Street FOIA[1] 101: Nuts, Bolts, and Loose Change

Lieutenant Colonel Craig E. Merutka[*]

Introduction—The FOIA Team: It Takes a Village

In a 17 September 2008 memorandum, the Director of the Army Staff and the Administrative Assistant to the Secretary of the Army emphasized the importance of the "FOIA Team," a group of professionals charged with implementing the Freedom of Information Act (FOIA)[2] throughout the Army. They discussed the bare bones team consisting of "FOIA Officers, Public Affairs Officers, servicing judge advocates, and Initial Denial Authorities,"[3] but there are certainly more members. The gist of the FOIA Team concept is that it takes a lot of coordinated effort to successfully implement the FOIA program, and it is important that this effort receive command and organizational support.[4] Managing and implementing the FOIA program is simply not a one-person job and it may very well take a village to do it correctly.

With over 34,000 FOIA requests received each year, the Army's FOIA program is and must be decentralized. Reliance upon installation FOIA Teams, therefore, is a necessity. Most installations and commands employ a designated FOIA Official who leads this team, though the amount of time each official can designate solely to the FOIA varies from location to location. At most locations, FOIA duties comprise only part of the duty day for the appointed official, who is typically also responsible for duties involving the Privacy Act, records management, the mail room, and/or command publications. Worse, with tight manning tables and perhaps an unrealistic hope that FOIA requesters will not find them overseas, most units even deploy to the combat zone without a designated FOIA Official. As a result, the management of the FOIA process often falls to Judge Advocates (JA) at the brigade and division levels who, back at home station, may or may not have even been a member of the FOIA Team. For an overwhelming majority of these JAs, processing FOIA requests during the deployment is not their primary duty. So, unlike other federal agencies that operate consolidated FOIA offices manned by full-time FOIA employees who process most agency FOIA requests, the Army must rely upon installation and command part-time FOIA employees and deployed JAs at division and brigade levels to manage a decentralized FOIA operation. This decentralization and reliance upon personnel, "down in the trenches," whose FOIA focus is often only part-time has been referred to by at least one anonymous JA as "street FOIA."

This article is written for members of the "street FOIA Teams" at various levels. It provides up to date information on recent changes and some practical nuts and bolts information on a number of FOIA topics. The issues raised are those that have impact at the installation and lower level, those that have been the subject of inquiry here at the Judge Advocate General's Legal Center and School, or are details the author did not necessarily know about when he was practicing out on the street but wishes he did.

FOIA Changes—The "Openness Promotes Effectiveness in Our National Government Act of 2007," (or the "OPEN Government Act of 2007"): Just When You Thought It Couldn't Get Any More Complex

Every ten years or so, Congress passes a major amendment to the FOIA. Prior to 2007, the last one was the E-FOIA Act in 1996.[5] Like the E-FOIA Act, the most recent amendment, the OPEN Government Act of 2007,[6] made several significant procedural changes to the FOIA.[7] Chief among those involve attorney fees, time limits, and annual reporting requirements.

---

[1] The Freedom of Information Act, 5 U.S.C. § 552 (2000).

[*] Judge Advocate, U.S. Army. Currently assigned as Professor, The Judge Advocate General's Legal Ctr. &Sch. (TJAGLCS), Charlottesville, Va. LL.M., 2003, TJAGLCS, Charlottesville, Va.; J.D., 1991, University of Tulsa; B.S., 1988, Oklahoma State University. The author acknowledges and appreciates the assistance of Mr. Richard L. Huff, former co-Director, Office of Information and Privacy, U.S. Department of Justice, and FOIA mentor to over twenty years worth of JAG School FOIA professors.

[2] Memorandum from Lieutenant General David H. Huntoon, Jr., Director of the Army Staff, & Joyce E. Morrow, Admin. Assistant to the Sec'y of the Army, to Principal Officials of HQDA et. al., subject: Freedom of Information Act (FOIA) Program (17 Sept. 2008), https://www.rmda.army.mil/foia/docs/foiaProgramMemo.pdf [hereinafter Huntoon Memo].

[3] *Id.* para. 2.

[4] "It is essential that core members of the 'FOIA Team' receive command and organizational support and are provided the training necessary to implement [the FOIA] program professionally, and in accordance with the mandates of law and regulation." *Id.* para. 3.

[5] The Electronic Freedom of Information Act of 1996, Pub. L. No. 104-231, 110 Stat. 3048.

[6] The Openness Promotes Effectiveness in our National Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524 [hereinafter OPEN Government Act].

