the federal agencies and requires public notice of all systems of records. It requires that the information contained in these record systems be accurate, complete, relevant, and timely. It provides procedures whereby individuals can inspect and correct inaccuracies in almost all Federal records about themselves. Finally, it limits disclosure of records; requires agencies to keep an accurate accounting of disclosures; and, with certain exceptions, makes these disclosures available to the subject of the record. In the event that the statute is violated there are both criminal sanctions and civil remedies.

CHAPTER C

**Health Insurance Portability and
Accountability Act**

Part I

Military Command Exception



TMA Privacy and Civil Liberties Office

Information Paper



Military Command Exception and Disclosing PHI of Armed Forces Personnel

HIPAA Privacy ♦ March 2013

I. Supporting Policies for this Information Paper

- A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule establishes requirements regarding uses and disclosures for specialized government functions. See 45 CFR 164.512(k).
- B. The DoD Health Information Privacy Regulation implements the above provision of the HIPAA Privacy Rule within the Military Health System (MHS). See (DoD 6025.18-R, C7.11).
- C. Federal Register Notice, Volume 68, No. 68, Page 17357, “DoD Health Information Privacy Program,” April 9, 2003, describes implementation of provisions that are made to allow appropriate uses and disclosures of protected health information (PHI) concerning members of the Armed Forces to assure the proper execution of the military mission.
- D. The DoD Instruction (DoDI) 6490.08, “Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members,” August 17, 2011, provides guidance for MHS and other DoD health care providers regarding disclosing PHI related to mental health and/or substance misuse problems.
- E. The DoD Directive 6490.02E, “Comprehensive Health Surveillance,” February 8, 2012, establishes policy and assigns responsibilities for routine, comprehensive health surveillance of all DoD personnel throughout their military service or DoD civilian employment.
- F. The Alcohol, Drug Abuse, and Mental Health Administration Reorganization Act (ADAMHA), 42 U.S.C. 290dd-2, and the implementing regulations, 43 CFR Part 2, establish special confidentiality rules for disclosing information about substance misuse treatment.

II. Definitions Associated with the Military Command Exception

- A. **Covered Entity:** A health plan or a healthcare provider within the MHS that transmits any health information in electronic form to carry out financial or administrative activities related to healthcare.

- B. Disclosure: The release, transfer, provision of access to, or revealing in any other manner of PHI outside the entity holding the information.
- C. Military Health System (MHS): All DoD health plans and all DoD healthcare providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by TMA, the Army, the Navy, or the Air Force.
- D. Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by a covered entity in its role as employer.
- E. Use: With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

III. Guidance Regarding the Military Command Exception

- A. Concept. As an exception to the HIPAA Privacy Rule's limits on the use and disclosure of PHI, a covered entity, including DoD and civilian covered entities, may use and disclose the PHI of Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.
- B. Appropriate Military Command Authorities. Appropriate military command authorities to whom PHI may be disclosed include:
 - 1. All commanders who exercise authority over the Service member.
 - 2. The commander's designee, authorized to take an action designed to assure the proper execution of the military mission.
 - 3. The Secretary of the Service of which the individual is a member.
 - 4. The Secretary's designee, authorized to take an action designed to assure the proper execution of the military mission.
- C. Authorized Purposes for Which the PHI May Be Disclosed. The purposes for which any and all of the Service member's PHI may be used or disclosed are the following:
 - 1. Determining the member's fitness for duty, including the member's compliance with disability evaluations and physical fitness standards or fitness to perform any particular mission, assignment, order, or duty.
 - 2. Carrying out comprehensive medical surveillance activities.
 - 3. Reporting on casualties in connection with a military operation or activity.
 - 4. Carrying out any other activity necessary to the proper execution of the military mission.
- D. Mental Health and/or Substance Misuse. DoD has issued distinct guidance regarding treatment for mental health and substance misuse. According to DoDI 6490.08, disclosure to a commander about a Service member's mental health and/or substance misuse treatment is either strictly **prohibited** or absolutely **required** (based on specific criteria). Thus, in contrast to most permitted disclosures under the HIPAA Privacy Rule, disclosures to military commanders by

DoD providers about mental health or substance misuse treatment are not left to the provider's discretionary judgment.

