ADAMS ML20063L676

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

National Source Tracking System (NSTS)

Date: February 25, 2020

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The National Source Tracking System (NSTS) is a resident application within the Integrated Source Management Portfolio (ISMP) and is owned by the Office of Nuclear Material Safety and Safeguards (NMSS). The purpose of the system is to track information on the manufacture, transfer, receipt, disassembly and disposal of nationally tracked radioactive sources. The list of nationally tracked sources is provided in Title 10 *Code of Federal Regulations* Part 20, Appendix E. The NSTS does not ensure the physical protection of sources rather it provides greater source accountability, which should foster increased control by NRC and Agreement State licensees.

2. What agency function does it support?

The purpose of the system is to track information on the manufacture, transfer, receipt, disassembly and disposal of nationally tracked radioactive sources. The list of nationally tracked sources is provided in Title 10 *Code of Federal Regulations* Part 20, Appendix E.

3. Describe any modules or subsystems, where relevant, and their functions.

N/A

4. What legal authority authorizes the purchase or development of this system?

Title VI - Nuclear Matters, Sub-Title D - Nuclear Security, of the Energy Policy Act of 2005.

5. What is the purpose of the system and the data to be collected?

The purpose of the system is to track information on the manufacture, transfer, receipt, disassembly and disposal of nationally tracked radioactive sources.

6. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
Joel Bristor	NMSS/PMDA	301-415-0299
Business Project Manager	**Office/Division/Branch**	**Telephone**
Ernesto Quinones	NMSS/MSST/SMPB	301-415-0271
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Joel Bristor	NMSS/PMDA	301-415-0299
Executive Sponsor	**Office/Division/Branch**	**Telephone**
John W. Lubinski	NMSS	301-415-5975
ISSO	**Office/Division/Branch**	**Telephone**
Rich Kristobek	NMSS/PMDA	301-415-5638
System Owner/User	**Office/Division/Branch**	**Telephone**
John W. Lubinski	NMSS	301-415-5975

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ____ New System

____ Modify Existing System

__X__ Other (Just updating information elements in the PIA).

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

The application is not being modified at this time, just updating the PIA.

(1) If yes, provide the date approved and ADAMS accession number.

November 29, 2019, ML19206A923.

(2) If yes, provide a summary of modifications or other changes to the existing system.

8. **Do you have an NRC system Enterprise Architecture (EA)/Inventory number?**

YES

a. If yes, please provide Enterprise Architecture (EA)/Inventory number.

20050004.

b. If, no, please contact EA Service Desk to get Enterprise Architecture (EA)/Inventory number.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

YES

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).

Federal employees, Federal contractors, licensees' business contacts and Radiation Safety Officers (RSO).

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific – e.g. SSN, Place of Birth, Name, Address)?

The only information about individuals collected by and maintained in the NSTS are the names of the Radiation Safety Officer and a business contact as supplied by the licensee.

c. Is information being collected from the subject individual?

NO

(1) If yes, what information is being collected?

N/A

d. Will the information be collected from individuals who are not Federal employees?

YES

(1) If yes, does the information collection have OMB approval?

YES

(a) If yes, indicate the OMB approval number:

OMB clearance No. 3150-0202 provides authority to the NRC for NRC Form 748 “National Source Tracking Transaction Report”, which covers the data elements needed for source tracking.

e. Is the information being collected from existing NRC files, databases, or systems?

NO

(1) If yes, identify the files/databases/systems and the information being collected.

f. Is the information being collected from external sources (any source outside of the NRC)?

YES

(1) If yes, identify the source and what type of information is being collected?

The information is collected from the business management of each licensee. The only information about individuals are the names of the Radiation Safety Officer and a business contact as supplied by the licensee.

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

This information is verified during the business process of reviewing

licensee applications, which is conducted by the Office of Nuclear Material Safety and Safeguards (NMSS).

h. How will the information be collected (e.g. form, data transfer)?

This information is collected through smart forms, wherein the licensee sends the data by clicking a Submit button on the form. An alternate reporting method is facsimile transmission of scanned transaction reporting forms.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. **Will information not about individuals be maintained in this system?**

YES

(1) If yes, identify the type of information (be specific).

