



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

APR 26 2002

OFFICE OF
ENVIRONMENTAL INFORMATION

MEMORANDUM

SUBJECT: Guidance on Homeland Security Information

FROM: Kim Nelson
Assistant Administrator and Chief Information Officer

TO: Assistant Administrators
General Counsel
Inspector General
Chief Financial Officer
Associate Administrators
Regional Administrators
Staff Office Directors

The purpose of this memorandum is to transmit to you a March 19, 2002, memorandum from Andrew H. Card, Jr., Assistant to the President and Chief of Staff. The Card Memorandum forwards a separate memorandum jointly issued by the Information Security Oversight Office (ISOO), and the Department of Justice's Office of Information and Privacy (the ISOO/DOJ Memorandum). These two memoranda address the issue of safeguarding Government information regarding weapons of mass destruction and other sensitive documents related to homeland security. They do not change the current policy of EPA concerning the handling of information, but suggest a heightened awareness when dealing with classified or otherwise sensitive information.

The ISOO/DOJ Memorandum addresses the treatment of classified information, as well as the procedure for properly classifying information that was previously unclassified or declassified under certain circumstances. EPA does not currently have original classification authority, and EPA's use of information classified by other departments or agencies is limited. EPA anticipates that it will be obtaining original classification authority in the near future.

Most importantly for EPA, the ISOO/DOJ Memorandum addresses the treatment of sensitive but unclassified information related to America's homeland security that might not meet one or more of the standards for classification. The need to protect such 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 information, especially scientific and technical information. All Freedom of Information Act (FOIA) requests for such information should be processed in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions. On November 20, 2001, Administrator Whitman transmitted the Attorney General's FOIA Memorandum to each of your offices. The Attorney General's FOIA Memorandum is attached, and can also be found, with additional guidance issued by DOJ, at <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>.

The ISOO/DOJ Memorandum counsels agencies that Exemption 2 of the FOIA should be used for the protection of sensitive critical infrastructure information. In addition, information that is voluntarily submitted to the Government from the private sector and claimed as confidential may readily fall within the protection of Exemption 4 of the FOIA (trade secret and confidential business information).

non-responsive portion has been removed



**United States Department of Justice
OFFICE OF INFORMATION AND PRIVACY**

FOIA Post



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.

. * * * * *

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

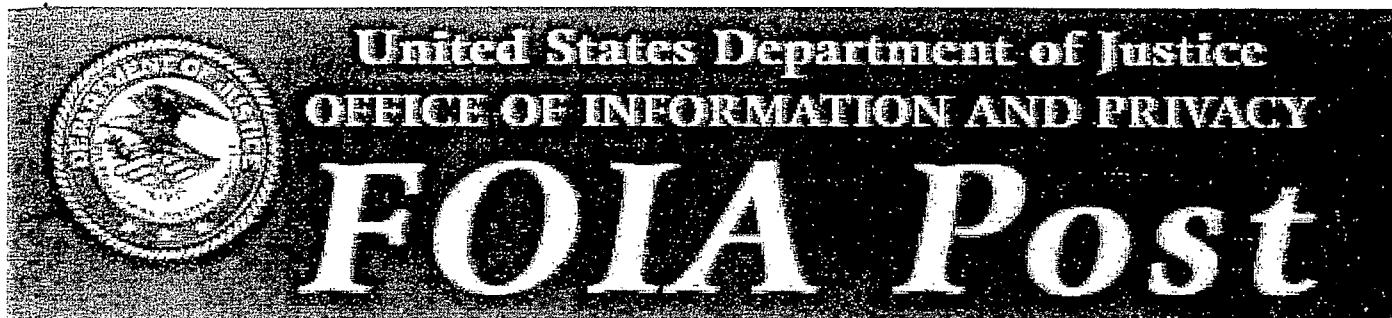
actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration 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), 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](#)



New Attorney General FOIA Memorandum Issued

A new statement of Administration policy on the Freedom of Information Act has been issued by Attorney General John Ashcroft and has been transmitted to all agencies across the executive branch of the federal government.

On October 12, Attorney General Ashcroft issued a memorandum to the heads of all departments and agencies that supersedes the Department of Justice FOIA policy memorandum that had been in effect since October 1993. The new Ashcroft FOIA Memorandum was effective immediately upon issuance, and the presidential statement on the FOIA that was issued in 1993 remains in effect as well.

The Ashcroft FOIA Memorandum emphasizes the Administration's commitment to full compliance with the FOIA as an important means of maintaining an open and accountable system of government. At the same time, it recognizes the importance of protecting the sensitive institutional, commercial, and personal interests that can be implicated in government records -- such as the need to safeguard national security, to maintain law enforcement effectiveness, to respect business confidentiality, to protect internal agency deliberations, and to preserve personal privacy.