The FOIA establishes a statutory right, *enforceable in court*, of access to government agency records.[8] Unsatisfied requesters can file a FOIA lawsuit in response to a variety of situations, most common are when an agency fails to meet a statutory deadline for responding to a request or addressing an appeal, or when records are not released. In addition to obtaining the requested records, the only relief available is the recovery of attorney fees and litigation costs that may be awarded to those requesters who "substantially prevail" in court.[9]

Immediately prior to the enactment of the OPEN Government Act, a complainant "substantially prevailed" only when a court ordered an agency to change its position or approved a consent decree between the parties.[10] Absent such an order or decree, agencies would not be liable for fees or costs. Agencies could, and sometimes would, release documents prior to the issuance of an order if they felt the court would rule against them, in order to avoid a court ordered release.[11] As a result, FOIA plaintiffs would not be awarded fees and costs even though their lawsuit essentially caused the agency to change their position regarding the previously withheld records.

The OPEN Government Act changed this analysis and reinstated the pre-*Buckannon* "catalyst" test which allowed for the awarding of fees and costs if a FOIA plaintiff's lawsuit was the catalyst that caused the government to change course.[12] Under this "catalyst" test, a plaintiff was deemed to have substantially prevailed if prosecution of the action was required and had caused the agency to release the records sought.[13] The OPEN Government Act defines substantially prevailed as relief obtained through either "a judicial order, or an enforceable written agreement or consent decree; or a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial."[14] If a lawsuit is filed and the suit causes the agency to change course, attorney fees and litigation costs can be awarded to a FOIA plaintiff.

Until the OPEN Government Act, however, the attorney fee and litigation cost provision of the FOIA was perhaps of little concern to the installation FOIA Team since any such award was paid for by the federal government out of the United States Judgment Fund.[15] This is no longer the case. Congress now mandates that any award of fees and costs be paid "only from funds annually appropriated for any authorized purpose for the Federal agency against which a claim or judgment has been rendered."[16] As of December 2008, the Department of Defense (DoD) has not issued definitive guidance on whether such judgments will be paid for by DoD or whether it will be passed down to components or even further—down to installations and units. Passing the responsibility down to that level has some precedence[17] and the possibility that an installation could be required to pay attorneys fees and litigation costs to a FOIA requester who files a lawsuit is very real. Doing things the right way will go a long way in keeping this from happening.

---

[7] *S*ee FOIA Post, Congress Passes Amendments to the FOIA (Jan. 9, 2008), *available at* http://www.usdoj.gov/oip/foiapost/2008foiapost9.htm (providing summary and explanation of the OPEN Government Act of 2007).

[8] U.S. DEP'T OF JUSTICE, OFFICE OF INFORMATION AND PRIVACY, FREEDOM OF INFORMATION ACT GUIDE 5 (Mar. 2007) [herinafter DOJ FOIA GUIDE].

[9] 5 U.S.C. § 552(a)(4)(E)(i).

[10] Buckhannon Bd. & Care Home, Inc. v. W. Va. Dep't of Health and Human Res., 532 U.S. 598 (2001).

[11] Telephone Interview with Richard L. Huff, former Co-Director, Office of Info. and Privacy, U.S. Dep't of Justice (Nov. 25, 2008).

[12] *See, e.g.*, Weisberg v. U.S. Dep't of Justice, 848 F.2d 1265 (D.C. Cir. 1988).

[13] *Id.*

[14] 5 U.S.C. § 552(a)(4)(E)(ii).

[15] 31 U.S.C.S. § 1304 (LexisNexis2008) (authorizing payment from the US Judgment Fund of final judgments issued by a federal court).

[16] OPEN Government Act, *supra* note 6, sec. 4.

[17] In 2002, President Bush signed the Notification and Federal Employee Anti-discrimination and Retaliation of 2002 (No FEAR) Act into law. No FEAR Act, 5 U.S.C. § 2301 note (2007). It mandates that all judgments, awards, and compromise settlements paid to a complainant as the result of a violation of anti-discrimination and whistleblower protection laws be paid from "any appropriation, fund, or other account . . . available for operating expenses of the federal agency to which the discriminatory conduct involved is attributable." *Id.* § 201. As a result, installations and units are paying these fees from their operations and maintenance funds.

FOIA plaintiffs often go into court when an agency fails to meet a statutory time limit. Unfortunately, one of the most difficult requirements of the FOIA is the twenty working-day period allotted to agencies to initially respond to a valid FOIA request.[18] Though this deadline can be extended an additional ten working-days in unusual circumstances,[19] even this extended deadline is often difficult to meet. It is critical then that it is understood when the time starts, when it is tolled, and when it actually ends.

