ORAL ARGUMENT NOT YET SCHEDULED

No. 19-5031

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER,
Plaintiff-Appellant,

v.

UNITED STATES DEPARTMENT OF COMMERCE, et al.,
Defendants-Appellees.

On Appeal from an Order of the
U.S. District Court for the District of Columbia
Case No. 18-cv-2711-DLF

ADDENDUM OF APPELLANT

MARC ROTENBERG
ALAN BUTLER
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff-Appellant

INDEX TO ADDENDUM

Statutes

Constitutional Provisions

Regulations

STATUTES

U.S.C. Title 5 – Government Organization and Employees

5 U.S.C. § 702

A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof. An action in a court of the United States seeking relief other than money damages and stating a claim that an agency or an officer or employee thereof acted or failed to act in an official capacity or under color of legal authority shall not be dismissed nor relief therein be denied on the ground that it is against the United States or that the United States is an indispensable party. The United States may be named as a defendant in any such action, and a judgment or decree may be entered against the United States: Provided, That any mandatory or injunctive decree shall specify the Federal officer or officers (by name or by title), and their successors in office, personally responsible for compliance. Nothing herein (1) affects other limitations on judicial review or the power or duty of the court to dismiss any action or deny relief on any other appropriate legal or equitable ground; or (2) confers authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought.

5 U.S.C. § 704

Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review. A preliminary, procedural, or intermediate agency action or ruling not directly reviewable is subject to review on the review of the final agency action. Except as

otherwise expressly required by statute, agency action otherwise final is final for the purposes of this section whether or not there has been presented or determined an application for a declaratory order, for any form of reconsideration, or, unless the agency otherwise requires by rule and provides that the action meanwhile is inoperative, for an appeal to superior agency authority.

5 U.S.C. § 706

To the extent necessary to decision and when presented, the reviewing court shall decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action. The reviewing court shall—

(1) compel agency action unlawfully withheld or unreasonably delayed; and

(2) hold unlawful and set aside agency action, findings, and conclusions found to be—

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

(B) contrary to constitutional right, power, privilege, or immunity;

(C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right;

(D) without observance of procedure required by law;

(E) unsupported by substantial evidence in a case subject to sections 556 and 557 of this title or otherwise reviewed on the record of an agency hearing provided by statute; or

(F) unwarranted by the facts to the extent that the facts are subject to trial de novo by the reviewing court.

U.S.C. Title 6 – Domestic Security

6 U.S.C. § 394

(a) Regulations required

Within 1 year of November 25, 2002, the Federal Acquisition Regulation shall be revised to include regulations with regard to unsolicited proposals.

(b) Content of regulations

The regulations prescribed under subsection (a) of this section shall require that before initiating a comprehensive evaluation, an agency contact point shall consider, among other factors, that the proposal--

(1) is not submitted in response to a previously published agency requirement; and

(2) contains technical and cost information for evaluation and overall scientific, technical or socioeconomic merit, or cost-related or price-related factors.

U.S.C. Title 13 – Census

13 U.S.C. § 5

The Secretary shall prepare questionnaires, and shall determine the inquiries, and the number, form, and subdivisions thereof, for the statistics, surveys, and censuses provided for in this title.

13 U.S.C. § 141(a)

(a) The Secretary shall, in the year 1980 and every 10 years thereafter, take a decennial census of population as of the first day of April of such year, which date shall be known as the "decennial census date", in such form and content as he may

determine, including the use of sampling procedures and special surveys. In connection with any such census, the Secretary is authorized to obtain such other census information as necessary.

13 U.S.C. § 221

(a) Whoever, being over eighteen years of age, refuses or willfully neglects, when requested by the Secretary, or by any other authorized officer or employee of the Department of Commerce or bureau or agency thereof acting under the instructions of the Secretary or authorized officer, to answer, to the best of his knowledge, any of the questions on any schedule submitted to him in connection with any census or survey provided for by subchapters I, II, IV, and V of chapter 5 of this title, applying to himself or to the family to which he belongs or is related, or to the farm or farms of which he or his family is the occupant, shall be fined not more than $100.

(b) Whoever, when answering questions described in subsection (a) of this section, and under the conditions or circumstances described in such subsection, willfully gives any answer that is false, shall be fined not more than $500.

(c) Notwithstanding any other provision of this title, no person shall be compelled to disclose information relative to his religious beliefs or to membership in a religious body.

