



DEPARTMENT OF THE NAVY

OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

SECNAVINST 5720.42G
OCIO
15 Jan 2019

SECNAV INSTRUCTION 5720.42G

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY FREEDOM OF INFORMATION ACT PROGRAM

Ref: (a) 5 U.S.C. §552
(b) 10 U.S.C. §1102
(c) 10 U.S.C. §130e
(d) 44 U.S.C. §3506
(e) DoD Directive 5400.07 of 2 January 2008
(f) 32 CFR 286
(g) DoDM 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information of 24 February 2012
(h) DoDM 5400.07, DoD Freedom of Information Act Program of 25 January 17
(i) E.O. 13392
(j) SECNAVINST 5215.1E
(k) SECNAVINST 5430.7R
(l) UNSECNAV memo of 14 May 2012 (NOTAL)
(m) OPNAVINST 3750.6 (Series)
(n) OPNAVINST 5102.1D
(o) MCO P5102.1B
(p) JAGINST 5800.7 (Series)

Encl: (1) Responsibilities
(2) Processing Requests
(3) FOIA Appeals
(4) Handling Classified Records
(5) Review Process for 10 U.S.C. §130e, Department of Defense Critical Infrastructure Security Information
(6) Definitions

1. Purpose. This instruction implements reference (a), the Freedom of Information Act (FOIA), references (b) through (d), as authorized by reference (e), and per related law and practice, notably as promulgated in references (f) through (l).

2. Summary of Changes. References (f) through (h) shall serve as the primary guidance for the Department of the Navy (DON)

FOIA program, supplemented by this instruction and the DON FOIA Policy website. Commanders and commanding officers bear primary responsibility for FOIA compliance, including adequate provision of resources and cooperation with DON FOIA program offices, namely: the Chief Information Officer, Senior FOIA Official for the DON; the head of FOIA Program Execution for the Navy (DNS-36); and the head of FOIA Program Execution for the Marine Corps. Applicability of reference (c) (i.e., Defense Critical/Critical Infrastructure Security Information) requires prior consultation with the Office of the Chief Information Officer (OCIO) and a determination by the Office of the Secretary of Defense.

3. Cancellation. SECNAVINST 5720.42F.

4. Applicability. This instruction applies to all DON personnel and offices, including the Office of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and their respective installations, commands, activities, and field offices within the DON.

5. Policy. It is DON policy that:

a. The DON shall fulfill, as integral to its mission, the requirements and purposes of the FOIA, including all executive orders and all policy and guidance set forth in Department of Defense (DoD) and DON written communications;

b. References (f) through (h) implement the FOIA throughout the DoD. These references shall serve as the primary guidance for the DON FOIA program. This SECNAV instruction supplements those references by addressing topics of particular importance to the DON, notably the unique elements of its organization, practice, and records. This instruction is in turn supplemented by the DON FOIA website.

6. Responsibilities. See enclosure (1).

7. Processing FOIA Requests. See enclosures (2) through (5).

8. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD)

portal page:

<https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx>.

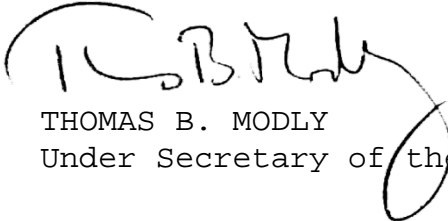
b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

9. Forms and Reports

a. FOIA program forms are available at Naval Forms Online (<https://navalforms.documentservices.dla.mil/web/public/home>) as well as the DON FOIA policy website. DD 2086 (Record of Processing Cost) and DD 2086-1 (Record of Processing Cost for Technical Data) are available on the DoD issuance website (<https://www.esd.whs.mil/DD/>). SF 180 (Request Pertaining to Military Record) is available on the standard forms website (<https://www.opm.gov/forms/standard-forms/>). Additional guidance is available at the DON FOIA website (see "Definitions," enclosure (6)).

b. The requirements contained in enclosure (1) paragraph 21 and 5g are assigned reports control symbol DD-CMO(A)1365.

10. Conflicts. To the extent there are any conflicts between this instruction and the DoD FOIA instructions, the DoD instructions shall control.



THOMAS B. MODLY
Under Secretary of the Navy

Distribution:

Electronic only, via Department of the Navy Issuances website
<http://doni.documentservices.dla.mil>.

RESPONSIBILITIES

1. All Commands and Activities. FOIA is a statutory obligation that is integral to the mission of the DON. All DON commanders, commanding officers, and activity heads bear primary responsibility for FOIA compliance. Accordingly, they must ensure availability of resources sufficient to meet all FOIA deadlines under the law for their respective commands, including manning, training, equipment, information technology, access to records (both unclassified and classified), and administrative support. FOIA compliance includes requiring use of FOIA online to process and track all FOIA requests, consultations, and appeals. A command or activity that processes few FOIA requests may receive assistance from its Immediate Superior in Command (ISIC) or another DON FOIA office in the discharge of these duties, but shall retain full responsibility for FOIA compliance. Every decision to deny a FOIA request must be made by a duly authorized Initial Denial Authority (IDA) (see below). Commanders, commanding officers, and activity heads shall ensure complete cooperation with the principal offices of the DON FOIA program, specifically:

a. The OCIO, which has overarching authority for FOIA policy for all commands and activities;

b. SECNAV/CNO FOIA/Privacy Act Program Office, DNS-36 for Navy commands and activities;

c. The Director, Marine Corps Staff, Administration and Resource Division (HQMC-ARSF), for Marine Corps commands and activities;

d. DON Appellate Authorities, for appeals, see enclosure (3).

