



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

5720 IN REPLY REFER TO  
Ser N09B10/2U512929  
27 Mar 02

From: Chief of Naval Operations  
To: E-Mail Distribution List (FOIA)  
Subj: FOIA POLICY LETTER - SAFEGUARDING INFORMATION REGARDING  
WEAPONS OF MASS DESTRUCTION AND OTHER SENSITIVE RECORDS  
RELATED TO HOMELAND SECURITY  
Encl: (1) Guidance on Homeland Security  
(2) Attorney General Ashcroft's Memo of October 12, 2001

1. Both the White House and Information Security Oversight Office (ISOO) issued memorandums on March 19, 2002, regarding what actions departments and agencies need to take to safeguard information regarding weapons of mass destruction and other sensitive documents related to homeland security. See enclosure (1).

2. The Department of Defense's Chief, Freedom of Information Act (FOIA) Division in the Freedom of Information and Security Review Directorate, requested that we make our activities aware of the policy set forth in these memoranda and take steps to ensure that all DON activities comply with such guidance when processing FOIA requests.

3. You are advised to immediately adopt the steps addressed in the ISOO memorandum at enclosure (1) when conducting a review of documents requested under FOIA. Please pay particular attention to Attorney General Ashcroft's memorandum of October 12, 2001 [enclosure (2)] by giving full and careful consideration to all applicable FOIA exemptions when processing documents that fall under this category.

4. The Department of Justice (DOJ) will issue its update of the Freedom of Information Act Guide and Privacy Act Overview sometime in July 2002. We have already ordered copies of this book along with a few of the revised FOIA Case List. If you would like to receive these publications, please fax your requirements to this office at (202) 685-6580 or e-mail your request to [navyfoia@hq.navy.mil](mailto:navyfoia@hq.navy.mil). Include your complete mailing address and telephone number. Please be advised that both the Office of the General Counsel and Headquarters Marine Corps will be making distributions to their constituencies.

5. The FOIA Post, an electronic publication that replaced FOIA Update, is issued by DOJ and posted on the Internet at <http://www.usdoj.gov/oip/foiapost/mainpage.htm>. We highly recommend that you routinely visit this site to learn of the most current news, developments, and guidance regarding the FOIA.

6. You are requested to ensure the widest dissemination of this policy memorandum to your reporting activities. Please address any questions/concerns to this office. Our e-mail address is [navyfoia@hq.navy.mil](mailto:navyfoia@hq.navy.mil). Our phone numbers are (202) 685-6545/6546 or DSN 325-6545/6546.

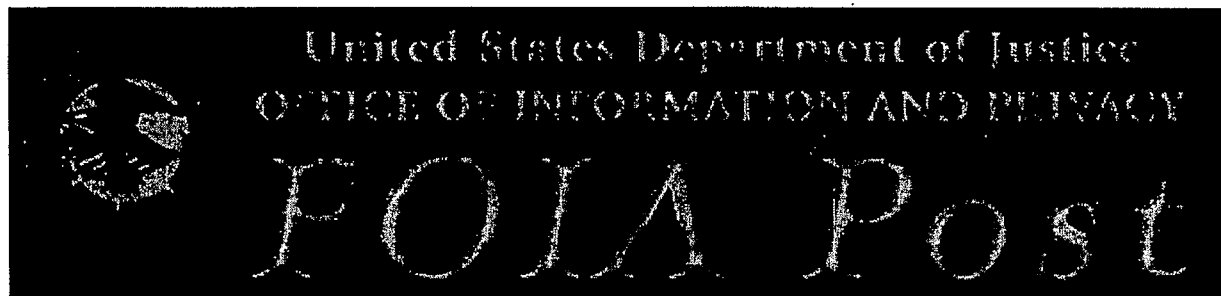
7. This policy memorandum and its attachments will be posted under resource materials on our Internet website at <http://foia.navy.mil>.



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

Distribution:

SECNAV (SAL)	CNR	COMNAVSURFPAC
OGC	COMNAVAIRLANT	COMNAVSUPSYSCOM
JAG (CODE 13)	COMNAVAIRPAC	COMSCOM
JAG (CODE 14)	COMNAVAIRSYSCOM	COMUSNAVCENT
JAG (CODE 15)	COMNAVCRUITCOM	HROC
OLA	COMNAVFACENGCOM	NAVAUDITSVC
ASN (F&MC)	COMNAVMETOCCOM	NAVINGEN
ASN (I&E)	COMNAVPERSCOM	NAVMECIACEN
ASN (M&RA)	COMNAVREGHI	NAVNETOPCEN
ASN (RD&A)	COMNAVREGMIDLANT	NAVOBSY
CNO (N00J)	COMNAVREGNE	NAVPGSCOL
CNO (N09BL)	COMNAVREGNW	NAVRESPERSCEN
CNO (N2J)	COMNAVREGSE	NAVSTRKAIRWARCEN
CNO (N3N5L)	COMNAVREGSW	NAVWARCOL
CNO (N45J)	COMNAVRESFOR	NCIS
CMC (ARAD)	COMNAVSAFECEN	NCPB
BCNR	COMNAVSEASYSYSCOM	NDW
BUMED	COMNAVSECGRU	NNMC BETHESDA MD
CHINFO	COMNAVSPACECOM	ONI
CINCLANTFLT	COMNAVSPAWARSYSCOM	PRESINSURV
CINCPACFLT	COMNAVSPECWARCOM	SSP
CINCUSNAVEUR	COMSUBLANT	USNA
CNATRA	COMSUBPAC	OPNAV Staff Offices
CNET	COMNAVSURFLANT	



## Guidance on Homeland Security Information Issued

The following memorandum regarding the safeguarding and protection of sensitive homeland security information was issued to the heads of all federal departments and agencies by the White House Chief of Staff on March 19. It forwards a memorandum from the Information Security Oversight Office and the Office of Information and Privacy, also set out below, which provides additional guidance on this important subject.

\*\*\*\*\*

### MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

**FROM:** ANDREW H. CARD, JR.  
Assistant to the President and Chief of Staff

**SUBJECT:** Action to Safeguard Information Regarding Weapons of Mass  
Destruction and Other Sensitive Documents Related to Homeland  
Security

As noted in many discussions during the past several months, you and your department or agency have an obligation to safeguard Government records regarding weapons of mass destruction. Weapons of mass destruction include chemical, biological, radiological, and nuclear weapons. Government information, regardless of its age, that could reasonably be expected to assist in the development or use of weapons of mass destruction, including information about the current locations of stockpiles of nuclear materials that could be exploited for use in such weapons, should not be disclosed inappropriately.

I asked the Acting Director of the Information Security Oversight Office and the Co-Directors of the Justice Department's Office of Information and Privacy to prepare guidance for reviewing Government information in your department or agency regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation and the safety of our people. Their guidance is attached, and it should be distributed to appropriate officials within your department or agency, together with this memorandum, to assist in your undertaking an immediate reexamination of current measures for identifying and safeguarding all such information at your department or agency.

All departments and agencies should review their records management

procedures and, where appropriate, their holdings of documents to ensure that they are acting in accordance with the attached guidance. They should report the completion, or status, of their review to this office through the Office of Homeland Security no later than 90 days from the date of this memorandum.

If agency officials need assistance in determining the classification status of records related to the development or use of weapons of mass destruction, they should contact the Information Security Oversight Office, at 202-219-5250. For assistance in determining the classification of nuclear and radiological weapons classified under the Atomic Energy Act, they should contact the Department of Energy's Office of Security, at 202-586-3345. If they need assistance in applying exemptions of the Freedom of Information Act (FOIA) to sensitive but unclassified information, they should contact the Justice Department's Office of Information and Privacy (OIP), at 202-514-3642, or consult OIP's FOIA Web site at [www.usdoj.gov/04foia/index/html](http://www.usdoj.gov/04foia/index/html).

\* \* \* \* \*

#### MEMORANDUM FOR DEPARTMENTS AND AGENCIES

FROM: LAURA L.S. KIMBERLY  
Acting Director  
Information Security Oversight Office

RICHARD L. HUFF  
DANIEL J. METCALFE  
Co-Directors  
Office of Information and Privacy  
Department of Justice

SUBJECT: Safeguarding Information Regarding Weapons of Mass Destruction  
and Other Sensitive Records Related to Homeland Security

At the request of the Assistant to the President and Chief of Staff, we have prepared this memorandum to provide guidance for reviewing Government information regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation or threaten public safety. It is appropriate that all federal departments and agencies consider the need to safeguard such information on an ongoing basis and also upon receipt of any request for records containing such information that is made under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000). Consistent with existing law and policy, the appropriate steps for safeguarding such information will vary according to the sensitivity of the information involved and whether the information currently is classified.

#### I. Classified Information

- If the information currently is classified and is equal to or less than 25 years old, it should remain classified in accordance with Executive Order 12958, Sec. 1.5 and Sec. 1.6. Although classified information generally must be declassified within 10 years of its original classification, classification or reclassification may be extended for up to 25 years in the case of information that could reasonably be expected to "reveal information that would assist in the development or use of weapons of mass destruction." Id., Sec. 1.6(d)(2).