U.S.C. Title 15 – Commerce and Trade

15 U.S.C. § 1501

There shall be at the seat of government an executive department to be known as the Department of Commerce, and a Secretary of Commerce, who shall be the head thereof, who shall be appointed by the President, by and with the advice and

consent of the Senate, and whose term and tenure of office shall be like that of the heads of the other executive departments; and the provisions of title 4 of the Revised Statutes, including all amendments thereto, shall be applicable to said department. The said Secretary shall cause a seal of office to be made for the said department of such device as the President shall approve, and judicial notice shall be taken of the said seal.

U.S.C. Title 28 – Judiciary and Judicial Procedure

28 U.S.C. § 1291

The courts of appeals (other than the United States Court of Appeals for the Federal Circuit) shall have jurisdiction of appeals from all final decisions of the district courts of the United States, the United States District Court for the District of the Canal Zone, the District Court of Guam, and the District Court of the Virgin Islands, except where a direct review may be had in the Supreme Court. The jurisdiction of the United States Court of Appeals for the Federal Circuit shall be limited to the jurisdiction described in sections 1292(c) and (d) and 1295 of this title.

28 U.S.C. § 1331

The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.

28 U.S.C. § 2201

(a) In a case of actual controversy within its jurisdiction, except with respect to Federal taxes other than actions brought under section 7428 of the Internal Revenue Code of 1986, a proceeding under section 505 or 1146 of title 11, or in

any civil action involving an antidumping or countervailing duty proceeding regarding a class or kind of merchandise of a free trade area country (as defined in section 516A(f)(10) of the Tariff Act of 1930), as determined by the administering authority, any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such.

(b) For limitations on actions brought with respect to drug patents see section 505 or 512 of the Federal Food, Drug, and Cosmetic Act, or section 351 of the Public Health Service Act.

U.S.C. Title 44 – Public Printing and Documents

44 U.S.C. § 3501

The purposes of this subchapter are to—

***

(4) improve the quality and use of Federal information to strengthen decisionmaking, accountability, and openness in Government and society;

***

44 U.S.C. § 3502

As used in this subchapter—

***

(3) the term "collection of information"--

(A) means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either--

(i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or

(ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and

(B) shall not include a collection of information described under section 3518(c)(1);

44 U.S.C. § 3505(a)(1)

(a) In carrying out the functions under this subchapter, the Director shall--

(1) in consultation with agency heads, set an annual Governmentwide goal for the reduction of information collection burdens by at least 10 percent during each of fiscal years 1996 and 1997 and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001, and set annual agency goals to--

(A) reduce information collection burdens imposed on the public that–

(i) represent the maximum practicable opportunity in each agency; and

(ii) are consistent with improving agency management of the process for the review of collections of information established under section 3506(c); and

(B) improve information resources management in ways that increase the productivity, efficiency and effectiveness of Federal programs, including service delivery to the public;

44 U.S.C. § 3506(c)

(c) With respect to the collection of information and the control of paperwork, each agency shall--

(1) establish a process within the office headed by the Chief Information Officer designated under subsection (a), that is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved under this subchapter, to--

(A) review each collection of information before submission to the Director for review under this subchapter, including--

(i) an evaluation of the need for the collection of information;

(ii) a functional description of the information to be collected;

(iii) a plan for the collection of the information;

(iv) a specific, objectively supported estimate of burden;

(v) a test of the collection of information through a pilot program, if appropriate; and

(vi) a plan for the efficient and effective management and use of the information to be collected, including necessary resources;

(B) ensure that each information collection--

(i) is inventoried, displays a control number and, if appropriate, an expiration date;

(ii) indicates the collection is in accordance with the clearance requirements of section 3507; and

(iii) informs the person receiving the collection of information of--

(I) the reasons the information is being collected;

(II) the way such information is to be used;

(III) an estimate, to the extent practicable, of the burden of the collection;

(IV) whether responses to the collection of information are voluntary, required to obtain a benefit, or mandatory; and

(V) the fact that an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number; and

(C) assess the information collection burden of proposed legislation affecting the agency;

(2)

(A) except as provided under subparagraph (B) or section 3507(j), provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected agencies concerning each proposed collection of information, to solicit comment to--

(i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;

(ii) evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information;

(iii) enhance the quality, utility, and clarity of the information to be collected; and

