



DEPARTMENT OF THE NAVY  
HEADQUARTERS UNITED STATES MARINE CORPS  
2 NAVY ANNEX  
WASHINGTON, DC 20380-1775

IN REPLY REFER TO:

5720  
ARSE/3U100489  
23 Apr 03

From: Commandant of the Marine Corps  
To: Distribution List

Subj: NOTICE OF POLICY CHANGES TO THE DEPARTMENT OF THE NAVY  
(DON) FREEDOM OF INFORMATION ACT (FOIA) PROGRAM

Ref: (a) SECNAVINST 5720.42F

Encl: (1) CNO ltr N09B10/3U507685 of 26 Mar 03 [w/o encl(3)]  
(2) EO 12958, as amended  
(3) CNO ltr N09B10/1U514379 of 26 Oct 01  
(4) CNO ltr N09B10/1U514545 of 20 Nov 01  
(5) DON PA Systems of Records Notice N05000-3  
(6) CNO ltr N09B10/2U512894 of 22 Mar 02  
(7) CMC ltr ARSE/3U100263 of 19 Feb 03 (w/encls)

1. This memorandum is provided for your immediate review, implementation, and compliance. Please ensure widest dissemination of this information.

2. By enclosure (1), the DON FOIA Policy Office apprises of new policy guidance issued by the Director, Freedom of Information and Security Review (DFOISR), Department of Defense (DoD), regarding the protection from disclosure of "voluntarily submitted" Critical Infrastructure Information (CII).

3. Enclosure (1) also provides "sample" correspondence that demonstrates the type of information that should be contained in a FOIA response. Please note that the content of your FOIA response correspondence is very important since it becomes part of your administrative record. In many instances of litigation, your administrative record is the only document a court will consider, especially in "reverse FOIA" cases where the plaintiff files his/her suit under the Administrative Procedures Act.

4. Enclosure (2) is a copy of Executive Order 12958, as amended by President Bush on 25 Mar 03. Since the Executive Order is the basis for claiming exemptions under the FOIA [exemption (b)(1)] and the Privacy Act [exemption (k)(1)], it is imperative that you review the new Order to identify changes. Effective immediately, you must cite to the appropriate classification category under paragraph 1.4 of enclosure (2) to deny "currently and properly"

Subj: NOTICE OF POLICY CHANGES TO THE DEPARTMENT OF THE NAVY  
(DON) FREEDOM OF INFORMATION ACT (FOIA) PROGRAM

classified information. References to paragraph 1.5 are no longer valid. Furthermore, even though the 28 Mar 03 issue of the Federal Register references the new Order as Executive Order 13292, the Information Security Oversight Office and the Department of Justice have determined that Executive Order 13292 does not cancel 12958 but, instead, amends it. Therefore, whenever referencing the new Order, you should cite to "Executive Order 12958, as amended" or "EO 12958, as amended". Otherwise, you will effectively be referencing the old Order. Further guidance is expected from the security classification policy makers in the near future.

5. In light of today's sensitive and sometimes hostile environment, you are asked to revisit previous policy guidance on the following issues:

a. Mailing lists/email addresses. As a result of many of our troops being deployed overseas, the Department of Defense and its military components, is seeing a tremendous increase in the number of inquiries by which the members of the public, including family members, seek access to U.S. Postal Service or email addresses of servicemembers so that they can contact them.

(1) You are reminded that, under the provisions of the FOIA, you must deny the duty station addresses and other personally identifying information (i.e.; name, duty station phone numbers, email addresses) of DoD personnel assigned to routinely deployable, sensitive, or overseas units under exemptions (b)(3), citing to 10 U.S.C. § 130b as the basis for withholding, and (b)(6). The one exception to this rule does allow for the disclosure of the name, duty station address, duty telephone number, and duty email address of flag officers, public affairs officers, FOIA/PA officers, and other officers who routinely deal with members of the public. Please note, however, the above policy does not preclude you from forwarding correspondence to the member on behalf of the requester, should you wish to do so.

(2) Additionally, subsequent to the attacks of 11 Sep 01, the Secretary of Defense made a decision to protect lists of names and addresses of all other DoD civilian and military personnel, to include contractors, under exemption (b)(6) of the FOIA. The same exceptions apply as detailed in paragraph 5a(1) above.

(3) Enclosures (3) and (4) pertain.

Subj: NOTICE OF POLICY CHANGES TO THE DEPARTMENT OF THE NAVY  
(DON) FREEDOM OF INFORMATION ACT (FOIA) PROGRAM

b. Recall rosters. In light of our current state of alert, many USMC activities are updating their recall rosters.

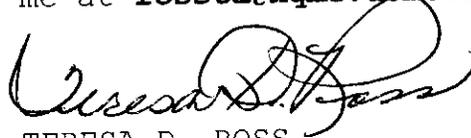
(1) You are reminded that USMC recall roster information is governed by DON Privacy Act Systems of Records Notice N05000-3, Organizational Locator and Social Roster. A copy of this Notice is provided as enclosure (5).

(2) Enclosure (6) details the DON's policy regarding the collection, maintenance, and use of recall roster information. Please review enclosure (6) to ensure that recall roster information is afforded proper protections and that it is not used for any purpose other than that for which it was collected.

c. Homeland security. By enclosure (7), you were apprised of the DFOISR special handling requirements of FOIA responsive documents pertaining to Chemical, Biological, Radiological, and Nuclear Weapons. Please ensure compliance.

6. Policy contained in this letter will be incorporated into the next revision of reference (a).

7. Questions concerning any of these issues may be directed to me at (703) 614-4008 or emailed to me at [rosstd@hqmc.usmc.mil](mailto:rosstd@hqmc.usmc.mil).



TERESA D. ROSS  
By direction

Distribution:

MARFORLANT NORFOLK VA  
MARFORPAC CAMP SMITH HI  
MARFORRES NEW ORLEANS LA  
MARFORSOUTH MIAMI FL  
MARFOREUR PANZER KASERNE,  
BOEBLINGEN GE  
MARCORLOGBASE ALBANY GA  
MARCORSYSCOM ALBANY GA  
MARCORBASESPAC CAMP SMITH HI  
FMFLANT CAMP LEJEUNE NC  
FMFPAC CAMP SMITH HI  
I MEF CAMP PENDLETON CA  
II MEF CAMP LEJEUNE NC  
III MEF OKINAWA JA  
1ST MARDIV CAMP PENDLETON CA

2D MARDIV CAMP LEJEUNE NC  
3D MARDIV OKINAWA JA  
1ST FSSG CAMP PENDLETON CA  
2D FSSG CAMP LEJEUNE CA  
3D FSSG OKINAWA JA  
1ST MAW OKINAWA JA  
2D MAW MCAS CHERRY POINT NC  
3D MAW MCAS MIRAMAR CA  
MAGTFTC 29 PALMS CA  
CG ERR PARRIS ISLAND SC  
CG WRR SAN DIEGO  
JLC MCAS CHERRY POINT NC  
JLC MCAS MIRAMAR CA  
DLC MCRD PARRIS ISLAND SC

**ENCLOSURE (1)**



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

5720  
Ser N09B10/3U507685  
26 Mar 03

From: Chief of Naval Operations  
To: EMail Distribution List (FOIA)

Subj: DON FOIA POLICY UPDATE

Ref: (a) SECNAVINST 5720.42F

Encl: (1) DFOISR Memo, 03-CORR-017, of 25 Mar 03  
(2) Response letters  
(3) Executive Order 12958, As Amended

1. This policy letter is provided for your immediate review, dissemination, and implementation. It addresses several changes that impact the Department of the Navy's (DON's) Freedom of Information Act (FOIA) program.

2. Enclosure (1) is the new policy guidance issued by the Department of Defense regarding how to protect voluntarily submitted Critical Infrastructure Information (CII) from disclosure.

3. Enclosure (2) provides detailed guidance on what information should be contained in a FOIA response letter. The contents of the FOIA response letter are important since it is the administrative record of how a request was processed and could be the only document a court considers in litigation.

