

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.