2. Chief Information Officer (CIO) is the Senior FOIA Official for the DON. The OCIO shall:

a. Set DON FOIA Program policy for procedures, education, training, and awareness;

b. Serve as principal policy advisor on all FOIA matters;

c. Oversee the administration of the DON's FOIA Program;

d. Serve as DON FOIA Public Liaison;

e. Coordinate with DNS-36 and HQMC-ARSF to post to the DON FOIA Policy website key guidance and "hot topics" (topics of recurring interest);

f. Develop and maintain DON FOIA-related electronic activities intended for the administration or furtherance of the DON FOIA program. This shall include managing the DON FOIA Policy website (see enclosure (6)) and ensuring that online guidance is available concerning DON FOIA program matters that are not specifically addressed by the DoD FOIA manual, (see reference (e)), or this instruction;

g. Coordinate self-inspection of DON FOIA programs by field offices in conjunction with DNS-36 and HQMC-ARSF. Develop and disseminate a compliance checklist to facilitate the inspection process;

h. Oversee participation in FOIA online, which is mandatory for all DON FOIA activities;

i. Coordinate and prepare responses and reports to DoD regarding FOIA issues;

j. Ensure the DON FOIA program complies with all laws and regulations pertaining to FOIA as may from time to time be enacted, amended, or published. This duty includes ensuring the review of all applicable forms, which shall be made available via the DON FOIA website (see enclosure (6)), reviewing SECNAV instructions that address FOIA or FOIA-related matters, determining all DON FOIA policy, and overseeing publications;

k. Represent the DON at meetings, symposia, and conferences regarding FOIA matters;

l. Review, compile, and submit reports to DoD that address FOIA issues, including the DON Annual FOIA Report, the DON Annual Chief FOIA Officer Report, and quarterly reports, in conjunction with DNS-36, HQMC-ARSF, and field offices as needed;

m. Review and disseminate information to stakeholders on proposed FOIA legislation that has potential to affect the DON;

n. Coordinate with DNS-36 and HQMC-ARSF to determine whether a request is "high visibility" or "significant" as defined by the DoD;

o. Conduct in-person staff-assistance visits for the purpose of program evaluations at commands and activities to ensure FOIA compliance;

(1) At least one such staff visit shall be completed annually;

(2) Staff assistance visits and program evaluations will be conducted across a broad range of commands over time;

(3) Geographic separation indicates a special need for staff-assistance visits and program evaluations.

p. Review and submit to the Office of the Secretary of Defense all requests in need of a determination of the applicability of reference (c) (i.e., the statute that governs the Defense Critical Infrastructure Security Information/Critical Infrastructure Security Information (see enclosure (5))).

3. DNS-36 and HQMC-ARSF. DNS-36 and HQMC-ARSF are responsible for execution of their respective Services' FOIA programs. DNS-36 serves the CNO/OPNAV and the SECNAV, including the Department of the Navy/Assistant for Administration (DON/AA) and the OCIO. HQMC-ARSF serves the CMC. DNS-36 and HQMC-ARSF shall each:

a. Serve as the primary FOIA Requester Service Center (RSC) for the Navy and the Marine Corps, respectively. Establish additional FOIA RSCs at their respective subcomponent activities as necessary;

b. Implement this instruction for the Navy and Marine Corps, respectively;

c. Provide program support and oversight for their respective FOIA coordinators and specialists;

d. Maintain a current list of FOIA coordinators at their respective subcomponent activities, which:

(1) Identifies the FOIA coordinator, mailing address, email address, and telephone number, unless the release of such information raises the prospect of foreseeable harm (e.g., it could endanger personnel assigned to overseas, sensitive, or routinely deployable units); in such a case, the generic term "FOIA Coordinator" and a general office email address and

telephone number shall be provided.

(2) Is published to the DON FOIA Policy website and updated annually.

e. Manage and maintain their respective FOIA processing activities, including coordinators and customer Service agents;

f. Serve as the senior FOIA coordinator and program manager for their respective Services: in the case of DNS-36, at the Secretariat and at OPNAV; in the case of HQMC-ARSF, at the Headquarters of the Marine Corps. In this role, both DNS-36 and HQMC-ARSF shall manage FOIA request processing to ensure all responses are complete, timely, and accurate;

g. Provide complete, timely, and accurate responses to queries from the Public Liaison;

h. Assist the OCIO in promoting the DON FOIA program;

i. Review their respective Service instructions and forms addressing the FOIA or FOIA-related matters, review proposed legislation and policy recommendations that may affect their respective FOIA programs or this instruction, and provide recommended changes or comments to the OCIO;

j. As needed, compile, review, and submit FOIA program reports on their respective FOIA programs to the OCIO;

k. Coordinate with the OCIO and the Chief of Information on all potential "high visibility" or "significant" FOIA requests as defined by the DoD or the OCIO. Provide all records of high public interest (i.e., subjects of "hot topics" requests) to the rest of the DON as appropriate, for use outside of one's respective Service within the DON (e.g., DNS-36 and HQMC-ARSF need to keep each other apprised) and for posting on applicable FOIA libraries, redacted as appropriate;

l. Conduct at least one FOIA inspection annually in their respective Services; ensure that Navy and Marine Corps commands conduct annual FOIA self-inspections using checklists provided on the DON FOIA Policy website (see "Definitions," enclosure (6)); submit the results of all such inspections to the OCIO, along with their input for the Chief FOIA Officer Report;

m. Ensure all FOIA specialists have met their training

requirements as prescribed by the OCIO and that general FOIA awareness training is provided to all command and activity personnel. DNS-36 and HQMC-ARSF shall provide a report on their respective compliance with these requirements along with their input for the Chief FOIA Officer Report;

n. Coordinate with the OCIO the preparation, review, and submission of all DON requests from the field that implicate reference (c). See enclosure (5);

o. Ensure full participation of their respective Services FOIA programs in FOIA online.