(iv) minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology; and

(B) for any proposed collection of information contained in a proposed rule (to be reviewed by the Director under section 3507(d)), provide notice and comment through the notice of proposed rulemaking for the proposed rule and such notice shall have the same purposes specified under subparagraph (A)(i) through (iv);

(3) certify (and provide a record supporting such certification, including public comments received by the agency) that each collection of information submitted to the Director for review under section 3507--

(A) is necessary for the proper performance of the functions of the agency, including that the information has practical utility;

(B) is not unnecessarily duplicative of information otherwise reasonably accessible to the agency;

(C) reduces to the extent practicable and appropriate the burden on persons who shall provide information to or for the agency, including with respect to small entities, as defined under section 601(6) of title 5, the use of such techniques as--

(i) establishing differing compliance or reporting requirements or timetables that take into account the resources available to those who are to respond;

(ii) the clarification, consolidation, or simplification of compliance and reporting requirements; or

(iii) an exemption from coverage of the collection of information, or any part thereof;

(D) is written using plain, coherent, and unambiguous terminology and is understandable to those who are to respond;

(E) is to be implemented in ways consistent and compatible, to the maximum extent practicable, with the existing reporting and recordkeeping practices of those who are to respond;

(F) indicates for each recordkeeping requirement the length of time persons are required to maintain the records specified;

(G) contains the statement required under paragraph (1)(B)(iii);

(H) has been developed by an office that has planned and allocated resources for the efficient and effective management and use of the information to be collected, including the processing of the information in a manner which shall enhance, where appropriate, the utility of the information to agencies and the public;

(I) uses effective and efficient statistical survey methodology appropriate to the purpose for which the information is to be collected; and

(J) to the maximum extent practicable, uses information technology to reduce burden and improve data quality, agency efficiency and responsiveness to the public; and

(4) in addition to the requirements of this chapter regarding the reduction of information collection burdens for small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)), make efforts to further

reduce the information collection burden for small business concerns with fewer than 25 employees.

44 U.S.C. § 3507

(a) An agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information--

(1) the agency has--

(A) conducted the review established under section 3506(c)(1);

(B) evaluated the public comments received under section 3506(c)(2);

(C) submitted to the Director the certification required under section 3506(c)(3), the proposed collection of information, copies of pertinent statutory authority, regulations, and other related materials as the Director may specify; and

(D) published a notice in the Federal Register--

(i) stating that the agency has made such submission; and

(ii) setting forth--

(I) a title for the collection of information;

(II) a summary of the collection of information;

(III) a brief description of the need for the information and the proposed use of the information;

(IV) a description of the likely respondents and proposed frequency of response to the collection of information;

(V) an estimate of the burden that shall result from the collection of information; and

(VI) notice that comments may be submitted to the agency and Director;

(2) the Director has approved the proposed collection of information or approval has been inferred, under the provisions of this section; and

(3) the agency has obtained from the Director a control number to be displayed upon the collection of information.

(b) The Director shall provide at least 30 days for public comment prior to making a decision under subsection (c), (d), or (h), except as provided under subsection (j).

(c)

(1) For any proposed collection of information not contained in a proposed rule, the Director shall notify the agency involved of the decision to approve or disapprove the proposed collection of information.

(2) The Director shall provide the notification under paragraph (1), within 60 days after receipt or publication of the notice under subsection (a)(1)(D), whichever is later.

(3) If the Director does not notify the agency of a denial or approval within the 60-day period described under paragraph (2)--

(A) the approval may be inferred;

(B) a control number shall be assigned without further delay; and

(C) the agency may collect the information for not more than 1 year.

(d)

(1) For any proposed collection of information contained in a proposed rule–

(A) as soon as practicable, but no later than the date of publication of a notice of proposed rulemaking in the Federal Register, each agency shall forward to the Director a copy of any proposed rule which contains a collection of information and any information requested by the Director necessary to make the determination required under this subsection; and

(B) within 60 days after the notice of proposed rulemaking is published in the Federal Register, the Director may file public comments pursuant to the standards set forth in section 3508 on the collection of information contained in the proposed rule;

(2) When a final rule is published in the Federal Register, the agency shall explain--

(A) how any collection of information contained in the final rule responds to the comments, if any, filed by the Director or the public; or

(B) the reasons such comments were rejected.

(3) If the Director has received notice and failed to comment on an agency rule within 60 days after the notice of proposed rulemaking, the Director may not disapprove any collection of information specifically contained in an agency rule.