The information in NSTS is specific to the status (e.g., manufacture, transfer, or disposal) of radioactive sealed sources of concern nuclear materials licensees and related inventories maintained by each affected licensee.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Licensees are required to report all transactions that result in changes in the status or possession of radioactive sealed sources of concern as covered under 10CFR20. Licensees are also required to validate their NSTS inventory information annually.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

The primary use of NSTS data is to ensure readily available, accurate information on the location of each radioactive source of concern. Through this, incident response analyses can readily assess security and exposure risks for a given radioactive material type within a given geographic location.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

YES

3. Who will ensure the proper use of the data in this system?

NMSS

4. Are the data elements described in detail and documented?

YES

a. If yes, what is the name of the document that contains this information and where is it located?

The data dictionary, which covers all ISMP applications is maintained in BitBucket. The data dictionary resides in:

Project: ISMP
Repository: ISMP_Int
Folder: DB
Filename: ISMP_Data_Dictionaries_Revised_V2.66.xlxs.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

NO

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)

NO
The data is generally retrieved by radioactive source attributes, including the radioactive isotope, activity level and location. In cases of materials license possession limit verification, the data may be retrieved by license number.

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

N/A

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

NO

a. If "Yes," provide name of SORN and location in the Federal Register.

N/A

8. If the information system is being modified, will the SORN(s) require amendment or revision?

N/A

9. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

NO

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

10. List the report(s) that will be produced from this system.

Report Name	Frequency	Used For
Monthly Submission and Transaction Report	Monthly	Monitoring regulatory compliance and system burden
PD-593 NSTS Transactions by User	Monthly	Monitoring regulatory compliance and system burden
PD-670 NSTS Transactions by Licensee	Monthly	Monitoring regulatory compliance and system burden
Pending Transfers	Weekly	Monitoring of compliance with timely reporting requirements

PD-633 Source Stats by Isotope	Quarterly	Ongoing statistical analyses
PD-644 Total Activity by Isotope	Quarterly	Ongoing statistical analyses
NSTS Data Dump for Google Earth	As needed	For event responses and routine geographic data analyses

a. What are the reports used for?

Please see table above.

b. Who has access to these reports?

NMSS source protection and incident response staff.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Any Office (HQ and Regional) that can verify a need. Most will be provided read-only access.

(1) For what purpose?

HQ and Regional personnel require access to NSTS to ensure the integrity of the data being reported by licensees and to verify licensee compliance with the reporting requirements found in 10 CFR Part 20. In addition, during times of emergencies HQ and Regional staff, working closely with Federal partners and State agencies, utilize the information within NSTS to ensure the safety and security of Category 1 and 2 radioactive materials.

(2) Will access be limited?

YES

Access to NSTS is restricted to users approved by NMSS or Agreement State representatives and within those groups by specifically assigned roles.

2. Will other NRC systems share data with or have access to the data in the system?

NO

(1) If yes, identify the system(s).

N/A

(2) How will the data be transmitted or disclosed?

N/A

3. Will external agencies/organizations/public have access to the data in the system?

YES

(1) If yes, who?

- Authorized NRC personnel;
- Authorized Agreement State (AS) Agency personnel;
- Authorized NRC Licensee personnel; and
- Authorized AS Licensee personnel.

(2) Will access be limited?

YES

(3) What data will be accessible and for what purpose/use?

User type	Data accessible	Purpose/use
NRC personnel	All NSTS data	For monitoring regulatory compliance and for event response risk assessment
Agreement State (AS) Agency personnel	All source data for licensees regulated by a given AS Agency	For monitoring regulatory compliance and for event response risk assessment
NRC Licensee personnel	All source data for the given licensee	To report source transactions and to review current licensee inventory
AS Licensee personnel	All source data for the given licensee	To report source transactions and to review current licensee inventory

(4) How will the data be transmitted or disclosed?

Via NSTS online web interface.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 U.S.C., 36 CFR). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management (RIM) and NARA's Universal Electronic Records Management (ERM) requirements, and if a strategy is needed to ensure compliance.

1) **Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule(NUREG-0910), or NARA's General Records Schedules?** YES

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

The current NARA approved schedule is N1-431-08-6 (9/25/2012). This schedule states the following for NSTS:

Master File:

Temporary. Cut off records when the source is disposed of or disassembled or is combined into a new source. Delete or destroy records 10 years after cutoff.

Annual Data Verification Confirmation and Correction:

Temporary. Cut off data related to annual verification information at the end of this calendar year. Transfer data to inactive storage 10 years after cutoff with the appropriate system documentation. Destroy 20 years after cutoff.