4. Enclosure (3) is a copy of Executive Order (E.O.) 12958 that was amended by President Bush on March 25, 2003. Since the E.O. is the basis for claiming exemption (b)(1) under FOIA; exemption (k)(1) under the Privacy Act; providing a neither confirm nor deny response, etc., it is imperative that you review the new order to identify changes. Guidance from the security classification policy makers will be forthcoming under separate cover.

5. I ask that you revisit the prior policy guidance on the following issues:

a. Mailing Lists/Email addresses: As a result of many of our troops being sent overseas, we are receiving increased queries as to addresses (email and mail) so they can be contacted. FOIA Officers must deny access to addresses of individuals who are assigned overseas, routinely deployable, or attached to a sensitive unit under FOIA exemption (b)(3) since withholding is required by 10 U.S.C. 130b. The exception to the rule is that we release the names and locations of our flag officers, public affairs officials, FOIA officers, and other officials who routinely deal with the public. Shortly after the attack on the Pentagon, the Secretary of Defense made a decision to protect lists of names and addresses of all other civilian and military personnel, to include contractors, under FOIA exemption (b)(6). Please ensure compliance. The same exceptions apply. See FOIA policy letters of 26 Oct and 20 Nov 02 which are downloadable from [www.foia.navy.mil](http://www.foia.navy.mil) under Resource Materials.

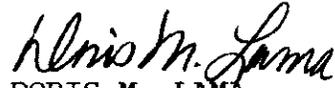
b. Recall Rosters: As a result of our state of alert, activities are updating recall rosters. Please revisit the policy guidance set forth in my policy letter of 22 Mar 02, which is downloadable from [privacy.navy.mil/policy/20020322.pdf](http://privacy.navy.mil/policy/20020322.pdf) regarding the collection, maintenance, and use of recall rosters. Also, please ensure that the recall roster information is not used for purposes other than those listed in the Privacy Act Statement and that all actions be taken to ensure protection for unauthorized use or disclosure.

c. Homeland Security: FOIA policy letter of 27 Mar 02 addresses Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security. Please review the guidance at <http://foia.navy.mil/020327policymemo.pdf>.

6. Training: There is a continuing need for FOIA training. Regrettably due to losses in personnel and constrained training/travel funds, it is not possible for this office to conduct uncompensated training. There are, however, several training sources available to you: training packages that are downloadable from [foia.navy.mil](http://foia.navy.mil); Department of Justice training (see [www.usdoj.gov/foia](http://www.usdoj.gov/foia)); training (both correspondence and in-house) provided by the Department of Agriculture Graduate School; training offered by the American Society of Access

Professionals (ASAP) (see their web site at [www.accesspro.org](http://www.accesspro.org)).

7. Policy contained in this letter will be incorporated into the next revision to reference (a). Direct any inquiries to the undersigned.



DORIS M. LAMA  
By direction  
(202) 685-6545  
DSN 325-6545



**DEPARTMENT OF DEFENSE**  
**DIRECTORATE FOR FREEDOM OF INFORMATION AND SECURITY REVIEW**  
**1155 DEFENSE PENTAGON**  
**WASHINGTON, DC 20301-1155**

**25 MAR 2003**

03-CORR-017

**MEMORANDUM FOR: SEE DISTRIBUTION**

**Subject: Freedom of Information Act (FOIA) Requests for Critical Infrastructure Information (CII)**

The Homeland Security Act of 2002, Public Law 107-296, established the Department of Homeland Security (DHS). A provision within the legislation established a new Exemption 3 Statute for applicable protection of CII. This Exemption 3 statute applies only to DHS and until further notice, may not be used to exempt CII maintained by the Department of Defense (DoD). Further guidance on the Exemption 3 statute was distributed by the Department of Justice (Office Of Information and Privacy) (DOJ (OIP)) on the Internet on FOIA Post at <http://www.usdoj.gov/oip/foiapost/2003foiapost4.htm>.

The DoD has recognized the need to protect voluntarily submitted CII when these records are requested under the FOIA. Efforts to obtain an Exemption 3 statute unique to DoD are ongoing. Until such time as an Exemption 3 statute for CII that includes the DoD is passed, the following guidance for exempting CII under the provisions of the FOIA is provided:

- a. Exemption (b)(1) may be used to exempt classified CII that is determined to be currently and properly classified after review.
- b. Exemption (b)(2)High may be used to exempt applicable unclassified CII. Recent guidance issued by DOJ(OIP) concerning the use of the (b)(2) High exemption for CII may be found on FOIA Post at <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>.
- c. Exemption (b)(4) may be used to exempt applicable unclassified CII that is voluntarily submitted and the release of which would cause competitive harm.
- d. Exemptions (b)(7)(E) and (b)(7)(F) may be used to exempt applicable law enforcement information.

Additional guidance or changes will be forwarded as it becomes available.

  
H.J. McIntyre  
Director



ENCL (1)

## FOIA RESPONSE LETTERS

1. A FOIA response letter is the administrative record on how a FOIA was processed. In cases of litigation, it may be the only document that the Court considers. Accordingly, a FOIA response letter must be accurate and complete and contain the following information:

a. Dates: Ensure that the date of the request and the date the request was received are addressed in the response letter. For example, "Your Freedom of Information Act request of January 3, 2003, was received on January 30, 2003."

b. Subject matter: Please address what the requester is seeking. For example: "This refers to your Freedom of Information Act request of January 3, 2003, in which you seek a copy of contract N00024-93-D-0031."

c. Case Number: Please assign a case number to the action. For example: "This refers to your Freedom of Information Act request of January 3, 2003, in which you seek a copy of contract N00024-93-D-0031. Your request was received on January 30, 2003, and assigned case number 2003001040."

d. Refinement: Reference any communications (verbal or written) whereby the requester has refined or modified his/her request. For example: "This also confirms our telephone conversation on February 3, 2003, wherein you refined your request and now seek...".

e. Fees:

(1) Fees must be resolved before processing a request, if the fees are likely to exceed the minimum fee waiver threshold of \$15. Accordingly, do not begin processing a FOIA that will exceed the \$15 minimum fee threshold without first resolving the fee issue.

(2) If fees are charged, you must cite the category you have placed the requester (i.e., commercial, media, educational, or all other) and breakout the fees being charged. For example, "As an "All Other Requester" you are responsible for fees that exceed the minimum fee waiver threshold of \$15 once you have been given the first two hours of search and first 200 pages for free. During

FNMJ. (2)

the processing of your request, we expended 4 hours in search and are forwarding 300 pages to you. Once the deductions are made, your fee is 2 hours of search at \$44 per hour (\$88) and 100 pages of duplication at \$.15 per page (\$15) for a total of \$105."

(3) Activities can collect fees totaling \$250 or more upfront prior to processing a request. For fees under \$250, they can complete processing the request and then apprise the requester that the documents will be released upon receipt of the check/money order.

(4) If fees are waived, address that in your response letter.

f. Exemptions: It is imperative that all exemptions claimed be cited. It is also advisable to be as explanative as possible when claiming an exemption so that the requester understands what kind of information has been withheld. This may serve to eliminate an appeal. For example: "Under exemption 5 U.S.C. 552(b)(6) we have withheld the names of other individuals, their home addresses, and social security numbers since release would constitute a clearly unwarranted invasion of personal privacy."

Note: DON activities shall not "black out" exempted information. Technology exists to restore "blacked out" information.

g. Adequacy of search: In the case of a "no record" response, advise the requester of where the search was conducted and what the requirement is regarding records disposal. For example: "A search of our files failed to disclose a copy of the 1992 FOIA request you filed with this office. This is not unusual since the retention of granted and no record FOIA requests is 2 years and those that are denied in whole or in part are 6 years."

h. Appeal Rights: Appeal rights should be provided to any requester who has been denied information. Also, in cases where no records could be located, the requester should be provided information on their ability to appeal the adequacy of search.

i. Appellate Authority: Provide the requester with the address of the appropriate Navy appellate authority.

We have two appellate authorities: the Judge Advocate General and the General Counsel. The delineation of their areas of responsibility is delineated in SECNAVINST 5720.42F.

2. Sample FOIA response letters can be downloaded from [www.foia.navy.mil](http://www.foia.navy.mil) under FOIA Resources.