(4) No provision in this section shall be construed to prevent the Director, in the Director's discretion--

(A) from disapproving any collection of information which was not specifically required by an agency rule;

(B) from disapproving any collection of information contained in an agency rule, if the agency failed to comply with the requirements of paragraph (1) of this subsection;

(C) from disapproving any collection of information contained in a final agency rule, if the Director finds within 60 days after the publication of the final rule that the agency's response to the Director's comments filed under paragraph (2) of this subsection was unreasonable; or

(D) from disapproving any collection of information contained in a final rule, if--

(i) the Director determines that the agency has substantially modified in the final rule the collection of information contained in the proposed rule; and

(ii) the agency has not given the Director the information required under paragraph (1) with respect to the modified collection of information, at least 60 days before the issuance of the final rule.

(5) This subsection shall apply only when an agency publishes a notice of proposed rulemaking and requests public comments.

(6) The decision by the Director to approve or not act upon a collection of information contained in an agency rule shall not be subject to judicial review.

(e)

(1) Any decision by the Director under subsection (c), (d), (h), or (j) to disapprove a collection of information, or to instruct the agency to make substantive or material change to a collection of information, shall be publicly available and include an explanation of the reasons for such decision.

(2) Any written communication between the Administrator of the Office of Information and Regulatory Affairs, or any employee of the Office of Information and Regulatory Affairs, and an agency or person not employed by the Federal Government concerning a proposed collection of information shall be made available to the public.

(3) This subsection shall not require the disclosure of--

(A) any information which is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; or

(B) any communication relating to a collection of information which is not approved under this subchapter, the disclosure of which could lead to retaliation or discrimination against the communicator.

(f)

(1) An independent regulatory agency which is administered by 2 or more members of a commission, board, or similar body, may by majority vote void--

(A) any disapproval by the Director, in whole or in part, of a proposed collection of information of that agency; or

(B) an exercise of authority under subsection (d) of section 3507 concerning that agency.

(2) The agency shall certify each vote to void such disapproval or exercise to the Director, and explain the reasons for such vote. The Director shall without further delay assign a control number to such collection of information, and such vote to void the disapproval or exercise shall be valid for a period of 3 years.

(g) The Director may not approve a collection of information for a period in excess of 3 years.

(h)

(1) If an agency decides to seek extension of the Director's approval granted for a currently approved collection of information, the agency shall--

(A) conduct the review established under section 3506(c), including the seeking of comment from the public on the continued need for, and burden imposed by the collection of information; and

(B) after having made a reasonable effort to seek public comment, but no later than 60 days before the expiration date of the control number assigned by the Director for the currently approved collection of information, submit the collection of information for review and approval under this section, which shall include an explanation of how the agency has used the information that it has collected.

(2) If under the provisions of this section, the Director disapproves a collection of information contained in an existing rule, or recommends or instructs the agency to make a substantive or material change to a collection of information contained in an existing rule, the Director shall--

(A) publish an explanation thereof in the Federal Register; and

(B) instruct the agency to undertake a rulemaking within a reasonable time limited to consideration of changes to the collection of information contained in the rule and thereafter to submit the collection of information for approval or disapproval under this subchapter.

(3) An agency may not make a substantive or material modification to a collection of information after such collection has been approved by the Director, unless the modification has been submitted to the Director for review and approval under this subchapter.

(i)

(1) If the Director finds that a senior official of an agency designated under section 3506(a) is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be

approved and has sufficient resources to carry out this responsibility effectively, the Director may, by rule in accordance with the notice and comment provisions of chapter 5 of title 5, United States Code, delegate to such official the authority to approve proposed collections of information in specific program areas, for specific purposes, or for all agency purposes.

(2) A delegation by the Director under this section shall not preclude the Director from reviewing individual collections of information if the Director determines that circumstances warrant such a review. The Director shall retain authority to revoke such delegations, both in general and with regard to any specific matter. In acting for the Director, any official to whom approval authority has been delegated under this section shall comply fully with the rules and regulations promulgated by the Director.

(j)

(1) The agency head may request the Director to authorize a collection of information, if an agency head determines that--

(A) a collection of information--

(i) is needed prior to the expiration of time periods established under this subchapter; and

(ii) is essential to the mission of the agency; and

(B) the agency cannot reasonably comply with the provisions of this subchapter because--

(i) public harm is reasonably likely to result if normal clearance procedures are followed;

(ii) an unanticipated event has occurred; or

(iii) the use of normal clearance procedures is reasonably likely to prevent or disrupt the collection of information or is

reasonably likely to cause a statutory or court ordered deadline to be missed.