Information used to Prepare Formal Reports [see List of Reports on page 7 of 2019 PIA]:

Temporary. Cut off when superseded or NRC Published Report is issued. Destroy information 5 years after cutoff.

b. If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

Users must apply for access to the system. To apply for NSTS a potential user must use the ISMP Portfolio Enrollment Module (PEM) to enter their name, business and basic license information then PEM passes that information over to the Identity, Credential, and Access Management system (ICAM) owned by OCIO. The PEM Privacy Impact Assessment (ML17033B413) review determined that PEM is covered by the Privacy Act, does not contain any Personally Identifiable Information (PII) and is covered under the OCIO NRC-45 Digital Certificates for Personal Identify Verification. The NRC or Agreement State agency program sponsor must then approve the user for access and assign the appropriate role. The user then goes through an identity verification process that is performed via NRC's ICAM. Once approved, the user accesses NSTS via a One-Time-Password device or X.509 digital certificate.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

All user access to NSTS is controlled via Role Based Access Controls.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

YES

(1) If yes, where?

The NSTS System Architecture Document (SAD), version 4.2, dated April 1, 2018 (ML18102B288), the ISMP Operations Support Guide, version

5.5, dated October 11, 2019 (ML19298C470) and the most recent ISMP System Security Plan (SSP), version 4.5, dated February 7, 2020 (ML20041E324).

4. Will the system be accessed or operated at more than one location (site)?

YES

a. If yes, how will consistent use be maintained at all sites?

As a component resident application of the ISMP, NSTS operates in the Microsoft Azure Government Cloud Virginia Region. NSTS is supported at the Leidos Gude Drive, Rockville, Maryland location via an Express Route connection to Microsoft Azure. NSTS is supported at the Leidos Richland, Washington location via an IPSEC tunnel to ISMP.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

Authorized NRC and Agreement State Agency users and credentialed Licensees.

6. Will a record of their access to the system be captured?

YES

a. If yes, what will be collected?

The NSTS application audit mechanism captures end user and application administrator access to the application. The following information is captured in the audit records: date and time of the event; the component of the information system (Internet Protocol (IP) address) where the event occurred; type of event; user/subject identity; and the outcome (success or failure) of the event.

7. Will contractors be involved with the design, development, or maintenance of the system?

YES

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*

- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

The NSTS application audit mechanism captures end user and application administrator access to the application.

The NSTS application implements role-based authorization, granting access to users based on their assigned role. The role assignment function is restricted to the application administrator. With regard to system administrator access, assigned authorizations to access the NSTS servers are enforced using the Windows operating system role-based access control mechanism.

All NSTS servers have anti-virus software, host-based intrusion prevention software, and host-based firewalls installed. Anti-virus software is configured for at least daily virus-definition updates. Network protections include layered firewall design that implements rule sets to deny all and permit by ***exception***. Network security groups provide the ability to filter traffic by source and destination IP address, port, and protocol and User Defined Routes (UDR) control the flow between each subnet. Additional technical safeguards and monitoring is provided using SecureVue SIEM, Tripwire (file integrity monitoring), ePO, Nessus (vulnerability scanner), Intrusion Prevention Systems, and F5's ASM (Application Security Manager).

9. Is the data secured in accordance with FISMA requirements?

YES

a. If yes, when was Certification and Accreditation last completed?

The ISMP Authority to Operate (ATO) was last renewed on July 16, 2018 (ML18197A165) and ISMP has since maintained its ATO via continuous monitoring. The NSTS ATO was approved on January 13, 2009 (ML083530155) and was incorporated into ISMP via the Security Impact Assessment process.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/ISB Staff)

System Name: National Source Tracking System (NSTS)

Submitting Office: NMSS

A. PRIVACY ACT APPLICABILITY REVIEW

_X_ Privacy Act is not applicable.

____ Privacy Act is applicable.

Comments:
The only information about individuals collected by and maintained in the NSTS are the names of the Radiation Safety Officer and a business contact as supplied by the licensee. Information is not retrieved by personal identifiable information.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	3/25/2020

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

____ OMB clearance is needed.

_X_ Currently has OMB Clearance.

Comments:
OMB Clearance 3150-0202 covers the collection of information in NSTS and NRC Form 748.

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	3/19/2020

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

_X_ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	3/18/2020

D. BRANCH CHIEF REVIEW AND CONCURRENCE

_X_ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

____ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/ Date: March 27, 2020

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **John W. Lubinski, NMSS**	
Name of System: **National Source Tracking System (NSTS)**	
Date ISB received PIA for review: **March 2, 2020**	Date ISB completed PIA review: **March 25, 2020**
Noted Issues:	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: /RA/ March 27, 2020
Copies of this PIA will be provided to: *Thomas Ashley, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Governance & Enterprise Management Service Division* *Office of the Chief Information Officer*	