Starting on 31 December 2008, the OPEN Government Act provides that the twenty working-day period starts when "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 first received by any component of the agency that is designated in the agency's regulations . . . to receive requests."[20] Army regulations designate Army field commands, installations, and organizations with FOIA Officials as organizations authorized to receive FOIA requests.[21] The OPEN Government Act provision actually provides for two start dates. First, the time starts when a valid request is received by the appropriate component of the agency.[22] So, when the appropriate Army installation FOIA Official receives a FOIA request for an Army record, the time starts. Second, when a component within an agency receives a request that asks for records of another component, the clock starts when the correct component receives the forwarded request or in ten days, whichever is shorter.[23] This imposes a duty to promptly forward misdirected requests to the correct component. So, an Army installation FOIA Official who receives a request for a Navy record has the obligation to forward the request to the Navy since Army installation FOIA Officials are those designated in Army regulations as those authorized to receive FOIA requests. The clock for the Navy starts the day the Navy receives the forwarded request from the Army or ten days after the Army first received it, whichever time is shorter.

The requirement to forward misdirected requests has existed *intra*-Army for some time now. Current Army regulation requires that misdirected requests be forwarded promptly to the component with the responsibility for the records requested, and that the period allowed for responding to the request does not start until the request is received by the component that manages those records.[24] The OPEN Government Act now requires Army FOIA Officials to forward misdirected FOIA requests to the correct installation or command within ten working-days. This should actually be viewed as neither a positive or negative development within the Army since forwarding misdirected requests is a current Army requirement and the ten working-day requirement serves as either a grace period or a limitation depending upon how it is viewed.

The best practice when it comes to misdirected FOIA requests is to forward any request as soon as it is determined that another DoD component or another Army installation or command is the correct recipient. Failure to do so only harms FOIA Teammates at other locations. Also, whenever forwarding requests to another component or location, the original receiving organization should keep the FOIA requester informed of the action, unless notifying him will reveal information that is rightfully protected by a FOIA exemption.

Starting with requests received on 31 December 2008, once the twenty working-day clock starts, the OPEN Government Act limits agencies ability to toll the clock to two circumstances.[25] "Tolling" refers to the situation where the twenty working-day clock stops. The first circumstance that tolls the clock is when an agency makes a "reasonable" request to the requester for additional information about the requested records. This information must not be fee related and can only toll the clock one time. While agencies may of course ask for additional information from the requester more than once, the

---

[18] 5 U.S.C § 552(a)(6)(A)(i).

[19] *Id.* § 552(a)(6)(B)(i).

[20] *Id.* § 552(a)(6)(A)(ii); *see also* FOIA Post, OIP Guidance: New Requirement to Route Misdirected FOIA Requests (Nov. 18, 2008), http://www.usdoj.gov/oip/foiapost/2008foiapost31.htm (providing Department of Justice (DoJ) guidance regarding misdirected FOIA requests).

[21] Department of the Army Freedom of Information Act Final Rule, 32 C.F.R. pt. 518, § 518.7(a) (Feb. 22, 2006) [hereinafter Final Rule], *available at* http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title32/32cfr518_main_02.tpl; U.S. DEP'T OF ARMY, REG. 25-55, THE DEPARTMENT OF THE ARMY FREEDOM OF INFORMATION ACT PROGRAM para. 5-206, at app. B. (1 Nov. 1997) [hereinafter AR 25-55] (requiring that requests for current publications and records of Army field commands, installations, and organizations be sent to the "commander of the command, installation, and organization, to the attention of the FOIA Official").

[22] A FOIA request for Army records is not perfected and the time does not start until "the request arrives at the FOIA office of the Activity in possession of the records" Final Rule, *supra* note 21.

[23] 5 U.S.C § 552(a)(6)(A)(ii).

[24] AR 25-55, *supra* note 21.

[25] *Id.* § 552(a)(6)(A)(ii).

clock tolls only one time. The second circumstance that tolls the clock occurs when it is "necessary to clarify with the requester issues regarding fee assessment."[26] There is no limit to how many times the agency can ask for fee related information from a requester and as long as the request is necessary to clarify a fee related issue the clock tolls every time. For both tolling situations the tolling stops and the clock starts ticking again when the information sought is received by the agency.[27]

Although agencies have twenty working-days to respond to a FOIA request, the clock does not stop ticking on day twenty-one – it keeps ticking until the request is answered. When it ultimately stops depends upon when the agency makes a release determination and responds to the request.[28] If the FOIA Official sends out all requested documents, the clock stops when the response is placed in the mail. If information is redacted and withheld from release, however, the request and all responsive records must be sent to an appropriate denial authority for action. "Only an IDA [Initial Denial Authority], his or her delegate, or the Secretary of the Army can deny FOIA requests for DA records."[29] Until one of these officials makes a release determination regarding the withheld information, and responds to the request the clock keeps ticking. It is important to know that the actions at the installation and command level by those engaged in "street FOIA" are only part of the twenty working-day process.

