



Tennessee Valley Authority Privacy Impact Assessment (PIA)

NETRMS

This PIA is a tool used by the TVA Privacy Office to identify system privacy risks at the planning/initiation phase of the system development lifecycle (SDLC). The PIA should be reviewed and updated every three years in conjunction with the anniversary of the Authority to Operate (ATO) or sooner, if the system undergoes a major change. For additional guidance on how to complete this PIA, please refer to the TVA Guide to Completing Required Privacy Documentation. Questions regarding this document should be directed to camarsalis@tva.gov.

PIA should be submitted to:
Christopher Marsalis
TVA Senior Privacy Program Manager
(865) 632-2467
camarsalis@tva.gov

Version 1.0
August 2013





PROGRAM MANAGEMENT


Name of PIA Author	Chris Marsalis	
Date of Submission	4-14-2014	System Owner Details
Responsible TVA Business Unit	TVA Security	Name: Richard Fisher Title: Program Manager Phone: 865-632-3780 Email: rfisher@tva.gov
Name of System/Collection	NETRMS	
Configuration Item	Not Assigned	
Reason for completing PIA	<input type="checkbox"/> New system <input type="checkbox"/> Significant modification to an existing system <input checked="" type="checkbox"/> To update existing PIA for a triennial security reauthorization	

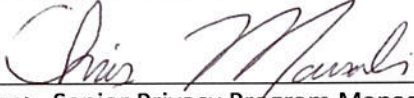
PRIVACY DETERMINATION

(To be completed by the TVA Privacy Program)

Privacy Office Comments	
--------------------------------	--

The signatures below certify that the information in this document has been reviewed and approved:

1.  4/17/14
 <Name>, System Owner Date

2.  4/17/14
 <Name>, Senior Privacy Program Manager Date

3. _____
 <Name>, Senior Agency Official for Privacy Date

SYSTEM OVERVIEW

1. Please describe the purpose of the system/collection:

<Develop a detailed description of the purpose(s) for which personally identifiable information (PII)¹ is collected, used, maintained, and shared. The section must tell a complete story including system name and acronym, the Business Unit that owns the system, mission of the Business Unit, purpose of the system, description of a typical transaction, the subjects of the collection, how information is collected (if not stated in the transaction), how information is retrieved, and any connections to other internal or external systems. If connections to other external systems exist, include information on relevant memorandum of understanding (MOU) allowing for the data sharing.>

Web Based application that contains information related to case investigation reports of all forms of incidents or events, visitor and employee registers occurring within the jurisdiction of TVA

2. What type of information can be collected, maintained, used, and/or disseminated? Check all that apply:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Mother's Maiden Name |
| <input checked="" type="checkbox"/> Home Phone | <input checked="" type="checkbox"/> Date of Birth |
| <input checked="" type="checkbox"/> Home Address | <input type="checkbox"/> Place of Birth |
| <input checked="" type="checkbox"/> Social Security number (SSN) | <input type="checkbox"/> Employment Information |
| <input type="checkbox"/> Medical or Health Information | <input checked="" type="checkbox"/> Criminal History |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Biometric Information |
| <input type="checkbox"/> Clearance Information | <input type="checkbox"/> Other: <Please specify> |

¹ OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, defines PII as information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.



AUTHORITY AND PURPOSE

3. Legal authority to collect, use, maintain, and share data in the system:	
<i><Include information on the legal authority that permits the collection, use, maintenance, and sharing of data in this system. The system of records notice (SORN) will contain details regarding the authorities. If SSNs are collected, please specify the legal authority for that collection.></i> Tennessee Valley Authority Act of 1933, 16 U.S.C 831-831ee; 5 U.S.C. 552a; and 28 U.S.C. 534	
4. For each box checked above in Question 2, please provide the business need for the collection:	Information related to case investigation report of all forms of incidents or events, visitor and employee registers occurring within the jurisdiction of of TVA
5. Will this information be retained in a Privacy Act System of Records Notice (SORN)? If data in the system can be retrieved using one or more of the identifiers listed in Question 2, this system is subject to the Privacy Act and requires a SORN.	<input type="checkbox"/> No <input checked="" type="checkbox"/> Yes TVA-37 TVA Police Records

ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT

6. What TVA employees and business units are responsible for the privacy governance and administration of this system?	
TVA's Office of the Chief Information Officer is the responsible program owner for TVA's Information Security and Privacy Programs, ensuring compliance with TVA-SPP-12.02, TVA Information Management Policy. TVA-SPP-12.02 implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government At of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) mandates, and other applicable North American Electric Reliability Corporation (NERC) and TVA Records Management procedures and guidance. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention and destruction of federal records. Federal and contract employees are given clear guidance in their duties as they relate to the collection, use, processing and security of privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, including "TVA Information Security Training". (See: TVA-SPP-12.01 §3.2.10.) The TVA Privacy Office will conduct period privacy compliance reviews of the [INSERT SYSTEM NAME] (ACRONYMN) in accordance with the requirements of the Office of Management and Budget (OMB) Circular A-130. TVA Police and Emergency Management	
7. What privacy orientation or training is provided to authorized users of the system?	
<i><Describe privacy orientations or training provided authorized users of the system, including if the training is tailored to differentiate and emphasize the privacy requirements of the specific system instead of simply covering basic topics common to any system. Describe any features about the operation and administration of the system that make users continuously aware of their access responsibilities.></i> All employees are required(beginning in 2014) t o complete an Online training module to increase awareness of privacy requirements and to ensure all TVA personnel understand their responsibilities in safeguarding personal information in the workplace. The training module will cover the procedures and best practices for Protecting Personally Identifiable Information (PII) and Restricted Personally Identifiable Information (RPPII). These procedures and best practices correspond to applicable laws and regulations for protecting the confidentiality, integrity, and availability of PII and RPPII.	