**ENCLOSURE (2)**

MS Word Version

**THE WHITE HOUSE  
Office of the Press Secretary**

For Immediate Release  
March 25, 2003

**EXECUTIVE ORDER**

-----

**FURTHER AMENDMENT TO EXECUTIVE ORDER  
12958, AS AMENDED,  
CLASSIFIED NATIONAL SECURITY INFORMATION**

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to further amend Executive Order 12958, as amended, it is hereby ordered that Executive Order 12958 is amended to read as follows:

**Classified National Security Information**

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nations progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nations security remains a priority.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**PART 1--ORIGINAL CLASSIFICATION**

ENIA 1 (2)

**Sec. 1.1. Classification Standards. (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:**

- (1) an original classification authority is classifying the information;**
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;**
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and**
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.**

**(b) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.**

**(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.**

**Sec. 1.2. Classification Levels. (a) Information may be classified at one of the following three levels:**

- (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.**
- (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.**
- (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.**

**(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.**

**Sec. 1.3. Classification Authority. (a) The authority to classify information originally may be exercised only by:**

**(1) the President and, in the performance of executive duties, the Vice President;**

**(2) agency heads and officials designated by the President in the Federal Register; and**

**(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.**

**(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.**

**(c) Delegation of original classification authority.**

**(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.**

**(2) "Top Secret" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section.**

**(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section; or the senior agency official described in section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.**

**(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.**

**(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives. Such training must include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.**

(e) **Exceptional cases.** When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

**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.

**Sec. 1.5. Duration of Classification.** (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the

national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. All information classified under this section shall be subject to section 3.3 of this order if it is contained in records of permanent historical value under title 44, United States Code.

(c) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

**Sec. 1.6. Identification and Markings.** (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a) or section 1.5(c);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b); or

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5 (b); and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information described in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

**(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.**

**Sec. 1.7. Classification Prohibitions and Limitations. (a) In no case shall information be classified in order to:**

- (1) conceal violations of law, inefficiency, or administrative error;**
- (2) prevent embarrassment to a person, organization, or agency;**
- (3) restrain competition; or**
- (4) prevent or delay the release of information that does not require protection in the interest of the national security.**

**(b) Basic scientific research information not clearly related to the national security shall not be classified.**

**(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:**

- (1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;**
- (2) the information may be reasonably recovered; and**
- (3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.**

**(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order.**

**(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items**

of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

**Sec. 1.8. Classification Challenges.** (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

## **PART 2—DERIVATIVE CLASSIFICATION**

**Sec. 2.1. Use of Derivative Classification.** (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.2. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

### **PART 3—DECLASSIFICATION AND DOWNGRADING**

Sec. 3.1. Authority for Declassification. (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the

classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

**Sec. 3.2. Transferred Records.** (a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives and Records Administration (National Archives) as of the effective date of this order shall be declassified or downgraded by the Archivist of the United States (Archivist) in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

**Sec. 3.3. Automatic Declassification. (a)** Subject to paragraphs (b)-(e) of this section, on December 31, 2006, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification, except as provided in paragraphs (b)-(e) of this section.

**(b)** An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which could be expected to:

- (1)** reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;
- (2)** reveal information that would assist in the development or use of weapons of mass destruction;
- (3)** reveal information that would impair U.S. cryptologic systems or activities;
- (4)** reveal information that would impair the application of state of the art technology within a U.S. weapon system;
- (5)** reveal actual U.S. military war plans that remain in effect;
- (6)** reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
- (7)** reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;
- (8)** reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or
- (9)** violate a statute, treaty, or international agreement.

(c) An agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and which the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the file series;
- (2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended. File series exemptions previously approved by the President shall remain valid without any additional agency action.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) of this section that the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the information, either by reference to information in specific records or in the form of a declassification guide;
- (2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended.

The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 5 additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

(3) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years for classified records that have been referred or transferred to that agency by another agency less than 3 years before automatic declassification would otherwise be required.

(4) By notification to the Director of the Information Security Oversight Office, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any

treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(h) Records containing information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies shall be referred for review to those agencies and the information of concern shall be subject to automatic declassification only by those agencies, consistent with the provisions of subparagraphs (e)(3) and (e)(4) of this section.

**Sec. 3.4. Systematic Declassification Review.** (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified records: (1) accessioned into the National Archives as of the effective date of this order; (2) transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall ensure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

**Sec. 3.5. Mandatory Declassification Review. (a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:**

**(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;**

**(2) the information is not exempted from search and review under sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403-5c, 403-5e, and 431); and**

**(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requesters appeal rights.**

**(b) Information originated by:**

**(1) the incumbent President or, in the performance of executive duties, the incumbent Vice President;**

**(2) the incumbent Presidents White House Staff or, in the performance of executive duties, the incumbent Vice Presidents Staff;**

**(3) committees, commissions, or boards appointed by the incumbent President; or**

**(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The**

information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

**Sec. 3.6. Processing Requests and Reviews.** In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

**Sec. 3.7. Declassification Database.** (a) The Director of the Information Security Oversight Office, in conjunction with those agencies that originate classified information, shall coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

(b) Agency heads shall fully cooperate with the Director of the Information Security Oversight Office in these efforts.

#### **PART 4—SAFEGUARDING**

**Sec. 4.1. General Restrictions on Access.** (a) A person may have access to classified information provided that:

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency heads designee;
- (2) the person has signed an approved nondisclosure agreement;  
and
- (3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and

telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

- (1) prevent access by unauthorized persons; and
- (2) ensure the integrity of the information.

(g) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(i) Except as otherwise provided by statute, this order, directives implementing this order, or by direction of the President, classified information originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency. Prior consent is not required when referring records for declassification review that contain information originating in several agencies.

**Sec. 4.2. Distribution Controls.** (a) Each agency shall establish controls over the distribution of classified information to ensure that it is distributed only to organizations or individuals eligible for access and with a need-to-know the information.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing this order and any procedures issued by agencies governing the classified information,

which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of Central Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

**Sec. 4.3. Special Access Programs.** (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic, and tactical programs), or intelligence sources or methods, this function shall be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

- (1) the vulnerability of, or threat to, specific information is exceptional; and
- (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations.

- (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.
- (2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office, or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency head shall brief the Assistant to the President for National Security Affairs, or a designee, on any or all of the agency's special access programs.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

**Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel.** (a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied policy-making positions to which they were appointed by the President under section 105(a)(2)(A) of title 3, United States Code, or the Vice President under 106(a)(1)(A) of title 3, United States Code; or

(3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the

information is safeguarded in a manner consistent with this order;  
and

(3) limits the access granted to former Presidential appointees and Vice Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee or a Vice Presidential appointee.

#### **PART 5--IMPLEMENTATION AND REVIEW**

**Sec. 5.1. Program Direction.** (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

- (1) classification and marking principles;
- (2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;
- (3) agency security education and training programs;
- (4) agency self-inspection programs; and
- (5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

**Sec. 5.2. Information Security Oversight Office.** (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

- (1) develop directives for the implementation of this order;

- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;
- (4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the Assistant to the President for National Security Affairs within 60 days of the request for access. Access shall be denied pending the response;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Assistant to the President for National Security Affairs;
- (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
- (7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
- (8) report at least annually to the President on the implementation of this order; and
- (9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

**Sec. 5.3. Interagency Security Classification Appeals Panel.**

**(a) Establishment and administration.**

- (1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the Assistant to the President for National Security Affairs shall each

be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panels functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panels activities.

**(b) Functions. The Panel shall:**

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order.

**(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the Federal Register. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:**

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the Federal courts; and

(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel shall report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) Notwithstanding paragraphs (a) through (e) of this section, whenever the Panel reaches a conclusion that information owned or controlled by the Director of Central Intelligence (Director) should be declassified, and the Director notifies the Panel that he objects to its conclusion because he has determined that the information could reasonably be expected to cause damage to the national security and to reveal (1) the identity of a human intelligence source, or (2) information about the application of an intelligence source or method (including any information that concerns, or is provided as a result of, a relationship with a cooperating intelligence element of a foreign government), the information shall remain classified unless the Director's determination is appealed to the President, and the President reverses the determination.