OPEN Government Act of 2007 Section 8—Reporting Requirements: Just the FACTS, Ma'am

The OPEN Government Act requires the use of additional requester notification procedures and mandates agencies to capture and include more detailed data on their annual FOIA report.[30] Beginning with requests received on 31 December 2008, agencies must assign individual tracking numbers to requests that will take more than ten days to process. Agencies must also establish a phone line or internet service that requesters can use to access information about the status of their requests. New extensive breakdown of data, such as the amount of time it takes to respond to requests in twenty day increments up to 200 days, and then by 100 day increments up to 400 days; median and average number of days required to respond to all requests; number of expedited review requests and fee waiver requests, and a listing of the ten longest pending requests, must now be maintained and submitted with annual FOIA reports. To top it all off, this information and more must all be made available to the public electronically.[31]

The Army's solution to these new requirements is the Freedom of Information and Privacy Acts Case Tracking System (FACTS). "FACTS is a web-based enterprise solution . . . designed to provide uniform data collection, reporting, and worldwide tracking of Army FOIA requests."[32] It is the "official Army tracking system, and it is mandatory that all Army FOIA offices enter, track, and close their FOIA requests in FACTS beginning 1 October 2008."[33] Registration of designated FOIA personnel is highly encouraged and can be accomplished by visiting https://www.foia.army.mil/facts/newUsrRegister.asp. The new FACTS is a great tool that can ease the record keeping burden of the FOIA (and of course, its use is mandatory).

The Exemptions*: *Protecting Government Interests

The FOIA is a release statute. As such, there is a presumption that upon receipt of a valid request for government records or information, executive branch agencies will disclose and release all records that are responsive to the request. Full disclosure and release, however, may run afoul of several other governmental interests. "Among them are safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and,

---

[26] *Id.*

[27] FOIA Post, OIP Guidance: New Limitations on Tolling the FOIA's Response Time (Nov. 18, 2008), http://www.usdoj.gov/oip/foiapost/2008foiapost29.htm (providing DoJ guidance regarding the tolling of twenty working-day response period).

[28] DoJ FOIA Guide, *supra* note 8, at 93.

[29] Final Rule, *supra* note 21, para. 518.16.

[30] 5 U.S.C § 552(a)(7).

[31] FOIA Post, OIP Guidance: Assigning Tracking Numbers and Providing Status Information for Requests (Nov. 18, 2008,) http://www.usdoj.gov/oip/foiapost/2008foiapost30.htm (providing DoJ guidance regarding new tracking and data collection and reporting requirements).

[32] Memorandum from Larry Stubblefield, Deputy Admin. Assistant to the Sec'y of the Army, to Assistant Sec'y of the Army et.al., subject: Freedom of Information and Privacy Acts Case Tracking System (FACTS) (May 16, 2008); *see also* Huntoon Memo *supra* note 2.

[33] *Id.*

not least, preserving personal privacy."[34] It is for the protection of these other governmental interests that Congress included nine exemptions to the release requirement of the FOIA.[35]

Discretionary Releases: Do We or Don't We?

The question often arises whether information *must* be redacted if one of the nine exemptions applies. The simple answer is no; the FOIA allows agencies some discretion to release information that the statute otherwise exempts from mandatory disclosure.[36] The current policy of the Department of Justice (DoJ), however, does not encourage discretionary releases. Set by Attorney General Ashcroft in 2001, the policy allows agencies "to disclose information protected under the FOIA . . . only after full and deliberate considerations of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."[37] It also states that the DoJ will defend in litigation all withholding decisions "unless they lack a sound legal basis."[38] In other words, if an exemption is correctly applied, the DoJ will defend the decision. In response to Attorney General Ashcroft's policy, the DoD issued its current policy stating that discretionary releases within the DoD were "no longer encouraged."[39]

Contrast Attorney General Ashcroft's policy with the previous policy under Attorney General Reno. Attorney General Reno required, in addition to the applicability of an exemption, that it was "reasonably foreseeable that disclosure would be harmful" to an interest protected by the law, before the DoJ would defend an agency action.[40] This had the effect of encouraging discretionary releases. It is important to stay abreast of the policy, especially as 2009 arrives. A new Administration will undoubtedly issue new FOIA guidance. Keeping with previous trends it is likely that a rule similar to that under Attorney General Reno will emerge.