1. In order to dispel stigma around Service members seeking mental health care or voluntary substance misuse education, DoDI 6490.08 establishes policy that balances patient rights to confidentiality with the commander's need to make informed operational and risk management decisions.
2. In accordance with DoDI 6490.08, DoD healthcare providers shall follow the strict presumption that they are **not** to notify a Service member's commander when the member obtains mental health care and/or substance misuse education services – unless the presumption is **overcome by one of the specific criteria** listed in D.3 below.
3. DoD healthcare providers shall notify the commander, providing only the minimum amount of information necessary to satisfy the disclosure's purpose, when a Service member meets the criteria for one of the following mental health and/or substance misuse conditions or related circumstances:
 - a. Harm to self. There is a serious risk of self-harm by the member.
 - b. Harm to others. There is a serious risk of harm to others. This includes any disclosures concerning child abuse or domestic violence.
 - c. Harm to mission. There is a serious risk of harm to a specific military mission.
 - d. Special personnel. The member is in the Personnel Reliability Program or has mission responsibilities of such potential sensitivity or urgency that normal notification standards would significantly risk mission accomplishment.
 - e. Inpatient care. The member is admitted or discharged from any inpatient mental health or substance misuse treatment facility.
 - f. Acute medical conditions interfering with duty. The member is experiencing an acute mental health condition or is engaged in an acute medical treatment regimen that impairs the member's ability to perform assigned duties.
 - g. Substance misuse treatment program. The member has entered into, or is being discharged from, a formal outpatient or inpatient treatment program for the treatment of substance misuse.
 - h. Command-directed mental health evaluation. The mental health services are obtained as a result of a command-directed mental health evaluation.
 - i. Other special circumstances. The notification is based on other special circumstances in which proper execution of the military mission outweighs the interests served by avoiding notification, as determined on a case-by-case basis by a covered entity.
4. Under the ADAMHA authority, DoD covered entities shall comply with the special rules protecting the confidentiality of substance misuse patient records in Federally-assisted substance misuse programs.
5. Commanders or other authorized officials, receiving PHI from a covered entity, shall protect the information in accordance with the Privacy Act of 1974 to ensure that it is not disclosed impermissibly. Information provided shall be restricted to personnel with a specific need to know; that is, access to the information must be necessary for the conduct of official duties.

IV. Frequently Asked Questions Regarding the Military Command Exception

- A. Are all covered entities required to disclose PHI of Armed Forces personnel when properly requested by appropriate military command authorities?

No. The DoD 6025.18-R, C7.11.1.1 and associated Federal Register notice state that covered entities “may” disclose PHI of Armed Forces personnel, indicating that disclosure of PHI is made at the discretion of the covered entity. DoD providers do not have such discretion with respect to mental health and substance abuse treatment information. See Section III.D above.

- B. What Military Treatment Facility (MTF) policies and procedures regarding this type of use and disclosure provision should be established?

1. Maintain an approved roster of commanders and other persons who may access unit members’ PHI on the commander’s behalf.
2. Develop criteria for requests to ensure release of only the minimum necessary PHI (e.g., cases requiring a clinical summary rather than the entire medical record).
3. Establish a policy to designate authority, within an MTF, for release of PHI.
4. Ensure proper training of personnel on the types of information that qualify as PHI.
5. Ensure that local policies and procedures include consideration of circumstances that duty crews encounter. Educate personnel about local policies concerning routine PHI requests from commanders that are considered necessary for making military mission impact determinations.

- C. Does the MTF have to account for these types of disclosures?

In accordance with DoD 6025.18-R, C13, the MTF is required to account for the disclosure of Armed Forces personnel PHI to command authorities. However, this accounting requirement does not apply to a Service member’s voluntary disclosure of his/her health information to a command authority.

- D. Are command authorities allowed access to PHI regarding a Service member’s family member if a situation with that beneficiary negatively impacts the Service member’s ability to perform his/her military mission?