4. Echelon II FOIA Coordinators. (Note on "Echelon" terminology: "Echelon I" is a Navy term that refers to the Office of the Chief of Naval Operations (OPNAV); for the Marine Corps, the equivalent is Headquarters, Marine Corps (HQMC). All commands that report directly to Echelon I are considered to be Echelon II). All Echelon II FOIA coordinators shall:

a. Serve as the primary FOIA RSCs for their own commands and subordinate commands. Establish additional FOIA RSCs at their respective subcomponent activities as necessary;

b. Ensure full compliance by their own commands and subordinate commands with DON FOIA policy and guidance, including the duties of command and activity-level FOIA coordinators, as set forth in paragraph 5, below;

c. If needed and not available through FOIA online, collect and compile command and feeder reports, and submit consolidated annual FOIA reports to DNS-36 and HQMC-ARSF;

d. Maintain and update listings of subordinate command and activity FOIA coordinators, including full name, address, and telephone (office and fax) on their public websites. For personnel in overseas, sensitive, or routinely deployable units, "FOIA Coordinator" may be used in place of an individual's full name;

e. Ensure FOIA personnel have met training requirements as prescribed by OCIO.

f. Conduct annual staff assistance visits, reviews, or self-evaluations within the command and lower echelon commands to assist the OCIO in ensuring FOIA compliance;

g. Ensure the full participation of their own commands and subordinate commands in FOIA online. Full participation includes providing all input to FOIA online necessary to ensure complete tracking and data availability for all mandated FOIA reports, specifically by:

(1) Entering into FOIA online all requests immediately upon receipt (manually by the FOIA personnel if not submitted directly into the system by the requester);

(2) Promptly completing all pertinent fields on FOIA online, including fees, whether perfected, dispositions, exemptions, and appellate authority, as applicable;

(3) Adding comments to FOIA online with sufficient detail to ensure up-to-date progress tracking (Note: to avoid needless duplication of effort, it is strongly recommended that FOIA online alone be used for such purposes);

(4) Uploading to FOIA online all response letters;

(5) Closing all cases promptly when processing is complete;

(6) When appropriate, promptly referring all cases within FOIA online to other activities that are served by FOIA online;

(7) Posting responsive documents provided to requesters on FOIA online and other websites, as appropriate. See enclosure (4).

h. Ensure all components provide links on their websites to the FOIA webpages of their respective Services, commands, and activities, to include the website of FOIA online and that of the DON FOIA Policy website (see "Definitions," enclosure (6)).

5. Command and activity-level FOIA coordinators shall:

a. Act on behalf of, and with authority vested by, their respective commanders, commanding officers, and activity heads;

b. Implement and administer local FOIA programs per this instruction;

c. Serve as principal point of contact on FOIA matters

within and concerning their commands and activities;

d. Receive and track FOIA requests to ensure responses are made in compliance with this instruction;

e. Provide general awareness training to command and activity personnel on the provisions of reference (a) and this instruction;

f. If needed, provide guidance to command and activity personnel on how to process FOIA requests and on the scope of FOIA exemptions;

g. Collect and compile FOIA statistics and submit annual FOIA reports to the respective Echelon II FOIA coordinator for consolidation if required and if not available through FOIA online;

h. Ensure full participation in FOIA online. Full participation is discussed in paragraph 4f, above;

i. Maintain links on the websites of their respective commands or activities to the FOIA RSC webpages of their respective Services.

6. IDAs. Every denial of a FOIA request must be made by a duly authorized IDA, who is generally responsible for ensuring payment of all costs incurred in FOIA litigation, including attorney fees. Accordingly, IDAs should familiarize themselves with the FOIA by taking an introductory course, typically no more than an hour in length, that is available online (see DON FOIA Policy website). An IDA should be a DON employee of a paygrade commensurate to at least O-4 or GS-12. The below-listed IDAs are authorized to delegate initial denial authority to subordinate activities for the purpose of streamlining FOIA processing or complying with FOIA time limits. To that end, they may delegate authority to a specific staff member, assistant, or individuals acting during their absence. Such delegations shall be limited to comply with reference (b), and should be to persons of a paygrade of least O-4 or GS-12. In deciding whether to delegate, it is imperative to ensure that not only speed and efficiency are addressed (a reason to delegate), but also uniformity in decision-making by the IDAs (a reason to limit delegation). Delegations of IDA authority should be reflected in the activity's supplementing FOIA instruction or by letter, with copies to OPNAV (DNS-36) or HQMC

(HQMC-ARSF), as appropriate. Initial denial authority must be exercised independently, not "by direction." DNS-36 and HQMC-ARSF retain the right to revoke any such delegation within their respective Service as appropriate.

a. The following officials possess IDA:

(1) On behalf of the SECNAV, all DON secretaries (i.e., the Under Secretary of the Navy, Deputy Under Secretary, and Assistant Secretaries, etc.);

(2) Within the Navy, each of the following officials, as well as their deputy or principal assistant:

(a) CNO;

(b) Vice CNO;

(c) Head, DNS-36;

(d) All Deputy CNOs;

(e) All heads of Echelon I and II components;

(3) Within the Marine Corps, each of the following officials, as well as their deputy or principal assistant:

(a) CMC, Assistant CMC, and Deputy Commandants;

(b) Head, HQMC-ARSF;

(c) Staff Judge Advocate to the Commandant;

(d) Legislative Assistant to the Commandant;

(e) Counsel for the Commandant;

(f) Director of Intelligence;

(g) Inspector General of the Marine Corps;

(h) All commanding generals;

(4) All officers authorized by Article 22, Uniform Code of Military Justice, or designated in section 0120, Manual of the Judge Advocate General (reference (p)), to convene general

courts-martial.

b. The Judge Advocate General (JAG), the General Counsel of the Navy (GC), and their deputies may not exercise IDA themselves because they serve as appellate authorities. However, they may delegate this authority to other senior officers or officials under the JAG or the GC, including, if appropriate, DNS-36. Accordingly, the following delegations have been made:

(1) The GC to the Assistant General Counsels and the Associate General Counsel (Litigation);

(2) The JAG to the Office of the Judge Advocate General (OJAG) Division Directors/the Deputy Assistant JAG.

7. Release Authority. This term refers to authority to grant, on behalf of the SECNAV, requests for agency records in one's possession. The possessor of a record has such authority, but only in coordination with the FOIA office responsible for management of the request or portion of the request related to the record(s) at issue, or ISIC. A FOIA office not responsible for a particular FOIA request or portions thereof shall not communicate with a requester about the request other than to refer the requester to the properly cognizant office. Thus, if one does not own a record, one may release it only with the express permission of the record's owner, a FOIA program headquarters office, or one's ISIC. Exercise of Release Authority also implies the duty to render the following Services, in coordination with a FOIA office, as appropriate:

a. To reach agreements with requesters to clarify or modify their requests;

b. To provide fee estimates;

c. To provide appeal rights to requesters concerning adequacy of search or fee estimates.