(2) The Director shall approve or disapprove any such authorization request within the time requested by the agency head and, if approved, shall assign the collection of information a control number. Any collection of information conducted under this subsection may be conducted without compliance with the provisions of this subchapter for a maximum of 180 days after the date on which the Director received the request to authorize such collection.

44 U.S.C. § 3510

(a) The Director may direct an agency to make available to another agency, or an agency may make available to another agency, information obtained by a collection of information if the disclosure is not inconsistent with applicable law.

(b)

(1) If information obtained by an agency is released by that agency to another agency, all the provisions of law (including penalties) that relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information.

(2) The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

44 U.S.C. § 3517

(a) In developing information resources management policies, plans, rules, regulations, procedures, and guidelines and in reviewing collections of information, the Director shall provide interested agencies and persons early and meaningful opportunity to comment.

(b) Any person may request the Director to review any collection of information conducted by or for an agency to determine, if, under this subchapter, a person shall maintain, provide, or disclose the information to or for the agency. Unless the request is frivolous, the Director shall, in coordination with the agency responsible for the collection of information--

(1) respond to the request within 60 days after receiving the request, unless such period is extended by the Director to a specified date and the person making the request is given notice of such extension; and

(2) take appropriate remedial action, if necessary.

44 U.S.C. § 3902

(a) There shall be at the head of the Office of Inspector General, an Inspector General who shall be appointed by the Director of the Government Publishing Office without regard to political affiliation and solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations. The Inspector General shall report to, and be under the general supervision of, the Director of the Government Publishing Office. The Director of the Government Publishing Office shall have no authority to prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation, or from issuing any subpena during the course of any audit or investigation.

(b) The Inspector General may be removed from office by the Director of the Government Publishing Office. The Director of the Government Publishing Office shall, promptly upon such removal, communicate in writing the reasons for any such removal to each House of the Congress.

E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002)

E-Government Act § 2(b)

(b) PURPOSES.—The purposes of this Act are the following:

(1) To provide effective leadership of Federal Government efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget.

(2) To promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government.

(3) To promote interagency collaboration in providing electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal electronic Government processes, where this collaboration would improve the efficiency and effectiveness of the processes.

(4) To improve the ability of the Government to achieve agency missions and program performance goals.

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

(6) To reduce costs and burdens for businesses and other Government entities.

(7) To promote better informed decisionmaking by policy makers.

(8) To promote access to high quality Government information and services across multiple channels.

(9) To make the Federal Government more transparent and accountable.

(10) To transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations.

(11) To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.

E-Government Act § 201

Except as otherwise provided, in this title the definitions under sections 3502 and 3601 of title 44, United States Code, shall apply.

E-Government Act § 208

(a) PURPOSE.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) PRIVACY IMPACT ASSESSMENTS.—

(1) RESPONSIBILITIES OF AGENCIES.—

(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—

(I) will be collected, maintained, or disseminated using information technology; and

(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) SENSITIVE INFORMATION.—Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) COPY TO DIRECTOR.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT.—

(A) IN GENERAL.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) GUIDANCE.—The guidance shall—

(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

(ii) require that a privacy impact assessment address—

(I) what information is to be collected;

(II) why the information is being collected;

(III) the intended use of the agency of the information;

(IV) with whom the information will be shared;

(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(VI) how the information will be secured; and

(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the "Privacy Act").

(3) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;

(B) oversee the implementation of the privacy impact assessment process throughout the Government; and

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) PRIVACY PROTECTIONS ON AGENCY WEBSITES.—

(1) PRIVACY POLICIES ON WEBSITES.—

(A) GUIDELINES FOR NOTICES.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) CONTENTS.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

(i) what information is to be collected;

(ii) why the information is being collected;

(iii) the intended use of the agency of the information;

(iv) with whom the information will be shared;

(v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(vi) how the information will be secured; and

(vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the "Privacy Act"), and other laws relevant to the protection of the privacy of an individual.