In replacing the predecessor FOIA memorandum, the Ashcroft FOIA Memorandum establishes a new "sound legal basis" standard governing the Department of Justice's decisions on whether to defend agency actions under the FOIA when they are challenged in court. This differs from the "foreseeable harm" standard that was employed under the predecessor memorandum. Under the new standard, agencies should reach the judgment that their use of a FOIA exemption is on sound footing, both factually and legally, whenever they withhold requested information.

Significantly, the Ashcroft FOIA Memorandum also recognizes the continued agency practice of considering whether to make discretionary disclosures of information that is exempt under the Act, subject to statutory prohibitions and other applicable limitations. It also places particular emphasis on the right to privacy among the other interests that are protected by the FOIA's exemptions.

The text of the Ashcroft FOIA Memorandum is as follows:

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.

* * * * *

This policy memorandum was issued pursuant to the Attorney General's specific statutory responsibility "to encourage agency compliance with [the Freedom of Information Act]," 5 U.S.C. § 552(e)(5) (2000), a responsibility that the Department of Justice discharges in several ways, including through statements of FOIA policy. See, e.g., Department of Justice Calendar Year 2000 Annual FOIA Report at 99-107 ("Description of Department of Justice Efforts to Encourage Agency Compliance with the Act").

A new FOIA policy statement traditionally has been issued by the Attorney General at the beginning of a new Administration. Such statements were issued in May 1977 by Attorney General Griffin B. Bell, in May 1981 by Attorney General William French Smith, and in October 1993 by Attorney General Janet Reno. The Ashcroft FOIA Memorandum continues that tradition and in so doing calls attention to the administration of the FOIA at the highest levels of all agencies.

Additionally, the Office of Information and Privacy is disseminating this new FOIA policy memorandum to the principal administrative and legal FOIA contacts at all agencies, with the request that it be further disseminated as widely and expeditiously as possible through FOIA administrative channels within each agency. This dissemination should ensure that the memorandum reaches all FOIA personnel within each agency directly, in addition to through its distribution by each agency head.

OIP also will be both distributing and discussing the Ashcroft FOIA Memorandum at a FOIA Officers Conference to be held on October 18. A second topic to be discussed at this FOIA Officers Conference will be agency implementation of the electronic availability and annual reporting requirements of the Electronic Freedom of Information Act Amendments of 1996, in accordance with this past year's General Accounting Office Report entitled, "Progress in Implementing the 1996 Electronic Freedom of Information Act Amendments"). OIP issued a policy guidance memorandum on that subject earlier this year, see *FOIA Post*, "GAO E-FOIA Implementation Report Issued" (posted 3/23/01), and issued follow-up guidance on the preparation of annual FOIA reports as well, see *FOIA Post*, "Supplemental Guidance on Annual FOIA Reports" (posted 8/13/01).

Lastly, a third topic that will be discussed at this FOIA Officers Conference is one that has become a subject of greatly increased significance since the horrific events of September 11. In light of those events, and the possibilities for further terrorist activity in their aftermath, federal agencies are concerned with the need to protect critical systems, facilities, stockpiles, and other assets from security breaches and harm -- and in some instances from their potential use as weapons of mass destruction in and of themselves. Such protection efforts, of course, must at the same time include the protection of any agency information that could enable someone to succeed in causing the feared harm.

Protection for such records or information, if requested under the FOIA, is available under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2) (2000). Any agency assessment of, or statement regarding, the vulnerability of such a critical asset should be protected pursuant to Exemption 2. See *FOIA Update*, Vol. X, No. 3, at 3-4 ("OIP Guidance: Protecting Vulnerability Assessments Through Application of Exemption Two"). Beyond that, a wide range of information can be withheld under Exemption 2's "circumvention" aspect, sometimes referred to as "high 2," as is discussed in the "High 2: Risk of Circumvention" Subsection of the "Exemption 2" Section of the "Justice Department Guide to the Freedom of Information Act." Agencies should be sure to avail themselves of the full measure of Exemption 2's protection for their critical infrastructure information as they continue to gather more of it, and assess its heightened sensitivity, in the wake of the September 11 terrorist attacks.

Any question concerning the Ashcroft FOIA Memorandum, about implementation of the Electronic FOIA Amendments, about the use of Exemption 2 to provide necessary protection in the wake of terrorism, or about any aspect of FOIA administration can be

raised through the Office of Information and Privacy's FOIA Counselor service, at (202) 514-3642. (posted 10/15/01)

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