8. Alternative Dispute Resolution Services

a. The Office of Government Information Services (OGIS) provides a voluntary mediation process for resolving disputes between persons making FOIA requests and the DON. For additional information, see enclosure (6).

b. The OCIO, as Office of the Chief FOIA Officer of the

15 Jan 2019

DON, serves as the primary agency liaison with OGIS, and shall designate one (1) or more FOIA Public Liaisons. The liaison shall be available to assist in the resolution of disputes. Contact information for DoD Component FOIA Public Liaisons, including the FOIA Public Liaison for DON, is available at <http://www.foia.gov/report-makerequest.html>.

PROCESSING REQUESTS

Note: For updates, see the DON FOIA Policy website (see enclosure (6)).

1. Processing FOIA requests, generally:

a. All correspondence with a FOIA requester must include the FOIA online request tracking number;

b. All transfers within the DON must be conducted through FOIA online. In any instance in which a DON activity is unable to process a FOIA matter in FOIA online, it must work with its ISIC to ensure this requirement is satisfied. A DON activity transferring a FOIA request to another activity must confirm the transfer with the other activity and provide the requester the following information:

(1) The tracking number of the request, including the new number(s) assigned in cases of partial referral(s);

(2) The point of contact information for the activity to which the request has been referred; specifically, name, email address, and telephone number.

c. Use FOIA online for all requests: A request submitted by means other than FOIA online (e.g., by mail, email) shall be promptly entered into FOIA online and an acknowledgement sent to the requester, unless the request was not submitted to a FOIA RSC, in which case rerouting the request shall be accomplished within 10 working days.

d. Required requester contact information: Per reference (d), the requester is required to provide contact information, such as an email address, a mailing address, or a telephone number. Failure to comply with this requirement is grounds to refuse the request or to close it as improper.

e. Responses to requests: The IDA shall inform the requester of the final decision to grant or deny the request, in whole or in part, by a written communication ("final notice"). In the case of any denial, this communication shall include:

(1) The signature of the responding IDA, accompanied by the official's name, duty title, and contact information;

(2) The name and contact information of the DON FOIA Public Liaison, the OGIS, or any other public liaison or mediation Service as appropriate, with an advisory as to the availability of such voluntary mediation;

(3) An explanation of the basis for denial, with sufficient detail to permit a reasonable FOIA requester to decide whether to make an appeal. Such details shall include:

(a) An identification of any exemption applied. When applying FOIA exemption (3) (the statutory exemption), the response letter shall also cite the particular statute that is being applied. In the case of Defense Critical Infrastructure Security Information (also called Critical Infrastructure Security Information), see enclosure (5);

(b) A brief explanation of each exemption applied and the reason why each is warranted.

(4) A brief explanation of any search conducted, including locations and keywords, if used;

(5) An appeal advisory that shall include:

(a) Notification that the requester may appeal the denial;

(b) Identification of the appropriate appellate authority;

(c) Instructions on how to make an appeal through FOIA online and, as an alternative, through the mail, for which the appropriate address should be provided;

(d) The deadline by which an appeal must be submitted, i.e., within 90 calendar days of the date of the final notice, where "submitted" means:

1. Transmitted if appealing by FOIA online;
2. Postmarked if appealing by mail.

(e) An advisory that the requester has the burden of proving timely submission;

(f) Notification that the FOIA requester should provide the following documentation as part of the written appeal:

1. Required: An explanation why the appeal should be granted;

2. Encouraged: A copy of the initial FOIA request (if not submitted directly through FOIA online);

3. Encouraged: A copy of the denial letter.

(6) If readily available, an estimate of the volume of records being denied, unless providing such an estimate would harm an interest protected by a FOIA exemption. This estimate should be expressed in number of pages or other reasonable terms. For redaction, if feasible, the IDA must annotate the pertinent section with the exemption applied.

(7) Whether or not fees are assessed, the FOIA processor shall provide the requester the following information in the final response letter:

(a) The FOIA requester's fee category; and

(b) If fees are assessed, a complete breakdown of costs.

(8) Interim release. To avoid delay, a FOIA processor may provide the requester an interim release. To be an interim release, the release must be identified as such in a written communication to the requester that provides an estimated date of completion for the final release. Such requests and responsive records that are denied shall be retained by the IDA and the appellate authorities per the current records retention policy.

2. Proactive posting. All FOIA processors are strongly encouraged to post all records provided in response to FOIA requests on their websites and on FOIA online. Such a practice

promotes transparency, a main goal of the FOIA. In addition, it should reduce the workload for FOIA processors by making repeated individual responses unnecessary. It is mandatory to post any records that have been requested three times (the "Rule of Three"). The DON recommends, but does not require, a "Rule of One," i.e., post material upon being requested once, since this would eliminate the need under the Rule of Three for tracking the number of requests.

3. Special considerations for processing certain types of DON records: A DON activity that receives a request for any of the following kinds of records shall promptly forward the request to the appropriate FOIA official and notify the requester of this action:

a. Court-Martial Records of Trial. The IDA for these records is the Office of the Judge Advocate General (Code 20), 1254 Charles Morris Street SE, Suite B01, Washington Navy Yard, DC 20374;

b. Judge Advocate General Manual (JAGMAN) Investigative Records. These records are no longer centrally processed. Accordingly, requests for JAGMAN investigation records should be directed to the following officials (using the mailing address only if unable to use FOIA online):

(1) For investigations conducted prior to January 1, 1996: the Judge Advocate General (Code 15), 1322 Patterson Avenue, SE, Washington Navy Yard, DC 20374;

(2) For investigations conducted thereafter, to the command that conducted the investigation. If, for investigations conducted after January 1, 1996, the command has already archived the investigation, it will request return of the file via Code 15;

(3) For Litigation Report Investigations, to the Judge Advocate General (Code 15), 1322 Patterson Avenue, SE, Washington Navy Yard, DC 20374;

(4) For reports of courts or boards of inquiry, to the General Court Martial Convening Authority over the command that convened the investigation;