Any change in policy, however, will not affect the primary purpose of the FOIA or the function served by the nine FOIA exemptions. This function is the protection of the other interests involved in the decision whether to disclose government records to the public. Regardless of whether discretionary releases are encouraged or discouraged, a familiarization with all the exemptions is required if the FOIA will be properly applied. Of the nine exemptions provided for by Congress, only the first seven are routinely utilized by DoD organizations. Among these seven, however, only four are discussed below.

Exemption 1: Do Not Rely Solely on the Markings

The federal government has a significant interest in preventing the release of classified information, particularly in time of war. Exemption 1 to the FOIA protects national defense and foreign policy information properly classified pursuant to Executive order, currently Executive Order 12, 958 as amended.[41] Only national security and foreign policy records—such as those involving military plans, weapons systems, operations, intelligence activities, intelligence sources or methods, and

---

[34] Memorandum from John Ashcroft, U.S. Attorney Gen., to Heads of all Fed. Dep'ts and Agencies, subject: The Freedom of Information Act (Oct. 12, 2001), *available at* http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm [hereinafter Ashcroft Memo]. The DoJ is the executive agent for the implementation of the Freedom of Information Act. *See* 5 U.S.C. § 552(e)(6).

[35] 5 U.S.C. § 552(b) (Exemption 1: Classified information, Exemption 2: Internal personnel rules and practices, Exemption 3: Other Federal withholding statutes, Exemption 4: Certain business information, Exemption 5: Privileged agency communications, Exemption 6: Protection of personal privacy, Exemption 7: Certain law enforcement records, Exemption 8: Financial institution examination information, Exemption 9: Geological and geophysical information).

[36] These are referred to as discretionary releases. The following exemptions, however, are not appropriate for discretionary release: 1, 3, 4, 6, and 7. This leaves 2 and 5 for consideration. AR 25-55, *supra* note 21, para.1-504.

[37] Ashcroft Memo, *supra* note 34.

[38] *Id.*

[39] Memorandum from H. I. McIntyre, DoD Directorate for Freedom of Info. and Security Review for Distribution, subject: DoD Guidance on Attorney General Freedom of Information (FOIA) Memorandum (Nov. 19, 2001), *available at* http://www.dod.mil/pubs/foi/AGmemo.pdf [hereinafter McIntyre Memo].

[40] Memorandum from Janet Reno, U.S. Attorney Gen., to Heads of Dep'ts and Agencies, subject: The Freedom of Information Act (Oct. 4, 1993), *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XIV_3/page3.htm.

[41] 5 U.S.C. § 552(b)(1) (implemented by Exec. Order No. 12,958, 3 C.F.R. 335 (1996)), *as amended in* Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 28, 2003) (referred to as Executive Order 12,958 (as amended)) [hereinafter EO 12,958].

foreign government information—qualify for classification.[42] Further, only documents properly classified as Confidential, Secret, or Top Secret qualify for Exemption 1 protection.

The classification of qualified information as Confidential, Secret, or Top Secret depends upon the potential harm that will result from the information's improper release. The more significant the potential harm, the higher the security classification. Obviously, the degree of harm that could result from release of classified information varies as time passes and circumstances change. In addition, some military units may over-classify some information, particularly while deployed. Before relying upon Exemption 1, therefore, it must be determined whether the information is *properly classified* in accordance with the Executive order at the time the FOIA request is made.

Some documents may still be marked but may have already been automatically declassified.[43] Still others may appear to be eligible for continued classification but still must be reviewed. Classification markings alone are not dispositive of whether a classification is still valid. A declassification review is required to make this determination.[44]

Just as the authority to originally classify information within the Army is limited, so is the authority to review and declassify information. For this reason, appropriate officials authorized to declassify documents must be an integral part of the FOIA Team when classified information is involved. This is not to say that those authorities themselves conduct the initial review (declassification authorities are typically high-ranking officials). Like many decisions made within the military, good preliminary staff work by someone familiar with the issue will expedite the process. Judge Advocates need to reach out and find members of the staff who can conduct this preliminary work. This is critical since time to respond to a FOIA request is limited.

Judge Advocates must also be familiar with the other authorized document markings. Document markings, such as For Official Use Only, Limited Distribution, or Controlled Unclassified Information[45] do not qualify for Exemption 1 protection but they should alert the reviewer that another FOIA exemption might apply. Also, if after a declassification review is conducted, previously classified information no longer qualifies for Exemption 1 protection, other exemptions may be applicable.