**Sec. 5.4. General Responsibilities.** Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) ensure that agency records systems are designed and maintained to optimize the safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information is established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information;

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

## **PART 6—GENERAL PROVISIONS**

Sec. 6.1. Definitions. For purposes of this order:

(a) "Access" means the ability or opportunity to gain knowledge of classified information.

(b) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(d) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(g) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(h) "Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

**Sec. 5.5. Sanctions.** (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(i) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(j) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(k) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(l) "Declassification authority" means:

- (1) the official who authorized the original classification, if that official is still serving in the same position;
- (2) the originators current successor in function;
- (3) a supervisory official of either; or
- (4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(m) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(n) "Derivative classification" means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(o) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(p) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(q) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(r) "Foreign government information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence;  
or

(3) information received and treated as "foreign government information" under the terms of a predecessor order.

(s) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(t) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a "violation," as defined below.

(u) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

(v) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(w) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(x) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

(y) "National security" means the national defense or foreign relations of the United States.

(z) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(aa) "Network" means a system of two or more computers that can exchange data or information.

(bb) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(cc) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

(dd) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ee) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(ff) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(gg) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(hh) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(ii) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(jj) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(kk) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(ll) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(mm) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(nn) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(oo) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(pp) "Weapons of mass destruction" means chemical, biological, radiological, and nuclear weapons.

Sec. 6.2. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, officers, employees, or agents. The foregoing is in addition to the specific provisions set forth in sections 3.1(b) and 5.3(e) of this order."

(d) Executive Order 12356 of April 6, 1982, was revoked as of October 14, 1995.

Sec. 6.3. Effective Date. This order is effective immediately, except for section 1.6, which shall become effective 180 days from the date of this order.

GEORGE W. BUSH

THE WHITE HOUSE,  
March 25, 2003.

**ENCLOSURE (3)**



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

5720

Ser N09B10/1U514379

26 Oct 01

From: Chief of Naval Operations  
To: Email Distribution List (FOIA)  
Subj: POLICY CHANGES TO THE DON FOIA PROGRAM  
Ref: (a) SECNAVINST 5720.42F  
(b) DOD 5400.7-R

1. This policy memo addresses a myriad of changes being made to the DON's FOIA Program. It is being emailed/faxed to you for immediate implementation and dissemination to those activities that report to you. As always, our policy letters are posted under FOIA Resource Materials at foia.navy.mil/.

2. On 12 Oct 01, Attorney General (AG) Ashcroft issued new FOIA policy. His memo supersedes the FOIA policy statement that was issued by AG Reno in 1993. A copy of the memo and analysis by the Department of Justice (DOJ) is downloadable (see <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>).

3. As a result of the AG memo, the following changes to FOIA policy are effective immediately. These changes will be incorporated into the rewrite of reference (a), once reference (b) is reissued.

a. DON activities will no longer use the "foreseeable harm" standard when adjudicating whether to release/deny information. Rather, DON activities will adopt the "Sound Legal Basis" standard reflected in the AG memo. DON activities will be responsible for presenting a rationale for denial that DOJ will be able to defend if the denial is litigated.

b. While the memo does not eliminate the ability to make a discretionary disclosure, DON activities are no longer encouraged to do so.

52-53 & B6

c. Exemption low (b) (2) is available for use by DON activities to protect routine housekeeping information that is relatively trivial in nature. Activities are encouraged to consult the DOJ "Freedom of Information Act Guide & Privacy Act Overview" for an in depth discussion of low (b) (2).

d. DON activities should consider using high (b) (2) to protect vulnerability assessments, stockpile information, and security assessments.

4. On 18 Oct 01, the Deputy Secretary of Defense (DepSecDef) issued a memorandum entitled "Operations Security Throughout the Department of Defense." The DepSecDef memo states "Much of the information we use to conduct DOD's operations must be withheld from public release because of its sensitivity. If in doubt, do not release or discuss official information except with other DOD personnel."

5. It has been the policy of DOD to release the names of personnel in response to a FOIA request unless those persons are assigned overseas, routinely deployable, or assigned to a sensitive activity. Today, regardless of their duties, DOD personnel are at increased risk solely by association with the on-going military efforts. Thus when responding to a FOIA request for lists of DON personnel (particularly computer data base lists) these lists shall be withheld. This is to include military members, civilian personnel, members of the Guard and Reserves, and Coast Guard personnel when it is operating as a service in the Navy. This information should be considered exempt under high (b) (2) because its release would result in circumvention of DOD statutes and regulations concerning the security of DOD personnel and operations and under exemption (b) (6) because release would result in a clearly unwarranted invasion of personal privacy. To this end, DON activities shall:

a. Withhold lists of DON personnel in response to FOIA requests for such information. For example:

(1) Under exemption (b) (3), specifically 10 U.S.C. 130b, continue to withhold lists of names, addresses, and other information concerning individuals who are stationed overseas or assigned to a routinely deployable or sensitive unit. This includes both civilian and military personnel.

(2) Under exemptions high (b)(2) and (b)(6), withhold lists of individuals under FOIA that do not fall under subparagraph 5a(1).

b. With regard to the release of individual names, DON activities should weigh heavily the public's right to know versus the individual's personal privacy. For example, activities may determine the release of names of high ranking officials (i.e., both flag rank and civilian equivalent) and those individuals that interact with the public as their primary job are releasable.

c. Case law is still evolving on the issue of high (b)(2). In some litigation cases, the courts have held that information must be "predominantly internal" in order to qualify for withholding under high (b)(2). This poses a potential problem in making arguments based solely on the premise that information should be denied because release would cause circumvention of agency regulations. DOJ maintains that it will be difficult to defend withholding information that has been previously released but may now pose a security risk.

#### 6. Impact of Policy Changes on Documents Placed in Our FOIA Electronic Reading Rooms:

a. We must continue to comply with the requirements of E-FOIA by placing frequently requested documents in our Electronic Reading Rooms.

b. We continue to receive frequent requests for impact credit card holders. DON activities shall discontinue releasing the names of individuals and when posting lists in the reading room, only list the office code, address, and telephone number.

c. Telephone directories and organizational charts are also frequently requested. DON activities shall continue to release and post such documents subject to redacting the names and other personal information on individuals.

d. Proactive placement of documents in E-FOIA Reading Room. DON activities should play careful attention to the kinds of documents that are being placed in their reading rooms in light of DepSecDef's memo on Operations Security

Throughout the Department of Defense which further states "We must ensure that we deny our adversaries the information essential for them to plan, prepare or conduct further terrorist or related hostile operations against the United States and this Department."

e. This change in policy does not apply to public affairs releases of information, the Navy locator, or SMARTLINK. Offices having cognizance over these matters will establish their own policies.

#### 7. Unit Prices

a. A recent joint reverse FOIA court decision, MCI v. GSA and Sprint v. GSA, has resulted in a change in the guidance concerning the release of unit prices. In light of this opinion, the Office of Information and Privacy (OIP), Department of Justice, advises that submitter notification, in accordance with Executive Order 12,600, should be made whenever an agency receives a FOIA request for documents that contain unit prices. Accordingly, depending upon the submitter's response, the release of unit prices should be made on a case-by-case basis.

b. Currently, the Department of Justice is discussing whether this decision will be appealed. Once that decision is made, OIP will issue further guidance concerning the release of unit prices. We will advise you of any new guidance from OIP as soon as it is received.

#### 8. foia.navy.mil

a. We continue to update our FOIA On-Line Resource Site and add new resource materials and points of contact. For example, we recently added an Electronic Reading Room door for the Naval Supply Systems Command. Now, information pertaining to the Fleet Industrial Supply Centers (FISCs) will appear behind that door.

b. If you are an Echelon 2 command and have a FOIA page on your activity's web site, please check foia.navy.mil to see if your activity is listed under "Points of Contact." If it's not, email your URL to navyfoia@hq.navy.mil so we can add you to our site.