(5) For admiralty letter reports or admiralty dual-purpose investigations, to the Judge Advocate General (Code 11), 1322 Patterson Avenue, SE, Washington Navy Yard, DC 20374.

c. Mailing Lists: When dealing with requests for mailing lists of Service Members, refer to the most recent DoD policy and instruction for guidance. See references (c) through (e);

d. Medical Quality Assurance Documents. The Chief, Bureau of Medicine and Surgery (BUMED), is the IDA for all naval medical quality assurance documents as defined by reference (b) and requests for those documents shall be promptly referred to BUMED and the requester notified of the referral;

e. Mishap Investigation Reports. See Safety Investigation Reports below;

f. Naval Attaché Documents and Information. The Director, Defense Intelligence Agency (DIA), is the release or denial authority for any naval attaché-originated documents or information. FOIA requests for naval attaché documents located in DON files or referred in error to a DON activity shall be promptly referred to DIA for action and direct response to the requester. Notify the requester in writing of the transfer to DIA;

g. Naval Audit Service Reports. The Director, Naval Audit Service, is the IDA for Audit Service reports. All applicable requests or documents shall be promptly referred for action to the Director, Naval Audit Service, Attn: FOIA, 1006 Beatty Place SE, Washington Navy Yard, DC 20374-5005. The requester shall be notified of the referral;

h. Naval Criminal Investigative Service (NCIS) Reports. The Director, NCIS, is the IDA for all NCIS reports and information as well as for records stored and maintained by NCIS that originated at other DON commands. If NCIS receives a request for non-NCIS-originated records concerning a "high visibility" or sensitive matter, NCIS shall notify DNS-36 or HQMC-ARSF, as appropriate, who may then request return of the records for originator release. Criminal Investigation Division reports are maintained locally for two years after case closure, at which time they are destroyed while the originals are maintained at NCIS. During the holding period, the original IDA

retains release or denial authority. All requests for and copies of NCIS reports located in DON activity files shall be promptly referred to the Naval Criminal Investigative Service, Attn: FOIA (Code 00LJF), 27130 Telegraph Road, Quantico, VA 22134 for action and, if appropriate, the requester so notified. Telephonic liaison with NCIS Headquarters is strongly encouraged;

i. Naval Inspector General (NAVIG) Records

(1) The NAVIG is the IDA for all DON Inspector General (IG) records and other DON records that pertain to IG records.

(2) The NAVIG may delegate authority to others within the Office of the Naval Inspector General (NAVINSGEN), or to other IDAs within the DON, on a categorical or case-by-case basis, as the NAVIG deems appropriate. Within NAVINSGEN, the Deputy Naval Inspector General/Inspector General of the Marine Corps (DNIG/IGMC) and HQMC-ARSF are delegated categorical and case-by-case release or denial authority for IGMC records and other pertinent DON records;

(3) In the absence of a written categorical delegation of authority, any DON office or activity holding a record subject to the NAVIG's release or denial authority shall promptly coordinate with the NAVIG or DNIG/IGMC to determine to which office or activity to assign the request. The transferring office or activity shall notify the requester of the transfer.

j. Naval Nuclear Propulsion Information (NNPI). The Director, Naval Nuclear Propulsion Program, CNO (N00NB)/Naval Sea Command (08) is the IDA for all information and requests concerning NNPI. Naval activities receiving such requests are responsible for searching their files for responsive records. If no pertinent documents are located, the naval activity shall respond to the requester and provide CNO (N00NB) with a copy of the request and response. The activity shall refer the request, any responsive documents, and a recommendation regarding release to CNO (N00NB), 2000 Navy Pentagon, Washington, DC 20350-2000, who will make the release determination to the requester;

k. Naval Telecommunications Procedures (NTP) Publications. Refer all requests for NTP Publications to the appropriate IDA,

the Commander, Fleet Cyber Command, at 9800 Savage Road, Suite 6586, Ft. George G. Meade, MD 20755-6586;

l. News Media Requests: All DON activities shall treat a FOIA request from the press as they would a request from any other source, except that when a request is received from a member of the press, the activity should notify the appropriate public affairs office (e.g., Navy Chief of Information for the Navy, and Office of Marine Corps Communications for the Marine Corps). Only notification to, not approval from, public affairs officers is expected. Public affairs considerations do not form a legitimate basis for withholding information under the FOIA;

m. Safety Investigation Reports and Hazard Reports. The Commander, Naval Safety Center (NAVSAFECEN), is the IDA for all requests concerning:

(1) Mishap investigations or documents containing mishap information, except for the corresponding JAGMAN investigations. All requests and responsive documents shall be promptly referred to the Commander, Naval Safety Center, Code 503, 375 A Street, Norfolk, VA 23511-4399 for action. Telephone calls to NAVSAFECEN (at 757-444-3520 ext. 7047) are encouraged. The requester shall be notified of the referral;

(2) Safety information generated per reference (m) through (o), including investigations, hazard reports, or data extracted from any database under the control of the Naval Safety Center. All requests for such information shall be immediately referred to the Commander, Naval Safety Center, Attn: Code 023, 375 A Street, Norfolk, VA 23511 for action. Telephone calls or emails to discuss such requests are encouraged. The NAVSAFECEN FOIA Office can be contacted at 757-444-3520 extension 6055, or via email at safe-FOIA@navy.mil.

FOIA APPEALS

Note: For updates, see the DON FOIA Policy website (see enclosure (6)).

1. FOIA Appellate Authority. The SECNAV has authority to act on all appeals of decisions on FOIA requests as follows:

- a. To release or withhold records, or portions thereof;
- b. To waive or reduce fees;
- c. To remand matters to the IDAs;
- d. To direct release or withholding of information requested under the FOIA;
- e. To make final decisions on appeals under the FOIA.

2. Delegation. The SECNAV has delegated FOIA appellate authority to JAG and GC, according to subject matter cognizance (see below). In turn, the JAG and the GC have delegated this authority respectively as follows:

- a. The JAG to:
 - (1) The Assistant JAG (Civil Law);
 - (2) The Deputy Assistant JAG (General Litigation)/Director, General Litigation Division (Code 14);
- b. The GC to:
 - (1) The Principal Deputy General Counsel (PDGC);
 - (2) The Deputy General Counsel (DGC);
 - (3) The GC, PDGC, and DGC may further delegate FOIA appellate authority as they deem appropriate for efficient processing of appeals. Such re-delegation must be in writing and specify the extent of authority re-delegated. The DON GC has previously delegated authority for all litigation within the GC's cognizance to the Associate General Counsel (Litigation).