- If the information is more than 25 years old and is still classified, it should remain classified in accordance with Executive Order 12958, Sec. 3.4(b)(2), which authorizes agency heads to exempt from automatic declassification any "specific information, the release of which should be expected to . . . reveal information that would assist in the development or use of weapons of mass destruction." (Agencies should note that the automatic declassification date for any classified information over 25 years old that involves the equities of more than one agency was extended until April 2003 by Executive Order 13142. Agencies have until then to exempt such information from automatic declassification under any one of the pertinent exemption categories in Executive Order 12958, Sec. 3.4(b).)

In this regard, agencies should note that Department of Defense (DOD) information that involves the equities of more than one DOD component is considered to have multi-agency equities. Information maintained by the Defense Technical Information Center (DTIC) or the National Archives and Records Administration (NARA) also is deemed to have multi-agency equities, i.e., those pertaining to DTIC or NARA and those pertaining to the component agency or agencies that created the information.

## II. Previously Unclassified or Declassified Information

- If the information, regardless of age, never was classified and never was disclosed to the public under proper authority, but it could reasonably be expected to assist in the development or use of weapons of mass destruction, it should be classified in accordance with Executive Order 12958, Part 1, subject to the provisions of Sec. 1.8(d) if the information has been the subject of an access demand (or Sec 6.1(a) if the information concerns nuclear or radiological weapons).
- If such sensitive information, regardless of age, was classified and subsequently was declassified, but it never was disclosed to the public under proper authority, it should be reclassified in accordance with Executive Order 12958, Part 1, subject to the provisions of Sec. 1.8(d) if the information has been the subject of an access demand (or Sec 6.1(a) if the information concerns nuclear or radiological weapons).

## III. Sensitive But Unclassified Information

In addition to information that could reasonably be expected to assist in the development or use of weapons of mass destruction, which should be classified or reclassified as described in Parts I and II above, departments and agencies maintain and control sensitive information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958. The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.

All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all

applicable FOIA exemptions. See *FOIA Post*, "**New Attorney General FOIA Memorandum Issued**" (posted 10/15/01) (found at [www.usdoj.gov/oip/foiapost/2001foiapost19.htm](http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm)), which discusses and provides electronic links to further guidance on the authority available under Exemption 2 of the FOIA, 5 U.S.C. § 552(b)(2), for the protection of sensitive critical infrastructure information. In the case of information that is voluntarily submitted to the Government from the private sector, such information may readily fall within the protection of Exemption 4 of the FOIA, 5 U.S.C. § 552(b)(4).

As the accompanying memorandum from the Assistant to the President and Chief of Staff indicates, federal departments and agencies should not hesitate to consult with the Office of Information and Privacy, either with general anticipatory questions or on a case-by-case basis as particular matters arise, regarding any FOIA-related homeland security issue. Likewise, they should consult with the Information Security Oversight Office on any matter pertaining to the classification, declassification, or reclassification of information regarding the development or use of weapons of mass destruction, or with the Department of Energy's Office of Security if the information concerns nuclear or radiological weapons.

\*\*\*\*\*

These memoranda are being made available through the Office of Information and Privacy's main FOIA Web site, as well as through *FOIA Post*, to encourage all agency FOIA personnel to be particularly aware of the careful attention that should be paid to any FOIA request that encompasses homeland security-related information. (posted 3/21/02)

Go to: [Main FOIA Post Page](#) // [DOJ FOIA Page](#) // [DOJ Home Page](#)

Office of the Attorney General  
Washington, D. C. 20530

October 12, 2001

MEMORANDUM FOR HEADS OF ALL FEDERAL DEPARTMENTS AND AGENCIES

FROM: John Ashcroft, Attorney General

SUBJECT: The Freedom of Information Act

As you know, the Department of Justice and this Administration are committed to full compliance with the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000). It is only through a well-informed citizenry that the leaders of our nation remain accountable to the governed and the American people can be assured that neither fraud nor government waste is concealed.

The Department of Justice and this Administration are equally committed to protecting other fundamental values that are held by our society. Among them are safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and, not least, preserving personal privacy.

Our citizens have a strong interest as well in a government that is fully functional and efficient. Congress and the courts have long recognized that certain legal privileges ensure candid and complete agency deliberations without fear that they will be made public. Other privileges ensure that lawyers' deliberations and communications are kept private. No leader can operate effectively without confidential advice and counsel. Exemption 5 of the FOIA, 5 U.S.C. § 552(b)(5), incorporates these privileges and the sound policies underlying them.

I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.

In making these decisions, you should consult with the Department of Justice's Office of Information and Privacy when significant FOIA issues arise, as well as with our Civil Division on FOIA litigation matters. When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.

This memorandum supersedes the Department of Justice's FOIA Memorandum of October 4, 1993, and it likewise creates no substantive or procedural right enforceable at law.

Go to: [DOJ FOIA Page](#) // [DOJ Home Page](#)