9. FOIA Annual Report Changes for FY 2002 Report Submission (1 Oct 01 - 30 Sep 02): As a result of a GAO

review, DOJ has requested that agencies make changes in how they collect and report information in the FOIA Annual Report. The four main areas of guidance from DOJ requiring adjustments in reporting for the FOIA Annual Report are: (1) Using only one determination per action; (2) Calculating processing days; (3) Itemizing requests for expedited access; and (4) Counting Privacy Act requests as FOIA requests. Accordingly,

a. When you complete the action on a FOIA request, only one determination may be made per action. If you have multiple actions on a single request, the predominant action will carry the weight in making the determination for reporting purposes. Therefore, on the FOIA Annual Report form (DD Form 2564), Block 1a (total initial requests processing during the FY) must equal the total of Blocks 1b, c, d and e. Block 1e, "Other Reasons" must be broken out in Blocks 2b1 through 2b9 and the total must equal Block 1e. The same process applies to appeal actions in Blocks 3a-f and 4b1-9.

b. The calculation of the processing days' median age reported in Blocks 5 and 7 will be done in "working days" and not "calendar days".

c. An additional reporting requirement beginning with the FY 2002 report is to report the number of requesters who asked that their request receive expedited processing. This is different from the number currently being reported as the number of cases that you granted expedited processing. The new requirement will be typed in the blank space after "Expedited Processing" in Block 7c. It should be represented as such: "Requests Rec'd: ##".

d. Clarification is also needed on the relationship of the Privacy Act (PA) and FOIA requests for purposes of the FOIA Annual Report. Paragraph 10d of reference (a) states that "Requesters who seek records about themselves that are contained in a PA system of records and who cite or imply the FOIA or both Acts will have their requests processed under the provisions of both the PA and the FOIA." This policy is to be continued, to include instances in which formal PA requests (written or local form) are made by first party requesters for non-exempt systems of records, and a total release is made.

(1) FOIA offices will count first party PA requests under Blocks 1a and 1b and complete Blocks 5 and 7 as they apply. No fees or program costs will be reported under Blocks 8 and 9, as fees still remain under the PA. However, you can count full and part time staff. DON activities that allow first party requesters to seek walk-in access to non-exempt records (e.g., personnel or medical files) without completing a PA form or requesting a signed letter may continue to follow their local procedures without counting such requests under the FOIA.

(2) First party PA requests for access to records that are exempt under the (j)(2) provision of the PA will continue to be processed under the provisions of both Acts and counted in Blocks 1a and 1c. In Block 2a, only count the FOIA exemptions claimed. You will complete Blocks 5 through 7 as they apply. Do not report fees or costs under Blocks 8 and 9, as such costs remain under the provisions of the PA, but you will reflect the number of full or part time staff.

(3) First party PA requests for access to records that are exempt under the (k) exemptions of the PA will continue to be processed under the provisions of both Acts. In Block 1, count the request once under "total requests" and once under "denied in part." If you cite to a FOIA exemption, report it in Block 2a. This report does not collect information on PA exemptions claimed. Complete Blocks 5 through 7 as they apply. Do not report fees or costs under Blocks 8 and 9, as such costs remain under the provisions of the PA, but you will reflect the number of full time or part time staff.

10. In view of the above, please discontinue using enclosure (9) to reference (a) as a tool to collect information for the Annual FOIA Report. This form will be revised in the next revision to reference (a). Note: These changes do not impact your FY 2001 submission.

**FINAL REMINDER: FY 2001 Submission by CMC, OGC, JAG, and Echelon 2 Commands are due to CNO (N09B10) by 5 Nov 01.**

11. Fee Status. DFOISR advised Mr. John Greenewald Jr., in a letter dated 15 Oct 01, that his fee status was being changed from "academic" to "commercial" requester since he is operating a fee for service company on the internet at [www.foiaservices.com](http://www.foiaservices.com). Accordingly, all open requests and future requests made by Mr. Greenewald will be charged

under the commercial requester fee schedule (i.e., all fees for search, review, and duplication are applicable if fees exceed \$15).

12. I will be representing DON at a meeting with DFOISR and the other military components to discuss changes to the DOD's FOIA Directive. If you have any recommended changes or concerns or wish issues discussed, please email your concerns to me at navyfoia@hq.navy.mil by 9 Nov 01.

13. This office strives to provide you with customer service and support. Accordingly, if you are in a time zone that makes us difficult to reach by telephone, please address your questions in an email and we will be happy to respond promptly. Our email address is navyfoia@hq.navy.mil. You can also fax us at (202) 685-6580, DSN 325-6580.

14. Finally, please accept my gratitude for the professionalism you continue to display in working your FOIA program. Ours is a tough job interacting with the public and meeting the demands of our respective commands. With little to no resources, we have creatively built impressive FOIA web sites, designed data bases to track requests, responded to complex and difficult requests in record time, and continue to weigh issues and bring up concerns in an effort to improve our program. I appreciate the interaction and proactivity that you have shown.



DORIS M. LAMA

By direction

(202) 685-6545/DSN 325-6545

**ENCLOSURE (4)**



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

5720  
Ser N09B10/1U514545  
20 Nov 01

From: Chief of Naval Operations  
To: E-Mail Distribution List (FOIA)  
Subj: UPDATE TO FOIA POLICY LETTER OF 26 OCT 01  
Ref: (a) CNO ltr Ser N09B10/1U514379 of 26 Oct 01

1. On November 9 and 19, 2001, the Department of Defense (DoD) issued policy guidance on the Freedom of Information Act (FOIA). Copies of their letters will be posted on the DoD web site at <http://www.defenselink.mil/pubs/foi/> guidance in the near future.

2. These policy letters address two issues: Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA) and DoD Guidance on Attorney General Freedom of Information Act (FOIA) Memorandum.

3. Prior to the issuance of these two policy letters, reference (a) was issued. Paragraph 5 stated that Department of the Navy (DON) activities could cite to both exemptions (b)(2) and (b)(6) as a basis to withhold certain names and addresses. After coordination with the Department of Justice, DoD has determined that exemption (b)(2) should not normally be cited. Accordingly, based on DoD's policy memo of 9 Nov 01, please only cite to exemption (b)(6), unless you can make a strong case to also cite to exemption (b)(2) [i.e., exemption (b)(6) does not fully protect DON's or an individual's interests].

4. The DoD policy memo of 9 Nov 01 contains the following guidance: Effective immediately, personally identifiable information (to include lists of e-mail addresses) in the categories listed below must be carefully considered and the interests in supporting withholding of the information given more serious weight in the analysis. This information may be found to be exempt under 5 U.S.C. 552(b)(6) because of the heightened interest in the personal privacy of DoD personnel that is concurrent with

the increased security awareness demanded in time of national emergency.

a. Lists of personally identifying information of DoD personnel: All DoD components shall ordinarily withhold lists of names and other personally identifying information of personnel currently or recently assigned within a particular component, unit, organization, or office with the DoD in response to requests under the FOIA. This is to include active duty military personnel, civilian employees, contractors, members of the National Guard and Reserves, military dependents, and Coast Guard personnel when the Coast Guard is operating as a service in the Navy. If a particular request does not raise security or privacy concerns, names may be released as, for example a list of attendees at a meeting held more than 25 years ago. Particular care shall be taken prior to any decision to release a list of names in any electronic format.

b. Verification of status of named individuals: DoD components may determine that release of personal identifying information about an individual is appropriate only if the release would not raise security or privacy concerns and has been routinely released to the public.

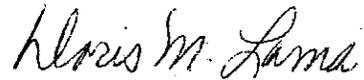
c. Names in documents that don't fall into the preceding categories: Ordinarily names of DoD personnel, other than lists of names, mentioned in documents that are releasable under the FOIA should not be withheld, but in special circumstances where the release of a particular name would raise substantial security or privacy concerns, such as a name may be withheld.

5. This policy does not preclude a DON activity from making a discretionary release of names and duty information of personnel who, by the nature of their position and duties, frequently interact with the public, such as flag/general officers, public affairs officers, or other personnel designated as official command spokespersons.

6. DON activities will continue to claim exemption (b)(3), specifically 10 U.S.C. 130b, to protect the names and duty station addresses of DON personnel who are stationed overseas, routinely deployable, or assigned to a sensitive unit.

7. This policy letter is being e-mailed/faxed to you for immediate implementation and dissemination to those activities that report to you. As always, our policy letters are posted under FOIA Resource Materials at [foia.navy.mil/](http://foia.navy.mil/).

