



*National Map Reengineering Project
(NMRP)*

**Major Application
Privacy Impact Assessment, Version 3**

June 5, 2012

Department of the Interior
Privacy Impact Assessment Template

Name of Project: *The National Map Re-Engineering Project (NMRP)*

Bureau: USGS

Project's Unique ID: 010-12-01-27-01-1080-00-109-026

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:

David J. Newman
Privacy Act Officer
U.S. Geological Survey
Enterprise Information Office
National Center, M.S. 807
12201 Sunrise Valley Drive
Reston, VA 20192-0002
Phone: (703) 648-7196
E-Mail: djnewman@usgs.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

TNM_SDW – No. The Spatial Data Warehouse (SDW) does not collect, maintain, or use private, personal user or employee information

TNM_NGTOC – Yes. **Note that the information contained in TNM_NGTOC is limited to that data that is stored on servers for data protection/backup purposes.** In that context, the TNM_NGTOC contains names, addresses, date of birth, and phone numbers of individuals (employees and volunteer employees). The system also contains personnel information such as work plans, awards justifications, personnel actions, performance write-ups, etc. Information

pertaining to ATA contractors resides on this system as well as financial information involving payroll data, travel, training, and the budget.

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).

TNM_SDW – See preceding B.1 for TNM_SDW. There is no further requirement to complete the remainder of the PIA document for TNM_SDW. NO personal information is collected, maintained, or used that is identifiable to the public individual or employee as detailed in the preceding for TNM_SDW.

TNM_NGTOC – Yes, information is identifiable to the individual.

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).

TNM_NGTOC – No information about members of the public exists in the system.

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).

TNM_NGTOC – Yes, as specified in Question 1.

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

TNM_NGTOC – The purpose of the TNM_NGTOC system is to provide essential support and functionality for the acquisition and management of trusted geospatial data, products, and services in support of *The National Map*. **Note that any information about individuals contained in TNM_NGTOC is limited to that data that is stored on servers for data protection/backup purposes.** In that context, the purpose of having that information is to maintain timely and

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).

accurate employee data as well as financial and budgetary information for the cost center.

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

TNM_NGTOC:

Employee Administrative Records - Interior, DOI-58; 5 U.S.C. 301, 3101, 5105-5115, 5501-5516, 5701-5709; 31 U.S.C. 66a, 240-243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C. 3101; Executive Order 11807

Personnel Records – Interior, DOI-79; 5 U.S.C. 2951, 5 U.S.C. 2954

Payroll, Attendance, Retirement, and Leave Records – Interior, DOI-85; 5 U.S.C. 5101, et seq; 31 U.S.C. 3512

Accounts Receivable: FBMS – Interior, DOI-86; 5 U.S.C. 5514; 31 U.S.C. 3701 and 3702; 31 U.S.C. 3711 et seq.; and 26 U.S.C. 6402

Acquisition of Goods and Services: FBMS – Interior, DOI-87; Chapter 1 of Title 48, CFR Chapter 1 (Federal Acquisition Regulation).

Travel Management: FBMS – Interior, DOI-88; 5 U.S.C. Chapter 57 and implementing Federal Travel Regulations (41 CFR 300-304); and 31 U.S.C. 3511 and 3512.

Grants and Cooperative Agreements: FBMS – Interior, DOI-89; 5 U.S.C. 5701 et seq.

C. DATA in the SYSTEM:

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

TNM_NGTOC – Federal employees, students, volunteers, and contractors are the categories of individuals covered by 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?**

TNM_NGTOC – Information is taken from the individual, as well as from the following:

Financial and Business Management System (FBMS)
Federal Personnel & Payroll System (FPPS)

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

TNM_NGTOC – None

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

TNM_NGTOC – None

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

TNM_NGTOC – None

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

TNM_NGTOC – Name, address, date of birth, phone number, and SSN will be collected from the employee. No information regarding members of the public resides in this system.

SDW – N/A

3) Accuracy, Timeliness, and Reliability

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

TNM_NGTOC – Individual information such as address and phone number is periodically reviewed and corrected by the individual.

b. How will data be checked for completeness?

TNM_NGTOC – Information will be periodically reviewed by the individual.

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).

TNM_NGTOC – Information is periodically reviewed by the individual and if necessary, corrections are made.

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

TNM_NGTOC – The data elements are described in detail and documented in the System of Record.

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?**

TNM_NGTOC – Yes. **Note that that any information about individuals contained in TNM_NGTOC is limited to that data that is stored on servers for data protection/backup purposes.** In that context, the purpose of the data use is to ensure that information required to maintain timely and accurate employee data as well as financial and budgetary information for the cost center is available when required.

