EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-08

February 11, 2005

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Designation of Senior Agency Officials for Privacy

The Administration is committed to protecting the information privacy rights of Americans and to ensuring Departments and agencies continue to have effective information privacy management programs in place to carry out this important responsibility. The President recently reaffirmed this commitment in the context of the War on Terror. In establishing the President's Board on Safeguarding Americans' Civil Liberties, the President directed agencies to "protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions." Executive Order 13353, Sec. 1 (August 27, 2004).

In furtherance of the Administration's commitment to protecting information privacy, OMB is today asking each executive Department and agency ("agency") to identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. Consistent with the Paperwork Reduction Act, the agency's Chief Information Officer (CIO) may perform this role. Alternatively, if the CIO, for some reason, is not designated, the agency may have designated another senior official (at the Assistant Secretary or equivalent level) with agency-wide responsibility for information privacy issues. In any case, the senior agency official should have authority within the agency to consider information privacy policy issues at a national and agency-wide level.

The senior agency official will have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. As is required by the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws and policies, each agency must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction. Agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies. And, agencies have the authority to conduct periodic reviews (e.g., as part of their annual FISMA reviews) to promptly identify deficiencies, weaknesses, or risks. When compliance issues are identified, agencies are obligated to take appropriate steps to remedy them.

The senior agency official shall have a central role in overseeing, coordinating, and facilitating the agency's compliance efforts. This role shall include reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date and, where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such procedures. Finally, the senior agency official shall ensure the agency's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information.

In addition to this compliance role, the senior agency official must also have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information. In evaluating these proposals, agencies must consider their potential impact on information privacy and take this impact into account in evaluating alternatives and making decisions. As OMB has previously explained, this type of evaluation needs to be conducted, for example, during the development of a new or significantly changed information system and during the promulgation of homeland security regulations.[1] In an agency's promulgation of other types of regulations that can have an impact on information privacy, or in its development of legislative proposals, testimony and comments under Circular A-19, agencies should similarly take into account the potential privacy impact, including identifying ways in which the agency can use technology to reinforce and sustain the privacy of personal information.

OMB appreciates your agency's continuing efforts in implementing and furthering the Administration's commitment to protecting information privacy. We are asking each agency, within 30 days of the date of this Memorandum, to provide OMB with the name, title and contact information (phone number and email address) for the senior agency official. This information should be provided to Ms. Eva Kleederman, Analyst for Privacy Policy, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, email Eva_Kleederman@omb.eop.gov.

This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, or any of its departments, agencies, entities, officers, employees, or agents, or any other person.

[1] *See* OMB Memorandum M-03-22 on the privacy impact assessments required by Section 208 of the E-Government Act of 2002, and OMB's 2003 Report to Congress on the Costs and Benefits of Federal Regulations, pp. 84-85.