(2) PRIVACY POLICIES IN MACHINE–READABLE FORMATS.—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) DEFINITION.—In this section, the term "identifiable form" means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

CONSTITUTIONAL PROVISIONS

U.S. Const. art. 1, § 2, cl. 3

Representatives and direct Taxes shall be apportioned among the several States which may be included within this Union, according to their respective Numbers, which shall be determined by adding to the whole Number of free Persons, including those bound to Service for a Term of Years, and excluding Indians not taxed, three fifths of all other Persons. The actual Enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct. The Number of Representatives shall not exceed one for every thirty Thousand, but each State shall have at Least one Representative; and until such enumeration shall be made, the State of New Hampshire shall be entitled to chuse three, Massachusetts eight, Rhode-Island and Providence Plantations one, Connecticut five, New-York six, New Jersey four, Pennsylvania eight, Delaware one, Maryland six, Virginia ten, North Carolina five, South Carolina five, and Georgia three.

U.S. Const. amend. XIV, § 2

Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed. But when the right to vote at any election for the choice of electors for President and Vice President of the United States, Representatives in Congress, the Executive and Judicial officers of a State, or the members of the Legislature thereof, is denied to any of the male inhabitants of such State, being twenty-one years of age,15 and citizens of the United States, or in any way abridged, except for participation in rebellion, or other crime, the basis of

representation therein shall be reduced in the proportion which the number of such male citizens shall bear to the whole number of male citizens twenty-one years of age in such State.

REGULATIONS

5 C.F.R. § 1320.3(c)

(c) Collection of information means, except as provided in § 1320.4, the obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency by means of identical questions posed to, or identical reporting, recordkeeping, or disclosure requirements imposed on, ten or more persons, whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit. "Collection of information" includes any requirement or request for persons to obtain, maintain, retain, report, or publicly disclose information. As used in this Part, "collection of information" refers to the act of collecting or disclosing information, to the information to be collected or disclosed, to a plan and/or an instrument calling for the collection or disclosure of information, or any of these, as appropriate.

(1) A "collection of information" may be in any form or format, including the use of report forms; application forms; schedules; questionnaires; surveys; reporting or recordkeeping requirements; contracts; agreements; policy statements; plans; rules or regulations; planning requirements; circulars; directives; instructions; bulletins; requests for proposal or other procurement requirements; interview guides; oral communications; posting, notification, labeling, or similar disclosure requirements; telegraphic or telephonic requests; automated, electronic, mechanical, or other

technological collection techniques; standard questionnaires used to monitor compliance with agency requirements; or any other techniques or technological methods used to monitor compliance with agency requirements. A "collection of information" may implicitly or explicitly include related collection of information requirements.

(2) Requirements by an agency for a person to obtain or compile information for the purpose of disclosure to members of the public or the public at large, through posting, notification, labeling or similar disclosure requirements constitute the "collection of information" whenever the same requirement to obtain or compile information would be a "collection of information" if the information were directly provided to the agency. The public disclosure of information originally supplied by the Federal government to the recipient for the purpose of disclosure to the public is not included within this definition.

(3) "Collection of information" includes questions posed to agencies, instrumentalities, or employees of the United States, if the results are to be used for general statistical purposes, that is, if the results are to be used for statistical compilations of general public interest, including compilations showing the status or implementation of Federal activities and programs.

(4) As used in paragraph (c) of this section, "ten or more persons" refers to the persons to whom a collection of information is addressed by the agency within any 12–month period, and to any independent entities to which the initial addressee may reasonably be expected to transmit the collection of information during that period, including independent State, territorial, tribal or local entities and separately incorporated subsidiaries or affiliates. For the purposes of this definition of "ten or more persons," "persons" does not include employees of the respondent acting within the scope of their

employment, contractors engaged by a respondent for the purpose of complying with the collection of information, or current employees of the Federal government (including military reservists and members of the National Guard while on active duty) when acting within the scope of their employment, but it does include retired and other former Federal employees.

(i) Any recordkeeping, reporting, or disclosure requirement contained in a rule of general applicability is deemed to involve ten or more persons.

(ii) Any collection of information addressed to all or a substantial majority of an industry is presumed to involve ten or more persons.

OMB, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016)

***

[Page 34]

63) 'Privacy impact assessment' means an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

***

[Appendix II at 10]

A PIA is one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks. Agencies shall conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle. In order to conduct a meaningful PIA, the agency's SAOP shall work closely with the program managers, information system owners, information technology experts, security officials, counsel, and other relevant agency officials.

Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles. Accordingly, a PIA shall be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.

***

OFFICE OF MANAGEMENT AND BUDGET

September 26, 2003

M-03-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
DirectoR

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

Background

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail Eva_Kleederman@omb.eop.gov.

