FGDC Policy on Access to Public Information and the Protection of Personal Information Privacy in Federal Geospatial Databases

Adopted by the Federal Geographic Data Committee in April 1998

This policy articulates the Federal Geographic Data Committee's (FGDC) endorsement of public access to information and appropriate protections for the privacy and confidentiality of personal information in federal geospatial databases. The policy supports the goals of the FGDC, and is in conformance with law, related federal policies, and well-regarded fair information and privacy practices and principles.

This policy is needed because federal geospatial databases are being built with increasing levels of geographic specificity and often include personal information. For example, individual's names are often linked to property addresses and street maps; cadastral records that identify land parcels and land owner names may be linked to high resolution imagery. Privacy concerns are raised because databases may contain personal information prohibited from disclosure by law. Privacy in this context means "information privacy," an individual's claim to control the terms under which personal information—information identifiable to an individual—is acquired, disclosed, and used.[1]

This policy applies to all federal[2] geospatial databases from which personal information is retrieved. A federal geospatial database may be considered a system of records subject to the Privacy Act of 1974. A systems of records is defined as: "A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." Systems of records that meet this definition, but have not been *officially* identified as Privacy Act systems of records, are also under the purview of the Privacy Act.

Information Access

- **Agencies should disclose geospatial data and information on request unless exempted under the Freedom of Information Act. Agencies should work to improve access to geospatial databases.**[3]

- **Agencies should continue to ensure public access to agency records and information.**[4]

- **Agencies should work to achieve a balance between maximizing the usefulness of geospatial data and information and minimizing the cost to the government and the public.**[5]

---

[1]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995.

[2]Federal geospatial databases in this context means all geospatial databases collected or produced, either directly or indirectly, (e.g. through grants, partnerships, or contracts with other entities) by Federal agencies. Executive Order 12906, Sec. 4(d); Office of Management and Budget, Circular A-16 Revised, "Coordination of Surveying, Mapping, and Related Spatial Data Activities," Sec. 3(a).

[3]Electronic Freedom of Information Act, Public Law 104-231, 110 Statute 2422, and Office of Management and Budget, Circular A-130, "Management of Federal Information Resources," 61 Federal Register 6428, February 20, 1996, Section 7(l).

[4]Freedom of Information Act, 5 U.S.C. § 552.

[5]Electronic Freedom of Information Act, Public Law 104-231, 110 Statute 2422, and Office of Management and Budget, Circular A-130, "Management of Federal Information Resources," 61 Federal Register 6428, February 20, 1996. Section 8a(5i).

Information Privacy

- **Agencies should, at the time of collection, inform individuals from whom personal information is collected directly:**[6]
  Why they are collecting the information;
  The legal authority to collect the information;
  What the information is expected to be used for;
  What steps will be taken to protect its confidentiality, integrity, and quality;
  The consequences of providing or withholding information;
  The means to correct their personal information that lacks sufficient quality to ensure fairness in its use;
  Of opportunities to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions;
  Of the opportunity to remain anonymous when appropriate;
  Any rights of redress; and
  Of the agency records retention schedule.

- **Agencies should acquire, disclose, and use personal information only in ways that respect an individual's privacy.** [7]

- **Agencies should ensure relevant agency staff, including Freedom of Information Act officers and Privacy Act officers, are aware of the privacy implications of geographic information system technology.** [8]

- **Agencies should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.** [9]

- **Agencies should limit the type and extent of personal information acquired, disclosed, and used in geographic information systems to the information reasonably expected to support current or planned activities.** [10]

- **Agencies should ensure the integrity of personal information. Personal information held in, or linked to, geospatial databases should not be improperly altered or destroyed.** [11]

- **Agencies should ensure that personal information held in geospatial databases is accurate, timely, complete and relevant for the purposes for which it is acquired and used.**[12]

---

[6]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Notice Principle (II.B.); Awareness Principle (III.A.); and Redress Principle (III.C.).

[7]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Information Privacy Principle (I.A.).

[8]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Education Principle (II.E.); Information and Privacy Commissioner/Ontario, *Geographic Information Systems and Privacy: Fundamental Principles*, April 1997, ; *Data Sensitivity Issues Regarding Public Access to U.S. Army Corps of Engineers Geospatial Data via the Internet* ,1 Mar 1996 Draft Information Paper, 5.a; Department of Defense Program Regulations 32 CFR Part 286.37, Education and Training, Federal Register Vol. 62, No. 33, February 19, 1997 (guidelines for Department-wide implementation of E-FOIA) is an example of how to incorporate the U.S. Information Infrastructure Task Force Education Principle (II.E.) into agency regulations.

[9]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Protection Principle (II.C.).

[10]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Acquisition Principle (II.A.). For an example of this principle as written in a Federal agency guideline see Natural Resource Conservation Service Online Directives Management System, General Manual, Title 120, Administrative Services, Part 408, Records, Subpart C, Freedom of Information and Privacy Act. <http://policy.nrcs.usda.gov/national/gm/title120/part408/Subpartc/index.htm>.

[11]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Information Integrity Principle (I.B.).

[12]Privacy Working Group, U.S. Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, October 1995, Information Quality Principle (I.C.), and Fairness Principle (II.D.).