3. Cognizance of the GC and the JAG. When in doubt, the JAG has cognizance. Otherwise, appeals are to be divided between the DON GC and the JAG per their subject matter as follows:

a. The GC: Generally all matters unrelated to military law (see JAG below), specifically, those related to business and commerce, real and personal property, intellectual property, fiscal questions, civilian personnel, labor relations, and the environment (unless the matter arises in the context of operations);

b. The JAG: Military law and all matters not delegated to the GC above.

4. Responsibilities of Appellate Authority include

a. Serving as principal points of contact on the DON FOIA appeals and litigation, and coordination of litigation of FOIA matters with the appropriate field offices;

b. Receiving and tracking FOIA appeals and ensuring responses are compliant with all applicable law and regulations;

c. Completing responsive portions of the Annual FOIA Report that address actions on appeals and litigation costs during the fiscal year and submitting that information to the OCIO;

d. Providing the OCIO, the pertinent IDA, and, as appropriate, DNS-36 or HQMC-ARSF, copies of all appeal determinations as they are issued.

5. Action by the Appellate Authority

a. Communication with the IDA. Upon receipt, the appellate authority will promptly notify the IDA of an appeal as follows:

(1) Within 10 working days, the IDA shall respond and provide the appellate authority the following documents, if not entered into FOIA online, so that a determination can be made:

(a) A copy of the request;

(b) Responsive records, if any, both redacted and unredacted (or with redactions highlighted);

(c) A copy of the denial letter;

(d) A memorandum setting forth the IDA's analysis and rationale for the original decision.

(2) The appellate authority retains authority to request a declassification review of any classified document by the original classification authority (OCA) or, if unable to determine the OCA, by another appropriate classification authority.

b. Notification to the appellant. Once an appeal is adjudicated, and if the decision is adverse to the appellant, the appeal authority shall inform the appellant of the right to seek judicial review. If the appellant seeks judicial review at any time during the FOIA proceedings, any subsequent responses to the appellant shall be coordinated with the Department of Justice (DOJ) through the assigned Navy litigation counsel.

6. Addresses for Filing Appeals. Appeals should be submitted to the office with appropriate cognizance (either that of the JAG or the DON GC, see below), using FOIA online (the preferred method), email, or mail. The default address is that of the JAG, Code 14.

a. Judge Advocate General (Code 14), 1322 Patterson Avenue SE, Suite 3000, Washington Navy Yard, DC 20374-5066;

b. Office of the General Counsel, Department of the Navy, Freedom of Information Act Appeals Office (5A532), 1000 Navy Pentagon, Washington, DC 20350-1000.

7. Consultation and Coordination

a. The Director of the NCIS, in his or her role as Special Assistant for Naval Investigative Matters and Security to the CNO, may be consulted to resolve inconsistencies or disputes involving classified records;

b. Direct liaison with officials within the DON and other interested Federal agencies is authorized at the discretion of the appellate authority, who also coordinates with appropriate DoD, DOJ, Navy Chief of Information, or DON GC officials as appropriate.

8. Denying an Appeal. The appellate authority must provide the appellant a final disposition communication that decides the appeal with a reason for the decision. In all instances, the final denial letter shall contain the name and title of the official responsible for the denial and advise the requester of the right to seek judicial review. The final denial letter constitutes the final agency decision of the DON for the purposes of the FOIA. When a letter invokes FOIA exemption (1) because classified information is withheld, it should explain that a declassification review was undertaken (if it was undertaken), that the information cannot be released, and that information denied does not contain meaningful portions that are reasonably segregable.

9. Granting an Appeal. The appellate authority must render a decision in writing. When an appellate authority decides to release or direct the release of all or a portion of records withheld by an IDA, copies of the releasable records shall be promptly forwarded to the requester. The appellate authority may comply with this requirement by directing the IDA to make appropriate releases. In addition, the appellate authority may grant an appeal by remanding the case to the IDA with specific directions to address IDA actions that were not taken but should have been, e.g., conducting an appropriate segregability analysis.

10. Processing Appeals Made Under Privacy Act and the FOIA. An appeal under the FOIA suffices for issues involving the Privacy Act.

11. Time Limits and Requirements

a. Deadline. A FOIA appeal must be postmarked or electronically submitted to an office designated to receive FOIA appeals within 90 calendar days of the date of the IDA's final notice. In the event an appeal is lost, misdirected, or does not arrive at the OJAG or GC appellate office within the time allowed, the requester bears the burden of proving timely postmark or electronic submission;

b. Misdirected Appeal. A FOIA appeal sent to the wrong appellate authority within the DON shall be referred expeditiously to the proper authority. Such an appeal may be rejected as untimely only if the initial submission was

untimely, regardless of which authority received it;

c. Time Management. Final determinations on appeals normally shall be made within 20 working days after receipt. When a DON appellate authority has a significant number of appeals preventing a response determination within 20 working days, the appeals shall be processed in a multitrack processing system based at a minimum on the three processing tracks established for initial requests.

12. FOIA Litigation

a. The DON GC is the Secretary's sole delegate for Service of process. Other offices should refuse to accept Service of process, including those for FOIA complaints. The DON GC shall provide copies of properly served FOIA complaints to the relevant appellate authority and IDA.

b. Apportionment of Litigation Costs: In a case in which attorney fees have been assessed, the counsel responsible for defense in that litigation shall recommend an apportionment of this assessment on the commands as appropriate.

c. The cognizant litigation authority (i.e., OJAG Code 14 or Naval Litigation Office, as the case may be) shall ensure litigation support and action in accordance with the policies and practices she/he has established in order to meet the following requirements:

(1) Providing the OCIO (as well as DNS-36 for Navy and SECNAV concerns, and HQMC-ARSF for those involving the Marine Corps) with a summary of any FOIA complaint filed against the DON, to be supplemented by status updates as appropriate;

(2) Forwarding a copy of the complaint to DoD Freedom of Information Policy Office for review;

(3) Forwarding a copy of the complaint to the cognizant field office, as appropriate;

(4) In the case of GC, entering cases under GC's cognizance into its Litigation Case Tracking Management database (see enclosure (6)).