Exemption 2: Rise of High Two

Exemption 2 prevents the mandatory disclosure of records that are "related solely to the internal personnel rules and practices of an agency."[46] Since the passage of the FOIA in 1966, the courts have interpreted this exemption to include two different categories of information. "Low 2" covers internal agency information that is "trivial and housekeeping in nature

---

[42] *Id.* sec. 1.4.

> Classification Categories. Information shall not be considered for classification unless it concerns: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) weapons of mass destruction.

[43] *Id*. sec. 1.5. EO 12,958 provides for automatic declassification based upon a date or event determined at the time of original classification, or upon the passage of time (ten year automatic declassification of most documents unless agency takes affirmative steps to keep classification in affect for a different amount of time up to twenty-five years).

[44] While declassification reviews can be burdensome, there are limits on how often they must be conducted. Units may rely upon a previous declassification review if conducted within two years of the FOIA request. *See* U.S. DEP'T OF DEFENSE, REG. 5200.1-R, INFORMATION SECURITY PROGRAM (Jan. 1997) [hereinafter DOD REG. 5200.1-R].

[45]

> '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 12958, 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 Dep'ts 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 controlled 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 Dep'ts, subject: Transition to New Markings for Controlled Unclassified Information (CUI) (Dec. 28, 2007).

[46] 5 U.S.C. § 552(b)(2).

for which there is no legitimate public interest or benefit to be gained by release, and it would constitute an administrative burden to process the request in order to disclose the records."[47] Examples include unit physical training rosters, office smoking policies, and holiday leave schedules. While DoD 5400.7-R, dated September 1998, states that DoD components shall not invoke low 2,[48] more recent DoD policy has rescinded this prohibition and low 2 is currently a viable option.[49]

Much more important than low 2, however, is the other half of Exemption 2. "High 2" provides authority to withhold internal agency information that would provide the means to circumvent an agency regulation or frustrate an agency function or mission.[50] This part of Exemption 2 has become increasingly more important since the start of the Global War on Terrorism and is used to protect sensitive yet unclassified information. In fact, DoD's invocation of Exemption 2 steadily increases every year – its total usage DoD-wide increasing over 130% from FY01 to FY07.[51]

Examples of high 2 information provided in DoD 5400.7-R include "operating rules, guidelines, and manuals for DoD investigators, inspectors, auditors, or examiners . . . examination questions and answers used in training course . . .[and] [c]omputer software, the release of which would allow circumvention of a statute or DoD rules, Regulations, orders, Manuals, Directives, or Instructions."[52] Courts have recently allowed agencies to protect agency research facility blueprints;[53] information concerning the design, array, structure, and construction of ammunition storage facilities;[54] aviation watch lists;[55] and unclassified rules of engagement.[56] Pursuant to the holdings of these courts and in light of current policy, sensitive items – such as rules of engagement cards, unit standard operating procedures and battle drills, and other information that would allow circumvention of security and force protection measures – should routinely be withheld from release using "High 2."

Exemption 3: How Am I Supposed to Know All Those Other Statutes?

The third exemption to the FOIA incorporates other federal statutes that have nondisclosure provisions.[57] The statute must require either "that the matter be withheld from the public in such a manner as to leave no discretion" to the agency or it must establish "particular criteria for withholding or refer to particular types of matter to be withheld."[58] A useful example is 10 U.S.C. §130b, which allows withholding of information on personnel of overseas, sensitive, or routinely deployable units. This statute protects from mandatory disclosure most personal identifying information, such as names and addresses, of servicemembers serving in those particular units. As a result, most of this information should be redacted from responsive records prior to release.

---

[47] U.S. DEP'T OF DEFENSE, REG. 5400.7-R, DOD FREEDOM OF INFORMATION ACT PROGRAM para. C3.2.1.2.2 (Sept. 1998) [hereinafter DOD REG. 5400.7-R]; *see also* Dep't of the Air Force v. Rose, 425 U.S. 352 (1976) (ruling that "low 2" applies only to information in which there is little or no public interest); Pruner v. Dep't of the Army, 755 F.Supp. 362 (D. Kan. 1991).

[48] DOD REG. 5400.7-R, *supra* note 47, para. C3.2.1.2.2.

[49] McIntyre Memo, *supra* note 39.

[50] Crooker v. BATF, 670 F.2d 1051 (D.C. Cir. 1981) (en banc) (withholding ATF surveillance manuals).

