

Department of the Interior
U.S. Geological Survey

LAND SATELLITES DATA SYSTEM (LSDS) PRIVACY IMPACT ASSESSMENT (PIA)

Version 4.0

February 18, 2014



Land Satellites Data System (LSDS)
Privacy Impact Assessment (PIA)

Name of Project: Landsat
Bureau: USGS/EROS Center

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:

William P. Reilly, USGS Acting Privacy Act Officer
12201 Sunrise Valley Drive
Reston, VA 20192
703-648-7239

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

No

a. Is this information identifiable to the individual¹?

(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).

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).

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).

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).

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

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

C. DATA in the SYSTEM:

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

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?

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

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

- d. From what other third party sources will data be collected?
- e. What information will be collected from the employee and the public?

3) Accuracy, Timeliness, and Reliability

- a. How will data collected from sources other than DOI records be verified for accuracy?
- b. How will data be checked for completeness?
- 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).
- d. Are the data elements described in detail and documented? If yes, what is the name of the document?

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?
- 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?
- 3) Will the new data be placed in the individual's record?
- 4) Can the system make determinations about employees/public that would not be possible without the new data?

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

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

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

- 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.

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

- 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.**

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?

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

- 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?

- 4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?
- 5) How does the use of this technology affect public/employee privacy?
- 6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
- 7) What kinds of information are collected as a function of the monitoring of individuals?
- 8) What controls will be used to prevent unauthorized monitoring?
- 9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.
- 10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

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

- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.
- 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)
- 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?
- 6) Do other systems share data or have access to the data in the system? If yes, explain.
- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?
- 9) How will the data be used by the other agency?
- 10) Who is responsible for assuring proper use of the data?

References

Please see http://landsat.usgs.gov/tools_acronyms_ALL.php for a list of acronyms.