8. If you have any questions, please don't hesitate to contact the undersigned or Tracy Ross, (202) 685-6546.

A handwritten signature in cursive script that reads "Doris M. Lama".

DORIS M. LAMA

By direction

(202) 685-6545/DSN 325-6545

**ENCLOSURE (5)**

**System name:**

**Organization Locator and Social Roster** (December 1, 2000, 65 FR 75260).

**System location:**

Organizational elements of the Department of the Navy. Official mailing addresses are published as an appendix to the Navy's compilation of systems of records notices

Commander in Chief, U.S. Joint Forces Command, 1562 Mitscher Avenue, Suite 200, Norfolk, VA 23551-2488.

Commander in Chief, U.S. Pacific Command, PO Box 64028, Camp H.M. Smith, HI 96861-4028.

**Categories of individuals covered by the system:**

Military and civilian personnel attached to the activity, Departments of the Navy and Defense, or other government agencies; family members; and guests or other invitees.

**Categories of records in the system:**

Manual or mechanized records. Includes information such as names, addresses, telephone numbers; official titles or positions and organizations; invitations, acceptances, regrets, protocol, and other information associated with attendants at functions. Locator records of personnel attached to the organization.

**Authority for maintenance of the system:**

5 U.S.C. 301, Departmental Regulations and E.O. 9397 (SSN).

**Purpose(s) :**

To notify personnel of arrival of visitors; recall personnel to duty station when required; locate individuals on routine matters; provide mail distribution and forwarding addresses; compile a social roster for official and non-official functions; send personal greetings and invitations; and locate individuals during medical emergencies, facility evacuations, and similar threat situations.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

The 'Blanket Routine Uses' that appear at the beginning of the Navy's compilation of systems of records notices apply to this system.

**Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**

**Storage:**

Manual and automated records.

**Retrievability:**

Name, Social Security Number, and/or organization code.

**Safeguards:**

Documents are marked 'FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE' and are only distributed to those persons having an official need to know. Computerized records are password protected and only accessible by those persons with an official need to know.

**Retention and disposal:**

Records are destroyed upon update of roster to add/delete individuals who have arrived/departed the organization.

**System manager(s) and address:**

Commanding officer of the activity in question. Official mailing addresses are published as an appendix to the Navy's compilation of systems of records notices.

**Notification procedure:**

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Commanding officer of the activity in question. Official mailing addresses are published as an appendix to the Navy's compilation of systems of records notices.

**Record access procedures:**

Individuals seeking access to information about themselves contained in this system should address written inquiries to the Commanding officer of the activity in question. Official mailing addresses are published as an appendix to the Navy's compilation of systems of records notices.

**Contesting record procedures:**

The Navy's rules for accessing records, and for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5; 32 CFR part 701; or may be obtained from the system manager.

**Record source categories:**

Individual and records of the activity.

**Exemptions claimed for the system:**

None.

**ENCLOSURE (6)**



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20380-2000

5211 IN REPLY REFER TO  
Ser N09B10/2U512894  
22 Mar 02

From: Chief of Naval Operations  
To: Distribution List

Subj: PRIVACY ACT (PA) POLICY ISSUES

Ref: (a) SECNAVINST 5211.5D

1. Please ensure distribution of this policy memo. It will be posted on the Navy's PA On-line Web Site at [privacy.navy.mil/](http://privacy.navy.mil/).

2. Just a reminder, all Navy Privacy Act systems of records are downloadable from our web site at [privacy.navy.mil](http://privacy.navy.mil/). You can also download Marine Corps, DoD and its components, and Government-wide systems from this site. As systems are added, deleted, altered, or amended the site is updated to reflect those changes. Systems managers are responsible for ensuring that CNO (N09B10) is apprised of any changes.

3. As a result of recent inquiries and the incidents of September 11, there is a concerted effort to ensure that our personnel can be contacted. Many activities are involved in updating and/or creating Recall/Social Rosters. The following information is provided to assist you:

a. Recall/Social Rosters

(1) The collection of personal information to formulate or update a Recall/Social Roster is permitted under the Navy's Privacy Act systems notice N05000-3, Organizational Locator and Social Roster.

(2) When directly soliciting personal information from an individual, activities are reminded of the need to include a Privacy Act Statement (PAS) whether the solicitation is done in writing or electronically. A sample PAS for use in requesting information for a recall/social roster is as follows:

Authority: 5 U.S.C. 301, Departmental Regulations and E.O. 9397 (SSN).

Purpose: To notify personnel of office closings; locate personnel and/or next of kin in case of emergency; invite personnel to social functions; recall personnel as necessary.

Routine Uses: Information is close-hold and shared with only those with a need-to-know. Supervisory personnel will have access to information concerning their employees. Administrative/web personnel will have access for purposes of maintaining the data base. Disclosure of information is treated as "For Official Use Only - Privacy Sensitive."

Disclosure: Mandatory for military. Mandatory for civilian employees who have been designated by their organization as "emergency personnel." Voluntary for all others. However, failure to provide information may result in them or their family not being accounted for or contacted during an emergency, invited to a social gathering, etc.

(3) Once the list is compiled, it should be marked "For Official Use Only - Privacy Sensitive - Any misuse or unauthorized disclosure may result in civil and criminal penalties."

(4) Dissemination of this list and access to all or part of the list is driven by an official need-to-know. In many cases, activities will limit access to those individuals who need to have access to specific information, rather than the entire recall roster. For example, the Commanding Officer and Executive Officer may require access to the entire roster, while a Division Director may only require access to information on individuals under his/her division.

(5) When is collection mandatory? Collection is mandatory if the agency is able to impose a penalty on the individual for failing to provide the information. For example, it is mandatory for members of the military because it is a lawful order. Failure to comply with a lawful order may result in disciplinary action being taken.

(6) Posting your recall roster on an Intranet web site: The document must be properly marked and access to all or part of the document should be limited to those officials having an official need-to-know. An effective tool is password access.

b. Collecting and posting photographs of individuals on an Intranet site:

(1) Some activities collect and maintain photographs of their employees. For example, public works centers maintain photographs of their personnel since they do not report to a regular office location and must be identified in case of emergency. Security offices maintain photographs of individuals who are issued badges.

(2) Activities are reminded, however, that while collection of photographs may be permissible, safeguards must be in place to ensure that only those individuals with an official need-to-know have access. There is a clear distinction between need-to-know and want-to-know. Need-to-know is defined as official requirement in line with why the information is being collected.

c. Processing requests that cite the Privacy Act

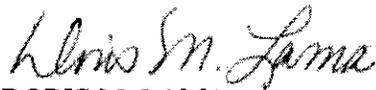
(1) When a person cites to the Privacy Act in a request, the activity's response letter must address whether or not the request is being processed under the provisions of the Privacy Act. For example, "Your request is not being processed under the provisions of the Privacy Act since the information you seek is not contained in a Privacy Act systems of records notice which is retrieved by your name and personal identifier. Hence, your request is being processed under the provisions of the Freedom of Information Act." Or, "Your request is being denied under the provisions of the Privacy Act under exemption \_\_\_\_\_. Accordingly, your request is being processed under the provisions of the Freedom of Information Act."

(2) When processing any request, activities must review all documents associated with the request. For example, if you are reviewing an investigation that lists enclosures, the enclosures must be processed unless the requester has asked for only the basic investigation.

(3) In compliance with Department of Justice reporting requirements, all Privacy Act requests must be counted as Freedom of Information Act requests.

d. The DOJ book, Freedom of Information Act Guide and Privacy Act Overview is being revised and is expected to be received by July. This publication is issued every other year. If you need a copy, please fax your requirement to this office at (202) 685-6580, Attn: Cassandra Bennett. Limited copies of the Case List will also be available.

4. Privacy Act issues/questions: This staff is available to answer your questions. You can call us at (202) 685-6545/46 or email us at navyfoia@hq.navy.mil.