Attachments

Attachment A

E-Government Act Section 208 Implementation Guidance

I. General

A. Requirements. Agencies are required to:
1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),

3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. Application. This guidance applies to:

1. all executive branch departments and agencies ("agencies") and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C. Modifications to Current Guidance. Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. Memorandum 99-05 (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. Memorandum 99-18 (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any web page collecting substantial personal information from the public; and
3. Memorandum 00-13 (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children's Online Privacy Protection Act ("COPPA").

II. Privacy Impact Assessment

A. Definitions.

1. Individual - means a citizen of the United States or an alien lawfully admitted for permanent residence.[1]
2. Information in identifiable form- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).[2]
3. Information technology (IT) - means, as defined in the Clinger-Cohen Act[3], any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. Major information system - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.
5. National Security Systems - means, as defined in the Clinger-Cohen Act[4], an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.
6. Privacy Impact Assessment (PIA)- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
7. Privacy policy in standardized machine-readable format- means a statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. When to conduct a PIA:[5]

1. The E-Government Act requires agencies to conduct a PIA before:
    a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
    b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
2. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

a. Conversions - when converting paper-based records to electronic systems;
b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
    - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
    - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
    - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
    - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

3. No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:
    a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants);[6]
    b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information;
    c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
    d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
    e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
    f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
    g. for minor changes to a system or collection that do not create new privacy risks.
4. Update of PIAs: Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. Conducting a PIA.

1. Content.
    a. PIAs must analyze and describe:
        i. what information is to be collected (e.g., nature and source);
        ii. why the information is being collected (e.g., to determine eligibility);
        iii. intended use of the information (e.g., to verify existing data);
        iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
        v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
        vi. how the information will be secured (e.g., administrative and technological controls[7]); and
        vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.
    b. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:
    a. Specificity. The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
        i. IT development stage. PIAs conducted at this stage:
            1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
            2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
            3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.
        ii. Major information systems. PIAs conducted for these systems should reflect more extensive analyses of:
            1. the consequences of collection and flow of information,
            2. the alternatives to collection and handling as designed,
            3. the appropriate measures to mitigate risks identified for each alternative and,
            4. the rationale for the final design choice or business process.
        iii. Routine database systems. Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.
    b. Information life cycle analysis/collaboration. Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.
3. Review and publication.
    a. a. Agencies must ensure that:
        i. the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);
        ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300[8]); and
        iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
            1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment[9]. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
            2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such

information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. Relationship to requirements under the Paperwork Reduction Act (PRA)[10].
   1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).
   2. If Agencies submit a Joint ICR and PIA:
      a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
         i. a description of the information to be collected in the response to Item 1 of the Supporting Statement[11];
         ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement[12];
         iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement[13];
         iv. a discussion in item 10 of the Supporting Statement of:
            1. whether individuals are informed that providing the information is mandatory or voluntary
            2. opportunities to consent, if any, to sharing and submission of information;
            3. how the information will be secured; and
            4. whether a system of records is being created under the Privacy Act)[14].
      b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
   3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.

   1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
   2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.
   3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

A. Privacy Policy Clarification. To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."

B. Effective Date. Agencies are expected to implement the following changes to their websites by December 15, 2003.

C. Exclusions: For purposes of web privacy policies, this guidance does not apply to:
   1. information other than "government information" as defined in OMB Circular A-130;
   2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
   3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).

D. Content of Privacy Policies.
   1. Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:
      a. Consent to collection and sharing[15]. Agencies must now ensure that privacy policies:
         i. inform visitors whenever providing requested information is voluntary;
         ii. inform visitors how to grant consent for use of voluntarily-provided information; and
         iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
      b. Rights under the Privacy Act or other privacy laws[16]. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
         i. in the body of the web privacy policy;

ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).

2. Agency Privacy Policies must continue to address the following, modified, requirements:
   a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in OMB Memorandum 99-18) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
      i. Privacy Act information. When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
         1. at the point of collection, or
         2. via link to the agency's general Privacy Policy[18].
      ii. "Privacy Act Statements." Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
      iii. Automatically Collected Information (site management data). Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
      iv. Interaction with children: Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C)[19].
      v. Tracking and customization activities.Agencies are directed to adhere to the following modifications to OMB Memorandum 00-13 and the OMB follow-up guidance letter dated September 5, 2000:
         1. Tracking technology prohibitions:
            a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
            b. agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:
               - the nature of the information collected;
               - the purpose and use for the information;
               - whether and to whom the information will be disclosed; and
               - the privacy safeguards applied to the information collected.
            c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII)[20].
         2. The following technologies are not prohibited:
            a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
            b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
               - the purpose of the tracking (i.e., customization of the site);
               - that accepting the customizing feature is voluntary;
               - that declining the feature still permits the individual to use the site; and
               - the privacy safeguards in place for handling the information collected.
            c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.
      vi. Law enforcement and homeland security sharing: Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.
   b. Security of the information[21]. Agencies should continue to comply with existing requirements for computer security in administering their websites[22] and post the following information in their Privacy Policy:

i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)