[51] In Fiscal Year 2001, DoD and its components utilized Exemption 2, 1219 times, while in FY07 the number had increased 134% to 2855 times. *See* U.S. DEP'T OF DEFENSE (DOD) FREEDOM OF INFORMATION ACT PROGRAM REPORT FOR FISCAL YEAR (FY) 2001, *available at* http://www.dod.mil/pubs/foi/01report.pdf [hereinafter DOD ANNUAL FOIA REPORT FOR FY01]; U.S. DEP'T OF DEFENSE FREEDOM OF INFORMATION ACT REPORT FOR FISCAL YEAR 2007, *available at* http;//www.dod.mil/pubs/foi/dfoipo/docs/FY2007report.pdf [hereinafter DOD ANNUAL FOIA REPORT FOR FY07].

[52] DOD REG. 5400.7-R, *supra* note 47, para. C3.2.1.2.1.

[53] Elliott v. USDA, 518 F.Supp.2d 217, 219 (D.D.C. 2007) (protecting agency research facility blueprints; records are internal because they are used for a variety of purposes by several sections within the facility; disclosure could render facility "vulnerable to potential threats and unnecessary risk in maintaining physical security").

[54] Milner v. U.S. Dep't of the Navy, No. 06-1301, 2007 U.S. Dist. Lexis 80221, at *23 (W.D. Wash. Oct. 30, 2007) (holding information concerning the design, array, structure, and construction of ammunition storage facilities is predominantly internal, notwithstanding that it was shared with local municipalities; ruling that disclosure "could provide essentially a roadmap to wreak the most havoc possible to those persons bent on causing harm").

[55] Gordon v. FBI, 388 F. Supp. 2d 1028 (N.D. Cal. 2005) (releasing aviation watch lists would allow terrorists to educate themselves and evade capture).

[56] Hiken v. DoD, 521 F. Supp. 2d 1047 (N.D. Cal. 2007) (unclassified rules of engagement eligible for protection even though the enemy may be aware of the ROE through experiences with U.S. forces in Iraq).

[57] 5 U.S.C. § 552(b)(3).

[58] *Id.*

There are many more Exemption 3 statutes, some that require the withholding of information and some that simply allow the withholding of information. The annual DoD FOIA Report lists all the Exemption 3 statutes DoD components relied upon during the report year.[59] Installation FOIA Teams should have a working knowledge of this list.

Exemption 6: Keeping Some Personal Things Private

Exemption 6 of the FOIA allows the withholding of records that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[60] "Personal and medical files" are normally easy to identify. They include Service members' Official Military Personnel Files, local unit personnel files, and military medical records. "Similar files" includes records containing any information of a personal nature.[61]

Exemption 6 protects this personal information if disclosure would constitute a clearly unwarranted invasion of privacy.[62] This determination requires the balancing of the personal privacy interest in the records against the public interest in the records. The Supreme Court 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."[63] Therefore, if the records are not informative on the operations and activities of the government there is no public interest in their release. Then if there is at least some identifiable privacy interest involved, the balance tips in favor of withholding the information.

The identification of the personal privacy interest is critical. Prior to 9/11, FOIA Officials relied upon Exemption 6 to redact some personal information, such as social security numbers and home addresses, but it was not widely used to redact names except those of victims and other individuals whose privacy interests were obvious. As a result, stateside records were not redacted like records involving those units described in 10 U.S.C. § 130b. Since 9/11, however, there is a heightened interest in the personal privacy of DoD personnel resulting from terrorist activity likely to weigh heavily in favor of protecting more personal information.[64] The result is that Exemption 6 usage has increased almost 60% since FY01 even though the overall number of FOIA requests received has actually decreased.[65]

After 9/11, the DoD issued several memoranda describing this heightened sense of privacy in the personally identifying information of those associated with DOD.[66] While these memoranda did not specifically state that names and other personal information should be automatically redacted from DoD records, they did lay the groundwork for courts to support the notion that the Exemption 6 balancing test will routinely tip in favor of personal privacy when it comes to the personal information of Service members and DoD civilian employees, particularly those of lower rank. For example, in 2006, the Federal District Court for the District of Columbia ruled that the protection of "names of civilian personnel below the level of office-director and military personnel below the rank of Colonel" in documents was valid because disclosure of those names would not shed light on the operations and activities of DoD.[67] The court also determined that it had "no reason to question" the DOD policy expressing "concern that employees of DOD could become targets of terrorist assaults."[68] The court confirmed this analysis

---

[59] *See, e.g.*, DOD ANNUAL FOIA REPORT FOR FY07, *supra* note 51, at 5–6.