DORIS M. LAMA

By direction

(202) 685-6545/DSN 325-6545

**Distribution:**

USCINCPAC (J1411)  
USCINCFCOM (J024)  
ASN (M&RA)  
HROC  
S/HHRO  
CMC (Code ARAD)  
CINCUSNAVEUR (Code 0132)  
CINCLANTFLT (Code N02P6)  
COMNAVAIRLANT (Code N02L)  
COMNAVSUBLANT (Code N02L1)  
COMNAVSURFLANT (Code N02L)  
CINCPACFLT (Code N00JPL)  
COMNAVAIRPAC (Code N01J)  
COMNAVSUBPAC (Code 00J)  
COMNAVSURFPAC (Code N00J)  
BCNR  
BUMED (Code 00L1)  
CNET (Code OOJE)  
CNR (Code OOC)  
COMNAVAIRSYSYSCOM (Code 7.7.6)  
COMNAVCRUITCOM (Code 017)  
COMNAVFACENCOM (Code OOC)  
COMNAVMETOCOM (Code 01L)  
COMNAVNETOPSCEN (Code 014A)  
COMNAVPERSCOM (Pers-06)  
COMNAVREG NE  
COMNAVREG MIDLANT  
COMNAVREG SE

COMNAVREG NW  
COMNAVREG SW  
COMNAVREG HI  
COMNAVRESFOR (Code 003)  
COMNAVRESPERSCEN  
COMNAVSAFECEN (Code 03)  
COMNAVSEASYSYSCOM (Code 09T3)  
COMNAVSECGRU (Code N00J)  
COMNAVSPACECOM (Code N171)  
COMSPECWARCOM (Code 004)  
COMNAVSUPSYSYSCOM (Code 939A)  
COMSPAWARYSYSCOM (Code 00C)  
JAG (Code 13)  
JAG (Code 14)  
MSC [Code N9(FOIA)]  
NAVAUDSVCHQ  
NAVINSGEN (Code OOL1)  
NAVPGSCOL (Code 006)  
NAVOBSY (Code AS)  
NAVSTKAIRWARCEN FALLON NV  
NAVWARCOL (Code 009)  
NCIS (Code 00JF)  
NCPB (Code 0031)  
NDW (Code N007)  
OGC (Mr. Fredman)  
ONI (Code OCB3)  
SSP (SP-104)  
USNA (Code 1E)

**ENCLOSURE (7)**



DEPARTMENT OF THE NAVY  
HEADQUARTERS UNITED STATES MARINE CORPS  
2 NAVY ANNEX  
WASHINGTON, DC 20380-1775

IN REPLY REFER TO:

5720  
ARSE/3U100263  
19 Feb 03

From: Commandant of the Marine Corps  
To: Distribution List

Subj: NOTICE OF POLICY CHANGES TO THE DEPARTMENT OF THE NAVY  
(DON) FREEDOM OF INFORMATION ACT (FOIA) PROGRAM

Encl: (1) CNO ltr 5720 N09B10/3U507352 of 8 Jan 03  
(2) CNO ltr 5720 N09B10/2U514304 of 20 Nov 02 (w/ encls)

1. Please ensure widest dissemination of this information.
2. The Director, Freedom of Information and Security Review (DFOISR), Office of the Secretary of Defense, has instructed that any DoD component receiving a FOIA request for copies of the intercepted communications referenced by Secretary Powell at the U.N. or for related material, should immediately refer the FOIA request to the Department of State. Any FOIA request seeking intercepted communications not specifically referenced or revealed by Secretary Powell should be referred directly to DFOISR. This procedure must be followed whether the component has responsive information or not. However, DFOISR asks that any component who receives such a request call Mr. Jim Hogan at (703) 697-5412 or DSN 227-5412 before referring the request or corresponding with the requester.
3. In a recent U.S. District Court, District of Columbia, FOIA lawsuit (Electronic Privacy Information Center (EPIC) v. DoD), Judge John Bates has ruled that EPIC qualifies for "news media" status. Based on this decision, it is recommended you handle all current and future EPIC FOIA requests as media requests. Formal FOIA policy on this issue is expected from DFOISR in the near future. Judge Bates' decision can be found at <http://www.dcd.uscourts.gov/02-1233.pdf>.
4. By Enclosure (1), the DON FOIA Policy Office apprises of the Congressional passage of the Intelligence Authorization Act for FY 2003, Public Law 107-306, which amends the (a)(3) provision of FOIA. The new language effectually now precludes any covered intelligence agency from disclosing records in response to FOIA requests from any foreign government or international government

Subj: NOTICE OF POLICY CHANGES TO THE DEPARTMENT OF THE NAVY  
(DON)FREEDOM OF INFORMATION ACT (FOIA) PROGRAM

organization. FOIA policy guidance is expected from DFOISR within 30 to 60 days. In the interim, intelligence activities receiving such requests should contact this office for guidance.

5. Enclosure (1) also apprises of an implemented change to paragraph 14k of reference (a), which reflects that the Auditor General of the Navy is now the sole release/denial authority for Naval Audit Service reports. Accordingly, please ensure that all FOIA requests for Naval Audit Service reports are forwarded to the Auditor General of the Navy, Naval Audit Service, 1006 Beatty Place SE, Washington Navy Yard, DC 20374-5005, for processing.

6. By Enclosure (2), the DON FOIA Policy Office emphasizes the need to ensure that senior Navy/Marine Corps leadership is apprised of any FOIA request likely to receive media and/or congressional attention. Accordingly, in meeting this need, USMC activities receiving such requests are to immediately forward a copy of the request to the DON FOIA Policy Office by email at **NAVYFOIA@navy.mil** or by fax to (202) 685-6580. Your transmission should reference "ATTENTION FOIA" in the subject line to distinguish it from other email and faxes. Once received, the DON FOIA Policy Office will review the request and, if appropriate, disseminate to an established group of Navy/Marine Corps officials, along with other officials having a need to know. This dissemination will be accomplished by email using the subject line "ATTENTION FOIA."

7. The DFOISR has apprised this office that numerous Navy/Marine Corps activities have cited the Procurement Integrity Act (41 USC § 423) as an underlying statute for invoking exemption (b)(3) to withhold such documents as pre-award contractor bids/proposals, source selection information, etc. Since the Department of Justice (DOJ) has found 41 USC § 423 to be an invalid (b)(3) statute (see the May 2002 edition of the DOJ Freedom of Information Act Guide & Privacy Act Overview), USMC activities are to cease reliance on this statute for withholding pre-award and/or source selection documents.

8. All USMC FOIA Coordinators and action officers are reminded that FOIA requests seeking access to chemical, biological, radiological, and nuclear (CBRN) information require special handling. Please coordinate with this office immediately upon receipt of such a request. Additional information on this matter was .

Subj: NOTICE OF POLICY CHANGES TO THE DEPARTMENT OF THE NAVY  
(DON) FREEDOM OF INFORMATION ACT (FOIA) PROGRAM

provided by the DON FOIA Policy Office in a May 2002 policy memorandum which can be found on the DON FOIA On-Line website at <http://foia.navy.mil/020520policymemo.pdf>.

9. Additionally, USMC FOIA Coordinators and action officers are reminded that a new FOIA fee schedule went into effect on 1 Jul 02 that impacts search and review fees (duplication fees remain unchanged). Clerical hours are now assessed at \$20.00 per hour, professional hours at \$44.00 per hour, and executive hours at \$75.00 per hour. You may download the new DD Form 2086 from the DON FOIA website at <http://foia.navy.mil/resources.html>.

10. Questions concerning any of these issues may be directed to me at (703) 614-4008 or emailed to me at [rosstd@hqmc.usmc.mil](mailto:rosstd@hqmc.usmc.mil).



