Department of the Interior
Privacy Impact Assessment Template

Name of Project: ISO Geospatial Metadata Editors Registry
Bureau: U.S. Geological Survey
Project's Unique ID: GX14EE000101000

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

1) **Who is the person completing this document?** (Name, title, organization and contact information).

Vaishal P. Sheth
Web Administrator
22nd Century Technologies Inc. (Contractor)
Federal Geographic Data Committee Office of the Secretariat, USGS
12201 Sunrise Valley Drive, MS 590
Reston, VA 20192
703-648-5930
vsheth@usgs.gov

2) **Who is the system owner?** (Name, organization and contact information).

Ken Shaffer
Deputy Executive Director
Federal Geographic Data Committee Office of the Secretariat, USGS
12201 Sunrise Valley Drive, MS 590
Reston, VA 20192
703-648-5740
kmshaffer@usgs.gov

3) **Who is the system manager for this system or application?** (Name, organization, and contact information).

Jennifer Carlino
FGDC Metadata Coordinator
Federal Geographic Data Committee Office of the Secretariat, USGS
Denver Federal Center, PO Box 25046, Bldg. 810
Room 8000, MS 302
Denver, CO 80225
303-202-4260
jcarlino@usgs.gov

4) **Who is the IT Security Manager who reviewed this document?** (Name, organization, and contact information).

Vaishal P. Sheth
Web Administrator
22nd Century Technologies Inc. (Contractor)
Federal Geographic Data Committee Office of the Secretariat, USGS
12201 Sunrise Valley Drive, MS 590
Reston, VA 20192
703-648-5930
vsheth@usgs.gov

5) **Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).

William Reilly
IT Specialist (Infosec)
USGS Administration and Enterprise Information
12201 Sunrise Valley Drive
Reston, VA 20192
703-648-7239
wreilly@usgs.gov

6) **Who is the Reviewing Official?** (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

Rich L. Frazier
Associate Director for Information Resources
USGS

MS 159
12201 Sunrise Valley Drive
Reston, VA 20192
703-648-6828
efrazier@usgs.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual[1]?
(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes

b. Is the information about individual members of the public?
(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Employees of the federal government agencies that have developed an ISO Geospatial Metadata Editor may elect to register the editor in the registry, in which case the system would contain their business email address.

2) What is the purpose of the system/application?

As National Spatial Data Infrastructure (NSDI) stakeholders move forward with the implementation of the International Organization for

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means 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).

Standardization's (ISO) 191** series of geospatial metadata standards, endorsed by the Federal Geographic Data Committee (FGDC), there is increasing demand for information about applications/editors that can be used to create ISO compliant metadata records.

As per Office of Management and Budget Circular A-16: "Metadata are information about data and/or geospatial services, such as content, source, vintage, spatial scale, accuracy, projection, responsible party, contact phone number, method of collection, and other descriptions. Metadata are critical to document, preserve and protect agencies' spatial data assets. Reliable metadata, structured in a standardized manner, are essential to ensuring that geospatial data are used appropriately, and that any resulting analysis is credible. Metadata also can be used to facilitate the search and access of data sets or geospatial services within a Clearinghouse or data library. All spatial data collected or derived directly or indirectly using federal funds will have FGDC metadata."

The USGS, through the FGDC Office of the Secretariat (www.fgdc.gov), proposes development of an online registration system for developers of ISO Geospatial Metadata Editors, either public or private entities, to voluntarily describe their metadata tools. Developers will be asked to include information such as features of the editor, its functionality, supported standards, and point of contact information through a login-based, online form. The FGDC Metadata Working Group (MWG) (www.fgdc.gov/participation/working-groupssubcommittees/mwg/), whose membership represents Federal, State, Local and Tribal governments and the Private Sector, has requested the development of the registry as a useful tool to learn about available ISO Geospatial Metadata Editors. Since the information about the editors may be of interest or utility to others implementing ISO geospatial metadata standards, supporting the advancement of the NSDI, the FGDC will make the information collected available on the Web in the form of a simple registry type database. FGDC MWG members as well as non FGDC MWG members including geospatial metadata implementers from private sector, academia, all forms of government, and the general public, will have read-only access to the editor information published in the registry.

3) What legal authority authorizes the purchase or development of this system/application?

OMB Circular A-16 -
http://www.whitehouse.gov/omb/circulars/a016/a016_rev.html

Executive Order 12906 -
http://govinfo.library.unt.edu/npr/library/direct/orders/20fa.html

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Federal, State, Local and Tribal governments, private sector, and others involved in the development of ISO geospatial metadata.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The information is taken directly from the developer or a company representative, of the ISO Geospatial Metadata Editor.

b. What Federal agencies are providing data for use in the system?

No particular federal agency is providing data but an employee of an agency that has developed an ISO Geospatial Metadata Editor can voluntarily register the editor in the registry at any time.

c. What Tribal, State and local agencies are providing data for use in the system?

No particular tribal, state or local agency is providing data but an employee of an agency that has developed an ISO Geospatial Metadata Editor can voluntarily register the editor in the registry at any time.

d. From what other third party sources will data be collected?

No particular third party source is providing data but representatives from the private sector, academia and others involved in the development of an ISO Geospatial Metadata Editor can voluntarily register the editor in the registry at any time.

e. What information will be collected from the employee and the public?