HANDLING CLASSIFIED RECORDS

1. Follow Appropriate DoD and DON guidance. See reference (g), which is superior to any guidance provided in this enclosure.
2. Refer to the IDA. Any request for information believed to be classified must be referred to an IDA. Any DON response to a FOIA request for classified information must come from an IDA or a FOIA appellate authority.
3. Withhold as appropriate. The Government shall withhold information that is properly and currently classified. When denying a record, it may be appropriate to withhold an estimate of the volume of information since such data may also be classified.
4. If needed, consult with appropriate authority
 - a. Consultation is generally not needed. When the requested document is properly and currently classified, deny the request per exemption (1) of the FOIA. In such a situation, there is no need to consult with another authority;
 - b. Consultation is needed when the document is not properly and currently classified. In such a case:
 - (1) Consult the OCA. This is the entity responsible for the classification. Ordinarily, the OCA is identified in a marking on the document;
 - (2) If the OCA is not identified in the document, or if it no longer exists, contact one of the following authorities as appropriate:
 - (a) For the Navy, the OPNAV Security Manager, DNS-34;
 - (b) For the Marine Corps, Headquarters Marine Corps, Plans, Policies and Operations Security Division.
 - c. Prohibited Consultation Practices. The IDA should never (unless explicitly allowed by the appropriate authority):

(1) Release material needing a consultation without first having obtained a determination from the appropriate authority;

(2) Inform the requester of the consultation.

5. Duty to segregate. Classification marking on a document does not necessarily exempt the entire document from disclosure under the FOIA. To ensure a requested record is properly and currently classified, a reviewer with the appropriate security clearance and permission needs to review it line by line and reasonably segregate its content into classified and unclassified portions.

6. "Automatically Declassified" Records may still need to be Withheld. Classified information of historical value more than 25 years old is subject to automatic declassification. However, exemptions may apply, so never assume that a record subject to Automatic Declassification is to be released automatically to the public. Thus, even if a record is older than 25 years, the FOIA processor must consult with the OCA (see paragraph 4 above) to ascertain the extent to which it may remain properly and currently classified.

7. Mailing Addresses for Classified Information. In the event of an appeal involving classified records, the records at issue should be emailed via SIPRNet, or mailed, using procedures in accordance with reference (g). Appropriate mailing addresses for classified information include the following:

a. Navy:

(1) Secret and below – FEDEX/UPS mail to:

Department of the Navy
Attn: Head
CNO/OPNAV DNS-36 FOIA/PA Program Office
1013 O St SE
Building 166, Suite 311
Washington Navy Yard, DC 20374-5029

(2) Top Secret – Mail to:

c/o OPNAV Security Office (DNS-34)
2000 Navy Pentagon
Washington, DC 20350-2000

b. Marine Corps:

(1) Secret and below:

Headquarters, U.S. Marine Corps
Attn: FOIA (ARSF), Rm 2B289
3000 Marine Corps Pentagon
Washington, DC 20350-3000

Phone: 703-614-4008
Fax: 703-614-6287

**REVIEW PROCESS FOR 10 U.S.C. §130E,
DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE SECURITY
INFORMATION**

1. Department of Defense Critical Infrastructure Security Information (DCRIT/CISI). DCRIT/CISI is information that is not classified, because of a need or desire for the limited availability of such information, but which nevertheless is likely to increase the vulnerability of the DoD and/or the public if released indiscriminately. Such limited availability exists for the purpose of coordination with local officials (e.g., police, fire, health departments). Examples include:

a. A map of explosives on a military installation (it may be unclassified to provide access to local firefighters, yet it would likely still pose a danger if widely disseminated);

b. Tactics or characteristics of an installation security or emergency response team.

2. The statute applicable to CISI is reference (c). "Treatment Under Freedom of Information Act of Critical Infrastructure Security Information." This citation should be used in connection with FOIA exemption (3), which recognizes the applicability of statutes outside of the FOIA.

3. Balancing Test: It is appropriate to invoke reference (c) when the public interest in the disclosure of such information does not outweigh preventing the disclosure of such information. This exemption should not be used without review at the policy level (see discussion below).

4. Review Process: Such review shall proceed as follows:

a. The FOIA processing office shall:

(1) Make an initial query to the DON OCIO to check if the full DCRIT review process may be avoided. The purpose is to relieve FOIA processors of unnecessary work. Accordingly, the initial query may be as simple as an email message to the OCIO, with no supporting documents. If the OCIO does not rule out the applicability of reference (c), the FOIA processing office shall proceed to prepare a package for review as set forth below;

(2) Prepare a review package, to be provided in electronic form, as follows:

(a) A copy of the initial FOIA request;

(b) A proposed memo from the OCIO to DoD. It should set forth the following:

1. All the known reasons for and against invoking reference (c), including details on how the information recommended for exemption meets the threshold of qualifying as DCRIT;

2. All relevant issues, including:

a. The nature of the danger to be avoided (attach signed statement by subject matter expert if available);

b. Why, if the information poses a danger, the information is not classified.

(c) All responsive documents with all of the proposed redactions that invoke reference (c);

(d) Any documentation of the public interest in the release of the information, including information provided to the FOIA processing office by the FOIA requester or other interested parties.