DATA QUALITY AND INTEGRITY

7. How is data quality is ensured throughout the data lifecycle and business processes associated with the use of the data? Check all that apply.

- Cross referencing data entries with other systems
- Character limits on text submissions
- Third party data verification
- Numerical restrictions in text boxes
- Data taken directly from individuals via a form(s). Please list form(s) name and number here:
- Other: <Please specify>

DATA MINIMIZATION AND RETENTION

8. What are the retention periods for the data in the system?

< Please describe policies, processes and procedures (if any) for retaining data in the system. This information should be consistent with the [TVA records disposition schedules \(RDS\)](#) published by National Archives and Records Administration. If your system does not have a RDS, please work with Records Management to complete and submit the [Standard Form \(SF\) 115](#) to obtain a job number and include details here regarding the proposed records schedule.>

TVA records retention schedule applies to this application

INDIVIDUAL PARTICIPATION AND REDRESS

9. How can an individual access their information and have it corrected, amended, or deleted?

Subject to the limitations of the Privacy Act, individuals may request access to information about themselves contained in a TVA system of records through TVA's Privacy Act/Freedom of Information Act (FOIA) procedures. Concurrent with the publication of <<Insert Name of SORN>>, exemptions from the access provisions of the Privacy Act may apply. TVA will review all Privacy Act requests on an individual basis and may as appropriate, waive applicable exemptions if the release of information to the individual would not detrimentally impact the law enforcement or national security purposes for which the information was originally collected or is subsequently being used. Submitting a Privacy Act Request is accomplished by sending a letter to the system manager listed on the cover of this PIA. The request should include the following:

- Name
- Mailing address
- Phone number or email address
- A description of the records sought, and if possible, the location of the records

Contesting record procedures: Individuals wanting to contest information that is contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected. Requests should be submitted to the attention of the TVA Privacy Office at the address below:

Tennessee Valley Authority
 Privacy Office
 400 W. Summit Hill Dr.
 Knoxville, TN 37902-1499

Individuals with concerns about privacy may also email the TVA Privacy Officer via the contact information provided in the privacy policy on the TVA's web site (<http://www.tva.gov/abouttva/privacy.htm>).

This information is provided in the [Privacy Policy](#), posted visibly on the TVA Web site.

SECURITY

<p>10. Has the Security Authorization Process (SAP) been completed?</p>	<p><input type="checkbox"/> Not applicable <input type="checkbox"/> Under Development: <Expected date of completion> <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes: <Date of Authority to Operate (ATO)></p>
<p>11. What types of physical safeguards exist to protect the information?</p>	<p><input checked="" type="checkbox"/> Guards <input type="checkbox"/> Biometrics <input checked="" type="checkbox"/> Identification Badges <input type="checkbox"/> Closed Circuit TV (CCTV) <input type="checkbox"/> Other: <Please specify></p>
<p>12. What types of access controls are in place to protect the information?</p>	<p><input checked="" type="checkbox"/> User Identification <input type="checkbox"/> Passwords <input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Virtual Private Network (VPN) <input type="checkbox"/> Public Key Infrastructure (PKI) <input type="checkbox"/> Smart Cards <input type="checkbox"/> Other: Encrypted Server</p>
<p>13. What types of administrative safeguards exist to protect the information?</p>	<p><input type="checkbox"/> Contingency Plan <input checked="" type="checkbox"/> User manuals for the system <input checked="" type="checkbox"/> Regular Back-up of files <input type="checkbox"/> Rules of Behavior <input type="checkbox"/> Offsite storage of back up files <input type="checkbox"/> Least privilege access <input type="checkbox"/> User training <input type="checkbox"/> Other: <Please specify></p>
<p>14. What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage?</p>	<p>Privacy Impact Assessments</p>
<p>15. Discuss any other potential privacy vulnerabilities to the system and safeguards that are in place to mitigate those vulnerabilities:</p>	<p>Access is limited by user id and password. Data is protected by an encrypted server.</p>

TRANSPARENCY

<p>16. How are individuals notified as to how their information will be collected, used, and/or shared within this system? N/A</p>



USE LIMITATION

17. Explain how the information in the system is limited to the uses specified in the notices discussed above.
Information is not shared
18. With which (if any) internal TVA systems/collections is the information shared?
N/A
19. With which (if any) organizations external to TVA is information shared?
<i>< For each instance of sharing, please provide how the information is share, for what reason the information is shared, and what safeguards are in place for the sharing arrangement(s). If contractors are authorized to access and/or administer the system, please also include that information here.></i> Law Enforcement Agenies
20. What methods are used to analyze the data?
N/A

END FORM

Please submit completed form to:

**Christopher Marsalis
TVA Senior Privacy Program Manager
(865) 632-2467
camarsalis@tva.gov**