Business email address, First Name, Last Name and Organization for registration purposes (such information is not made public) and information about the ISO Geospatial Metadata Editor (no such information is user related or personally identifiable). This information is only used to provide user authentication. Developers of ISO Geospatial

Metadata Editors voluntarily elect to submit information describing their metadata editor and create an account profile that contains their business email address.

3) **Accuracy, Timeliness, and Reliability**

a. How will data collected from sources other than DOI records be verified for accuracy?

Users of the site will be responsible for accurately submitting their information. Email addresses will be verified for complete format only. Before access to the additional features is granted, a return email will be sent to verify that the email address is a functioning address. The submitted information will be reviewed for appropriateness prior to being published.

b. How will data be checked for completeness?

Emails addresses will be verified for complete format only. Before access to the additional features is granted, a return email will be sent to verify that the email address is a functioning email address. This is a spam reduction measure.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The features of the registry requiring a login are made available for voluntary use. Users will be responsible for accurately submitting an email address. We rely on the users to update their email address if it changes. Before access to the additional features is granted, a return email address will be sent to verify that the email address is a functioning email address. This is a spam reduction measure.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Data elements are self-explanatory.

D. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   Yes

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

   No

3) **Will the new data be placed in the individual's record?**

   No new data; not applicable

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

   No new data; not applicable

5) **How will the new data be verified for relevance and accuracy?**

   No new data; not applicable

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   No new data; not applicable

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

   No new data; not applicable

8) **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

   Email address is used for authentication purposes within the account at the time of first login. All subsequent retrieval of data internal to the system is done using a unique database id number that is sequentially assigned to users on registration which on its own is not personally identifiable.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

An email list of website users could be produced, but no process is in place to produce any such reports.

10) **What opportunities do 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.)**

All information is voluntary. Individuals have the option to not provide the information in which case the account won't be created and no information could be submitted.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The system will operate only on one site.

2) **What are the retention periods of data in this system?**

The registry will retain users' registration details permanently, unless the user deletes their account, which they may do at any time by email to a support address. This is a standard feature of websites in which the creation of a unique, persistent user account is a requirement for participation. (In this case, it is a requirement only for certain optional uses of the site.)

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The registry will retain users' registration details permanently, unless the user deletes their account, which they may do at any time by email to a support address, or the online capability is sun-setted. The continued use of the registry and the need for information retention will be evaluated annually by the FGDC OS and appropriate retention steps will be taken based on the submitted information, its source, and value.

4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

5) **How does the use of this technology affect public/employee privacy?**

No new technology; not applicable

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No

7) **What kinds of information are collected as a function of the monitoring of individuals?**

Not applicable

8) **What controls will be used to prevent unauthorized monitoring?**

Not applicable

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Not applicable. Business Email address is used for authentication purposes within the account at the time of first login.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Not applicable

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Access to the database is limited to Web administrators which may include contractors. Public will have access to the editor data submitted by the users, but not to their email address or profile information. Reviewers will have access to the data submitted by the users for approval purposes, but not to their email address or profile information.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the data for system administrators is determined by a series of controls. A userid is established which governs the rights to use the system.

This userid must then be included in an Administrator group for access to user-supplied data within the application. Direct access to the database is governed by a separate database user id and required permissions. Controls on userid and password security are documented in the USGS Computer and Network Security Handbook.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   A user has access to their data only; administrator or elevated access privileges to the database is limited by the controls specified above.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

   Security measures and controls consist of: passwords, application permissions, user identification, IP addresses, database permission, and software controls. All employees including contractors must meet the requirements for protecting Privacy Act protected information.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

   Contractors are involved in the development and maintenance of the system. There is a Privacy Act clause included in their contracts.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   No

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   Not applicable, no interface with other systems.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

   No

9) **How will the data be used by the other agency?**

Not applicable

10) **Who is responsible for assuring proper use of the data?**

Not applicable

See Attached Approval Page

The Following Officials Have Approved this Document

1) System Manager

JENNIFER CARLINO Digitally signed by JENNIFER CARLINO DN: c=US, o=U.S. Government, ou=Department of the Interior, ou=Geological Survey, cn=JENNIFER CARLINO, 0.9.2342.19200300.100.1.1=14001000300426 Date: 2014.09.29 18:26:28 -06'00'

_____ **(Signature)** _____**(Date)**

Name: Jennifer Carlino

Title: FGDC Metadata Coordinator

2) IT Security Manager

VAISHAL SHETH (Affiliate) Digitally signed by VAISHAL SHETH (Affiliate) DN: c=US, o=U.S. Government, ou=Department of the Interior, ou=Geological Survey, 0.9.2342.19200300.100.1.1=14001000855067, cn=VAISHAL SHETH (Affiliate) Date: 2014.09.29 12:44:11 -04'00'

_____ **(Signature)** _____**(Date)**

Name: Vaishal Sheth

Title: Web Administrator
22nd Century Technologies Inc. (Contractor)

3) Privacy Act Officer

_____ **(Signature)** _____**(Date)**

Name: William Reilly

Title: Privacy Act Officer

4) Reviewing Official

_____ **(Signature)** _____**(Date)**

Name: Eldrich Frazier

Title: Associate Director for Information Resources