No. This military command exception is only valid for Armed Forces personnel. PHI of family members or other categories of beneficiaries is never shared with command authorities without a valid authorization.

- E. Are medical appointment reminders concerning Armed Forces personnel permitted to be shared with command authorities?

Yes. Command authorities and/or their designee may require notification of medical appointments for Armed Forces personnel to determine fitness for duty and to ensure proper execution of the military mission. Medical appointment notifications include treatment reminders (physicals, immunizations, laboratory, etc.) and notifications of missed and cancelled

appointments. These reminders and notifications are considered “treatment” and are therefore, not currently required to be included in any accounting for disclosures. However, when these reminders and notifications are disclosed to command authorities under the military command exception, the HIPAA required, minimum necessary standard applies. Thus, MHS workforce members may disclose information regarding medical appointments of Armed Forces personnel to command authorities only to the extent necessary to accomplish the permitted purpose of the disclosure.

F. What resources are available to help with making a determination regarding the disclosure of Armed Forces personnel PHI to command authorities?

In addition to the supporting policies cited above, be sure to also utilize the local legal office, MTF Privacy Officer, and/or the Service HIPAA Privacy Representative.

For additional information, please refer to the “Military Command Exception” web page on the TMA Privacy and Civil Liberties Office web site at:

<http://www.tricare.mil/tma/privacy/Military-Command-Exception.aspx>.

CHAPTER C

Part II

HIPAA/Privacy Act Comparison

Information Paper

The Federal Privacy Act of 1974 and HIPAA Privacy Rule of 1996: A Comparison

Introduction

While health care providers have a long tradition of safeguarding private health information, protection of patient rights has recently been at the forefront of discussion. The old system of storing private patient information in locked filing cabinets is no longer practical or feasible—modern technology now allows for the rapid transmission of medical information electronically. However, along with this ease of sharing come new concerns regarding the confidentiality and protection of patient information. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule of 1996 provides clear standards for protection of personal health information or Protected Health Information (PHI). Prior to the Privacy Rule, PHI could be distributed without notice or authorization by the patient for reasons other than the patient’s medical treatment and/or health care payment. While improving the efficiency of the healthcare delivery system, the act protects the privacy of PHI by simplifying the processes involved in transmitting data by standardizing electronic data interchange. This act sought to close a gap in the 1974 Privacy Act, which provided some safeguards to the collection and use of personal information by the federal government and its entities.

The Privacy Act of 1974, Public Law 93-579

The Privacy Act of 1974 provides individuals the right of access to information concerning themselves that is maintained by any federal agency in the Executive Branch. The Act also established controls over what personal information the federal government collects and how it uses or discloses that information. The Act arose out of concerns about how the creation and use of computerized databases might impact individuals’ privacy rights. It safeguards privacy with the use of four personal data rights: Government agencies must show an individual any records kept on him or her; Agencies must follow certain principles, called “fair information practices,” regarding personal data. Agencies are restricted in how they can share individual data with other people and agencies; Individuals may sue the government for violating the Act’s provisions.

Health Insurance Portability and Accountability Act of 1996

The HIPAA Privacy Rule (*45 CFR Parts 160 and 164*)

HIPAA improves the efficiency and effectiveness of the health care industry in three primary ways; 1) by administrative simplifications provisions that develop single and universal claims and payment transaction codes, 2) by protecting the privacy and security of PHI, and 3) by providing provisions for the enforcement of its rules. The scope of HIPAA encompasses the following entities: health care plans, health care clearinghouses, and all health care providers who conduct certain health care transactions electronically.

The Privacy Rule is the foundation for federal protection for the privacy of PHI. PHI includes individually identifiable health information related to the past, present or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Even the fact that an individual received medical care is protected information under the regulation.