(3) Submit the package, in electronic form, to the pertinent FOIA program manager: either DNS-36 or HQMC-ARSF.

b. The pertinent FOIA program manager (DNS-36 or HQMC-ARSF) shall ensure appropriate subsequent review of the package by emailing an electronic version to all stakeholders (while copying the FOIA processing office that submitted the package), namely:

(1) If the request relates to physical infrastructure, to the Assistant Secretary of the Navy (Energy, Installations and Environment);

(2) To any other DON stakeholder organization as appropriate (e.g., the chain of command for the FOIA processing

office that submitted the package);

(3) In all cases, to:

(a) The DON GC Office (to a representative of the office apart from the FOIA program-execution headquarters);

(b) The OCIO, for the final review and chop needed for submission to the DoD. The package to the OCIO shall include:

1. A memorandum of opinion as to the appropriate disposition of the package from the pertinent FOIA program manager (either DNS-36 or HQMC-ARSF);

2. An electronic version of the above memorandum of opinion formatted for submission to the DoD by the OCIO.

c. The OCIO:

(1) Shall finalize the package and submit it to DoD as appropriate;

(2) May revise this procedure at its own discretion for practical considerations (e.g., allow concurrent review in order to save time, provided doing so does not compromise the integrity of the review process).

DEFINITIONS

1. CISI: Critical Infrastructure Security Information. See DCRIT.
2. CMC: Commandant of the Marine Corps, the highest ranking officer in the United States Marine Corps.
3. CNO: Chief of Naval Operations, the senior naval officer of the Department of the Navy.
4. CNO/OPNAV DNS-36: SECNAV/CNO Freedom of Information Act (FOIA)/Privacy Act (PA) Program Office, the official responsible for FOIA program execution for all activities supervised by the CNO/OPNAV and the SECNAV, including DON/AA and the OCIO.
5. DCRIT: Also known as CISI, DCRIT (Defense Critical Infrastructure Security Information) is the term adopted instead by the National Archives and Records Administration for "Defense Critical Infrastructure Security Information" in its Controlled Unclassified Information Registry. DCRIT/CISI requires a special process of consultation and determination. See enclosure (6). DCRIT is: "sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in DoD critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security."
6. DMCS: Director, Marine Corps Staff, who holds responsibility for FOIA program execution for the Marine Corps. See also "HQMC-ARSF" below.
7. DNIG/IGMC: Deputy Naval Inspector General/Inspector General of the Marine Corps.
8. DNS-36: See "CNO/OPNAV DNS-36."

9. DoD: The Department of Defense. It consists of various components, including the DON.
10. DON: The Department of the Navy. It consists of two uniformed Services: the Navy and the Marine Corps.
11. DON/AA: Department of the Navy/Assistant for Administration. This official provides administrative management and support to the Office of the SECNAV.
12. DON CIO: The Department of the Navy Chief Information Officer, including his or her staff and office. The Under Secretary of the Navy serves as the CIO, with day-to-day management of the office provided by the Director, OCIO, and FOIA oversight by the FOIA Lead. The OCIO coordinates regularly with DON Secretariat offices, the Navy, the Marine Corps, DoD, and other Federal Agency CIOs.
13. DON Enterprise FOIA Tracking System: The FOIA-processing system in use by the DON at the time of the adoption of this instruction (i.e., FOIA online), or whatever other FOIA-processing system that is mandated thereafter by the DON or the DoD.
14. DON FOIA Policy website: The website maintained by the OCIO for guidance on the FOIA for the entire DON, including the Navy and the Marine Corps. It is presently located on the OCIO website (at <http://www.doncio.navy.mil>). Click on "BROWSE ALL TOPICS" for dropdown box with alphabetical list that includes link to "Freedom of Information Act" (or click on <http://www.doncio.navy.mil/ContentView.aspx?ID=5232>). See also "FOIA Requester Service Center (RSC) website."
15. FOIA: The Freedom of Information Act, 5 U.S.C. §552.
16. FOIA Library: Per reference (e), each DoD component shall establish one or more FOIA libraries. The DON will meet this requirement by having a FOIA library on each FOIA RSC website. Additional FOIA libraries are maintained on the DON FOIA Policy Website and on FOIA online.
17. FOIA online: The FOIA-processing system in use by the DON at the time of the adoption of this instruction, or whatever other FOIA-processing system that is mandated thereafter by the

DON or the DoD.

18. FOIA Requester Service Center (RSC): See "RSC."
19. FOIA RSC Website: Per reference (e), each FOIA RSC shall have a website that serves to educate the public on the FOIA process. The primary FOIA RSC website for the Navy is <http://www.secnav.navy.mil/foia/>. For the Marine Corps it is <http://www.hqmc.marines.mil/Agencies/USMC-FOIA>. See also "DON FOIA Policy website."
20. GC: The General Counsel of the Department of the Navy.
21. HQMC-ARSF: Headquarters Marine Corps-Administration and Resource Division, Security Branch, FOIA, which is responsible for FOIA program execution for the Marine Corps. See also "DMCS."
22. IDA: See "Initial Denial Authority."
23. IGMC: See "DNIG/IGMC."
24. Initial Denial Authority: Authority to deny a request under the FOIA, or an official with such authority. Every denial of a FOIA request must be signed by an IDA. For more information, see enclosure (1), paragraph 6.
25. LCTM: the Litigation Case Tracking Management system managed by the Navy Litigation Office.
26. NAVIG: The Naval Inspector General.
27. NAVINSGEN: The Office of the NAVIG.
28. OGIS: Office of Government Informational Services, a Federal agency that provides voluntary mediation and advisory opinions. For more information, go to <https://www.archives.gov/ogis/about-ogis/contact-information>.
29. OJAG: Office of the Judge Advocate General.
30. OCIO: Office of the Chief Information Officer. See also "DON CIO."

31. OPNAV: Office of the Chief of Naval Operations. See "CNO."
32. PA: The Privacy Act, 5 U.S.C. §552a.
33. Public Liaison: A point of contact within each Federal agency, whose role is to assist FOIA requesters in making requests, appeals, and resolving FOIA disputes between requesters and agencies. The IDA should provide contact information for the Public Liaison.
34. Release Authority: Authority to grant requests, on behalf of the SECNAV, for agency records in one's possession.
35. RSC: Requester Service Center. A DoD or DON component office that receives FOIA requests. See also "Public Liaison."
36. SECNAV: The Secretary of the Navy. The SECNAV is responsible for, and has the authority under Title 10 of the United States Code, to conduct all the affairs of the DON, including formulation and implementation of policies and programs that are consistent with the national security policies and objectives established by the President and the Secretary of Defense.
37. Website: See "FOIA RSC website."