E. Placement of notices. Agencies should continue to follow the policy identified in OMB Memorandum 99-18 regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:
1. their principal web site;
2. any known, major entry points to their sites;
3. any web page that collects substantial information in identifiable form.

F. Clarity of notices. Consistent with OMB Memorandum 99-18, privacy policies must be:
1. clearly labeled and easily accessed;
2. written in plain language; and
3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short "highlights" notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. Actions.
1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site.
2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

B. Reporting Requirement. Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency's progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official
Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

A. Agencies must:
1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.
3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
4. designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.

B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

A. Information technology systems or information collections for which PIAs were conducted. Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
B. Persistent tracking technology uses. If persistent tracking technology is authorized, include the need that compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.
C. Agency achievement of goals for machine readability: Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.
D. Contact information. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

Attachment B
E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. PURPOSE. — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. PRIVACY IMPACT ASSESSMENTS.—

1. RESPONSIBILITIES OF AGENCIES.—
    a. IN GENERAL.—An agency shall take actions described under subparagraph (b) before—
        i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
        ii. initiating a new collection of information that—
            1. will be collected, maintained, or disseminated using information technology; and
            2. includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.
    b. AGENCY ACTIVITIES. —To the extent required under subparagraph (a), each agency shall—
        i. conduct a privacy impact assessment;
        ii. ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
        iii. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
    c. SENSITIVE INFORMATION. —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
    d. COPY TO DIRECTOR. —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.
2. CONTENTS OF A PRIVACY IMPACT ASSESSMENT. —
    a. IN GENERAL. —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
    b. GUIDANCE. — The guidance shall—
        i. ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
        ii. require that a privacy impact assessment address—
            1. what information is to be collected;
            2. why the information is being collected;
            3. the intended use of the agency of the information;
            4. with whom the information will be shared;

5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
6. how the information will be secured; and
7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the `Privacy Act').

3. RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—
   a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
   b. oversee the implementation of the privacy impact assessment process throughout the Government; and
   c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —
   a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
   b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
      i. what information is to be collected;
      ii. why the information is being collected;
      iii. the intended use of the agency of the information;
      iv. with whom the information will be shared;
      v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
      vi. how the information will be secured; and
      vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the `Privacy Act'), and other laws relevant to the protection of the privacy of an individual.
2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, the term `identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Attachment C

This attachment is a summary by the Federal Trade Commission of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA).

The hallmarks of COPPA for purposes of federal online activity are (i) notice of information collection practices (ii) verifiable parental consent and (iii) access, as generally outlined below:

- Notice of Information Collection Practices

  Agencies whose Internet sites offer a separate children's area and collect personal information from them must post a clear and prominent link to its Internet privacy policy on the home page of the children's area and at each area where it collects personal information from children. The privacy policy should provide the name and contact information of the agency representative required to respond to parental inquiries about the site. Importantly, the privacy policy should inform parents about the kinds of information collected from children, how the information is collected (directly, or through cookies), how the information is used, and procedures for reviewing/deleting the information obtained from children.

  In addition, the privacy policy should inform parents that only the minimum information necessary for participation in the activity is collected from the child.In addition to providing notice by posting a privacy policy, notice of an Internet site's information collection practices must be sent directly to a parent when a site is requesting parental consent to collection personal information from a child. This direct notice should tell parents that the site would like to collect personal information from their child, that their consent is required for this collection, and how consent can be provided. The notice should also contain the information set forth in the site's privacy policy, or provide an explanatory link to the privacy policy.

- Verifiable Parental Consent

  With limited exceptions, agencies must obtain parental consent before collecting any personal information from children under the age of 13. If agencies are using the personal information for their internal use only, they may obtain parental consent through an e-mail message from the parent, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, agencies might seek confirmation from a parent in a delayed confirmatory e-mail, or confirm the parent's consent by letter or phone call[23].

***