[60] 5 U.S.C. § 552(b)(6).

[61] U. S. Dep't 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).

[62] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

[63] *Id.* at 775.

[64] Memorandum from D.O. Cooke, Director, Admin. and Mgmt., Office of the Sec'y of Defense, to DoD FOIA Offices, subject: Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA) (Nov. 9, 2001) [hereinafter Cooke Memo]. Since DoD personnel are at increased risk regardless of their duties or assignment, release of names and other personal information must be more carefully scrutinized and limited. Memorandum from Howard G. Becker, Deputy Dir., Admin. and Mgmt., Office of the Sec'y of Defense, to Secretaries of the Military Dep'ts et.al., subject: Withholding of Information that Personally Identifies DoD Personnel (Sept. 1, 2005) [hereinafter Becker Memo] ("In general, release of information on DoD personnel will be limited to the names, official titles, organizations, and telephone numbers for personnel only at the office director level or above, provided a determination is made that disclosure does not raise security or privacy concerns"), *available at* http://www.acq.osd.mil/dpap/pcard/Withholding_personally_identifying_information_09-01-05.pdf.

[65] In FY01, DoD and its components utilized Exemption 6 6,729 times while processing 81,682 FOIA requests; however, in FY07 the number had increased 60%, to 10,679 times in 78,392 requests. *Compare* DOD ANNUAL FOIA REPORT FOR FY01, *supra* note 51, *with* DOD ANNUAL FOIA REPORT FOR FY07, *supra* note 51.

[66] Cooke Memo, *supra* note 64; Becker Memo, *supra* note 64.

[67] Kimmel v. DOD, No. 04-1551, 2006 WL 112682 (D.D.C. Mar. 31, 2006)

[68] *Id.* at 10–11.

as late as August 2008 when it upheld the withholding of names of Air Force personnel below the office director level amid post-9/11 security concerns and the fact that revealing names would not shed any light on the Air Force's performance of its statutory duties.[69]

Following this trend, it appears that the privacy interest of DoD personnel in their personally identifiable information will often outweigh the public's interest in knowing that information, particularly when dealing with lower ranking personnel. Those reviewing records for release should be familiar with the balancing test and ensure it is applied with the post 9/11 heightened security and personal privacy interests in mind. The result should be that most personal information qualifies for redaction.

Conclusion: Managing FOIA—OK, Maybe Not a Village but Certainly a Team

With so many FOIA requests to respond to and an expanding list of FOIA requirements to address, the Army relies upon FOIA Teams at installation and command levels to implement the Army FOIA program. To satisfy the new requirements of the OPEN Government Act of 2007 and in order to correctly apply FOIA exemptions to the current situation within DoD, FOIA Teams must stay up to date on changes to the FOIA and the way it is implemented. The OPEN Government Act imposed several new procedural requirements, chief among them involve attorney fees and litigation costs, time limits, and annual reporting requirements. And while the FOIA exemptions have not changed recently, the way they are applied has changed, most notably Exemptions 2 and 6. Undeniably, there are a lot of requirements imposed by the FOIA and meeting the requirements, particularly the response time requirement, is often difficult. Certainly, one person cannot do it. Fortunately, one person does not have to do it because although it probably does not really take an entire village, hopefully there is a FOIA Team, properly trained and supported, available to do the job.

[69] Schoenman v. FBI, No. 04-2202, 2008 U.S. Dist. LEXIS 64833 (D.D.C. Aug. 25, 2008; *see also* Cochran v. United States, 770 F.2d 949 (11th Cir. 1985) (holding that adverse information on high ranking official (major general) found guilty at disciplinary hearing of wrongful appropriation of government aircraft and improper use of government facilities and manpower "qualifies as a textbook example of information the FOIA would require to be disclosed. According to the court, the public interest in disclosure of information relating to a violation of the public trust by a senior government official was overwhelming and outweighed MG Cochran's right to privacy); Schmidt v. U.S. Air Force, No. 06-3069, 2007 U.S. Dist. Lexis 69584 (C.D. Ill. Sept. 20, 2007) (holding that the Air Force properly released adverse information on pilot (major) involved in friendly fire mishap in Afghanistan that resulted in the deaths of several members of the Canadian Army. While the pilot had a privacy interest in maintaining the confidentiality of the information, this privacy interest was outweighed by the public interest in disclosing information about the highly publicized incident (the incident garnered significant public and media attention, was a deadly incident, and had international effects.) The information gave the public "insight into the way in which the United States government was holding its pilot accountable.")