TERESA D. ROSS

By direction

Distribution:

|  |                             |
|--|-----------------------------|
| MARFORLANT NORFOLK VA                      | 2D MARDIV CAMP LEJEUNE NC   |
| MARFORPAC CAMP SMITH HI                    | 3D MARDIV OKINAWA JA        |
| MARFORRES NEW ORLEANS LA                   | 1ST FSSG CAMP PENDLETON CA  |
| MARFORSOUTH MIAMI FL                       | 2D FSSG CAMP LEJEUNE CA     |
| MARFOREUR PANZER KASERNE,<br>BOEBLINGEN GE | 3D FSSG OKINAWA JA          |
| MARCORLOGBASE ALBANY GA                    | 1ST MAW OKINAWA JA          |
| MARCORSYSCOM ALBANY GA                     | 2D MAW MCAS CHERRY POINT NC |
| MARCORBASESPAC CAMP SMITH HI               | 3D MAW MCAS MIRAMAR CA      |
| FMFLANT CAMP LEJEUNE NC                    | MAGTFTC 29 PALMS CA         |
| FMFPAC CAMP SMITH HI                       | CG ERR PARRIS ISLAND SC     |
| I MEF CAMP PENDLETON CA                    | CG WRR SAN DIEGO            |
| II MEF CAMP LEJEUNE NC                     | JLC MCAS CHERRY PONT NC     |
| III MEF OKINAWA JA                         | JLC MCAS MIRAMAR CA         |
| 1ST MARDIV CAMP PENDLETON CA               | DLC MCRD PARRIS ISLAND SC   |



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20380-2000

IN REPLY REFER TO

5720  
Ser N09B10/3U507352  
8 Jan 03

From: Chief of Naval Operations  
To: Email Distribution List (FOIA)  
Subj: DON FOIA PROGRAM UPDATE/POLICY CHANGE  
Ref: (a) SECNAVINST 5720.42F

1. On November 15, 2002, Congress passed the Intelligence Authorization Act for FY 2003, Public Law 107-306. Signed by President Bush on November 27, 2002, the legislation amended the (a)(3) provision of the Freedom of Information Act (FOIA) as follows:

SEC. 312. PROHIBITION ON COMPLIANCE WITH REQUESTS FOR INFORMATION SUBMITTED BY FOREIGN GOVERNMENTS.

Section 552(a)(3) of title 5, United States Code, is amended--

(1) in subparagraph (A) by inserting "and except as provided in subparagraph (E)," after "of this subsection,"; and

(2) by adding at the end the following:

"(E) An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) shall not make any record available under this paragraph to--

"(i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or

"(ii) a representative of a government entity described in clause (i)."

2. In effect, this new statutory language in the FOIA now precludes any covered intelligence agency from disclosing records in response to any FOIA request that is made by any foreign government or international

governmental organization. By its terms, it prohibits disclosure in response to requests made by such other-than-U.S. governmental entities either directly or through a "representative." This amendment will impact the Department of the Navy. I along with OSD and the other DoD Components are examining the change and discussing the impact and how to implement within DoD. Because there are a lot of issues to resolve, I anticipate policy guidance being issued within the next 30-60 days. In the interim, intelligence activities receiving such requests should contact this office for guidance. You can review DOJ's analysis at FOIA Post (see Resource Materials at foia.navy.mil).

3. This office has also been rewriting paragraph 14 to reference (a), "Processing Specific Kinds of Records," in an effort to incorporate policy changes, administrative changes, and the recent amendment to the FOIA. One change that has been staffed and can be immediately implemented is paragraph 14k, Naval Audit Service Reports. Please change paragraph 14k to reference (a) to read as follows:

k. Naval Audit Service Reports

(1) The Auditor General of the Navy is the release/denial authority for Navy Audit reports. All requests for Naval Audit Service reports shall be promptly referred to the Auditor General of the Navy, Naval Audit Service, 1006 Beatty Place SE, Washington Navy Yard, DC 20374-5005 for action. Activities locating Naval Audit Service reports or portions thereof in their files in response to a FOIA request, shall refer those documents to the Naval Audit Service for their review and direct response to the requester. In both instances, activities shall notify the requester of the referral.

(2) Findings and recommendations in a final audit report to which management disagrees encompass the final findings and recommendations of the Auditor General of the Navy. Prior to the Auditor General's public disclosure of a final audit report that contains undecided issues, the Auditor General shall provide affected activities the opportunity to comment on public disclosure of any undecided findings or recommendations. Such findings and recommendations will not change as a result of the audit resolution process with management. However, such final reports may not reflect management's final resolution on

the issues raised in the audit and may be deliberative to management's decision-making process. Accordingly, it is appropriate for the Auditor General to initially claim exemption (b)(5) to withhold from public disclosure undecided issues in a final audit report.

(3) If the Auditor General decides to initially withhold contested findings or recommendations under the deliberative process privilege of exemption (b)(5) of the FOIA, a disclosure shall be made of any withheld information no later than six months from the date of issuance of the final audit report.

(4) When a disclosure of a final report containing undecided issues is made, the Auditor General shall notify the FOIA requester that the final report contains such undecided issues. In addition, the Auditor General will refer the request to the Naval IG for release to the requester of the IG addendum that reflects the completion of the audit resolution process.

(5) Prior to release of a final audit report under FOIA, the Auditor General shall notify the Secretary of the Navy; Under Secretary of the Navy; Director, Navy Staff and/or Director, Marine Corps Staff; Chief, Office of Information; Office of Legislative Affairs; Assistant Secretary of the Navy (EMB); and other DON offices responsible for implementing audit recommendations.

4. The DON FY 2002 Annual FOIA Report is now available under [foia.navy.mil/](http://foia.navy.mil/). Go to the electronic reading room and download it from the SECNAV/OPNAV reading room.

5. NMCI has arrived resulting in the change to our email addresses. You can email me at [navyfoia@navy.mil](mailto:navyfoia@navy.mil) or [doris.lama@navy.mil/](mailto:doris.lama@navy.mil). Sarah English's contact information has changed as follows: email: [sarah.english@navy.mil](mailto:sarah.english@navy.mil); telephone number 202-685-6546; Code N09B10C.

6. The change to paragraph 14 will be made in the next update to reference (a). Please ensure widest dissemination.

*Doris M. Lama*

DORIS M. LAMA

By direction

(202) 685-6545/DSN 325-6545



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

5720  
Ser N09B10/2U514304  
20 Nov 02

From: Chief of Naval Operations

Subj: FREEDOM OF INFORMATION ACT (FOIA) POLICY LETTER

Ref: (a) SECNAVINST 5720.42F, Department of the Navy FOIA Program  
(b) SECNAVINST 5720.44A, Department of the Navy Public Affairs Policy and Regulations

Encl: (1) Sample listing of topics

1. This policy memo is being emailed to you. Please ensure widest dissemination. It will be posted at <http://foia.navy.mil> under Resource Materials.
2. While the Department of the Navy's (DON's) FOIA program is decentralized, there is a need to ensure that our senior Navy/Marine Corps leadership is apprised of any FOIA requests that are likely to receive media or congressional attention. Enclosure (1) contains a sample listing of topics that may result in media or congressional attention.
3. Upon receipt of a request that may receive media or congressional attention, DON activities shall:
  - a. Email a copy of that request to [NAVYFOIA@navy.mil](mailto:NAVYFOIA@navy.mil) or fax it to CNO (N09B10) at 202-685-6580. Please place "ATTENTION FOIA" in the subject line to distinguish it from other emails; and,
  - b. If from the media, follow the guidance set forth in paragraph 14 to reference (a) and guidance prescribed in reference (b).
4. Once received, CNO (N09B10) will review the request and if appropriate disseminate it to an established group of senior Navy/Marine Corps officials along with other officials having an official need to know. This will be done via email using the subject line "ATTENTION FOIA."

5. This requirement is effective immediately and will be incorporated in reference (a) during the next rewrite. Please contact the undersigned with any questions you may have.



DORIS M. LAMA

By direction

(202) 685-8545/DSN 325-6545

Distribution  
FOIA Email List 1

## **SAMPLE OF TOPICS THAT MAY REQUIRE HIGH-LEVEL NOTIFICATION**

**Cases that have major litigative impact**

**Homeland security**

**Hot issues (e.g., Guantanamo Bay detainees, accidents, Vieques, A-12, etc)**

**International incidents**

**Investigations (e.g., senior officials, major contractors, major programs, major fraud, theft of major government property, espionage, etc)**

**Major programs (e.g., weapons, BRAC, environment, homeporting, etc)**

**Senior officials (e.g., pay bonuses, ethics issues, etc)**

**Sweeping press inquiries that have Navy-wide interest**

**Major historical issues (e.g., Pearl Harbor detainees, etc)**

**Major personnel issues (e.g., military selection boards, women in the military, don't ask-don't tell policy; family advocacy; morale and welfare, etc)**

**Navy realignment issues**

**War on drugs**

**War on terrorism**

**White House/Vice President issues**