Privacy Rights

Together, the 1996 HIPPA Privacy Rule and the 1974 Privacy Act allow patients more rights and control over personal and medical information. In combination the acts do the following:

- Set boundaries on the use and release of personal data;
- Generally limit release of information to the minimum reasonably needed for the purpose of the disclosure.
- Establish safeguard standards for protecting the privacy of personal data.
 - Enable individuals to learn how their data may be used and about certain disclosures of their data that have been made
 - Empower individuals to control certain uses and disclosures of their personal data.
- Generally give individuals the right to examine and obtain a copy of their own personal data and request corrections.
- Hold violators accountable, with civil and criminal penalties that can be imposed if they violate individuals' rights.

Oversight

The Privacy Act empowers the Director of the Office of Management and Budget to develop regulations and guidelines on how agencies should implement the Act.

HIPAA empowers Health and Human Services (HHS) Office for Civil Rights to enforce the Privacy Rule by promoting voluntary compliance and using civil monetary penalties.

Penalties for Violations of Privacy

Both acts impose penalties on violators. The HIPAA Privacy Rule is the stricter of the two, imposing both civil and criminal penalties for violations of privacy. Penalties are generally assessed when organizations or individuals act with willful neglect or intent to cause harm. Civil penalties are specified at \$100 per violation, not to exceed \$25,000 per person per year for identical violations. Criminal penalties for wrongful disclosure of PHI can go up to \$250,000 and/or 10 years imprisonment if the offense is committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm.

The 1974 Privacy Act gives an individual the right to sue the federal government if it violates the statute. In addition:

- Any officer or employer of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information, and conveys that information to any person or agency not entitled to receive it shall be guilty of a misdemeanor and fined not more than \$5,000.
- Any officer or employee of an agency who willfully maintains a system of records for personal use shall be guilty of a misdemeanor and fined not more than \$5000.

Any person who knowingly and willfully requests or obtains and record concerning an individual from an agency under false pretense shall be guilty of a misdemeanor and fined not more than \$5000.

Discussion

The purpose of both acts was to strengthen the rights of the public in regards to the collection and use private information. Both work together to achieve the goal of protecting the privacy of personal information. Though HIPAA focuses mainly on medical information, the HIPAA Privacy Rule provision strengthens the intent of the Privacy Right Act of 1974 in that it requires all Federal agencies and/or Federal contractors that maintain personal records of individuals to adhere to the Privacy Rule's requirements and comply with the Privacy Act.

Comments

The Acts differ in that the 1974 Act covers overall personal data collection and use by the federal government, not private entities. HIPAA seeks to close this gap by targeting an industry that has more information on the public than the government—the medical field. HIPAA is more specific because it only targets medical information—but it is far reaching because it closes all of this personal data off to others, including the government, if they cannot show a compelling interest for having access to this data.

CHAPTER C

Part III

Guide for Law Enforcement

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

What is the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (*HIPAA*) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?

HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan). These are known as covered entities. Hospitals, and most clinics, physicians and other health care practitioners are HIPAA covered entities. In addition, HIPAA protects PHI held by business associates, such as billing services and

others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?

Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students at a university health clinic.



Under what circumstances may a HIPAA covered entity disclose PHI to law enforcement?

A HIPAA covered entity may disclose PHI to law enforcement with the individual's signed HIPAA authorization.

A HIPAA covered entity also may disclose PHI to law enforcement without the individual's signed HIPAA authorization in certain incidents, including:

- To report PHI to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
- To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the premises of the covered entity.
- To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.
- When responding to an off-site medical emergency, as necessary to alert law enforcement to criminal activity.
- To report PHI to law enforcement when required by law to do so (such as reporting gunshots or stab wounds).

- To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or an administrative request from a law enforcement official (the administrative request must include a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used).
- To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person, but the information must be limited to basic demographic and health information about the person.
- To respond to a request for PHI about an adult victim of a crime when the victim agrees (or in limited circumstances if the individual is unable to agree). Child abuse or neglect may be reported, without a parent's agreement, to any law enforcement official authorized by law to receive such reports.

For More Information

This is a summary of the relevant provisions and does not include all requirements that are found in the HIPAA Privacy Rule. For complete information, please visit the U.S. Department of Health and Human Service's Office for Civil Rights HIPAA web site at <http://www.hhs.gov/ocr/privacy>.