- 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?**

Note that that any information about individuals contained in TNM_NGTOC is limited to that data that is stored on servers for data protection/backup purposes. In that context, the TNM_NGTOC system itself cannot derive new data or create previously unavailable data. New payroll data can be derived daily, but normally is updated on a biweekly basis. The information is maintained and filed by name, SSN, or other appropriate designation such as hours, grade, pay rate, etc. These actions occur through applications outside of the TNM_NGTOC (NMRP) system boundary.

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

TNM_NGTOC – The data will be placed in the individual's record in the existing file system.

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

TNM_NGTOC – Yes.

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

TNM_NGTOC – New personal data will be verified for relevance and accuracy through periodic review by the individual. New payroll data is verified through system checks and balances and through reports generated and checked by the payroll administrators. These actions occur through applications outside of the TNM_NGTOC (NMRP) system boundary.

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

TNM_NGTOC – Access controls prevent unauthorized access of private data.

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

TNM_NGTOC – Proper controls are in place to protect the data and prevent unauthorized access. Select privileges are granted before data / reports can be accessed and/or generated. All data is protected by access control lists and menu options.

- 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.**

TNM_NGTOC – The data will be retrieved through the use of the individual's name, SSN, or other unique identifier.

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

Payroll, time and attendance, and emergency notification are reports that can be produced on individuals. These reports will be used to verify information and only authorized personnel 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.)**

TNM_NGTOC - Information is used only for the purposes for which it is gathered. Individuals have the right to decline to provide information at the time of the information request.

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?**

TNM_NGTOC – Coordination between the NGTOC employees with compliance responsibilities and those who have the need to work with the identified data.

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

TNM_NGTOC – The retention periods of data are described in the individual Systems of Records for each system referenced.

- 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?**

TNM_NGTOC – Personal data that has become obsolete will be deleted by the responsible individual. Printed reports of payroll and financial data are kept in a controlled environment and will be shredded at the end of their useful life cycle. Data that has been backed up will be either overwritten by the tape rotation cycle or the backup media will be properly destroyed. Procedures are documented in the individual System of Record.

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

TNM_NGTOC – No.

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

TNM_NGTOC – N/A

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

TNM_NGTOC – Yes. **Note that any information about individuals contained in TNM_NGTOC is limited to that data that is stored on servers for data protection/backup purposes.** In that context, users are identified and authenticated to the system through their logon name and password. If the user is unauthorized to access the information, access controls will deny access to the system in general or the data in particular.

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

TNM_NGTOC – Audit trails of user activity are kept. Invalid logon attempts are recorded.

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

TNM_NGTOC – Access Control Lists are in place to guard against unauthorized access.

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

TNM_NGTOC:

Employee Administrative Records - Interior, DOI-58

Personnel Records – Interior, DOI-79

Payroll, Attendance, Retirement, and Leave Records – Interior, DOI-85

Accounts Receivable: FBMS – Interior, DOI-86

Acquisition of Goods and Services: FBMS – Interior, DOI-87

Travel Management: FBMS – Interior, DOI-88
Grants and Cooperative Agreements: FBMS – Interior, DOI-89

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

TNM_NGTOC - No. While it is highly likely that the data will be modified on a daily basis, the type of data collected will remain static.

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)

TNM_NGTOC – Access will be obtained only by those whose names are on the Access Control Lists of the system.

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

TNM_NGTOC – Access to the data is determined by an individual’s “need-to-know”, job description, and decision of management. Criteria, procedures, controls, and responsibilities regarding access are documented by those responsible for the data.

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

TNM_NGTOC – The user’s access will be restricted to only the data that pertains to their specific job function.

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)

TNM_NGTOC – Access Control Lists are in place to prevent unauthorized users from gaining access to the system. Users who have access to personal data are required to use such measures as screen locks, secure password schemes, etc. in order to safeguard data that is accessed through desktop computer systems. All employees, including contractors and volunteers, are required to complete the mandatory IT Security Awareness Training on an annual basis.

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?

TNM_NGTOC – Contractors will be involved in updating their own personal information on the system such as emergency contact information. Contractors are required to complete the mandatory IT Security Awareness Training on an annual basis. Privacy Act concerns are addressed in their contracts.

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

TNM_NGTOC – Other systems such as FPPS and FBMS interact with the data on either a daily or biweekly basis. These systems reside outside of the TNM_NGTOC (NMRP) system boundary.

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

NGTOC, Shared Services Managers

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

TNM_NGTOC – No.

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

TNM_NGTOC – N/A

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

TNM_NGTOC – N/A