



## **Tennessee Valley Authority Privacy Impact Assessment (PIA)**

---

### ***TVA Enterprise Emergency Notification System (TEENS)***

This PIA is a tool used by the TVA Privacy Office to identify privacy risks at the planning/initiation phase of the system development lifecycle (SDLC) or early stages of project/program development. The PIA should be reviewed and updated on an annual basis, or sooner, if the system undergoes a major change. Questions regarding this document should be directed to [privacy@tva.gov](mailto:privacy@tva.gov).

PIA should be submitted to:

TVA Privacy Office  
[privacy@tva.gov](mailto:privacy@tva.gov)

Version 3.0  
September 2018



PROGRAM MANAGEMENT

Author Name

[Redacted]

Date of Submission

03/04/2024

Responsible TVA Business Unit

TVAP Emergency Mangement

Name of System

TVA Enterprise Emergency Notification System

System Owner Details

Reason for Completing PIA

Name  
Title  
Phone  
Email

[Redacted]

- New system
- Significant modification to an existing system
- To update existing PIA for a security authorization

PRIVACY DETERMINATION  
(To be completed by the TVA Privacy Program)

Privacy Office Comments

[Redacted]

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

	Name	Signature	Date
System Owner	[Redacted]	[Redacted]	03/04/2024
Senior Privacy Program Manager	Chris Marsalis	Chris Marsalis (E-Signature)	03/04/2024



### SYSTEM OVERVIEW

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

The TVA Enterprise Emergency Notification System (TEENS) is used to notify key employees about business-related emergencies or to quickly alert many employees of an urgent situation. This can also be used to alert external stakeholders. It has the capabilities to deliver messages by various means, including e-mail, telephonically, and by SMS. Employee contact information is collected, including name, work address, work email, work phone number, home phone number if provided in the HR system, and work/personal cell phones.

2. About whom does the system collect, maintain, use and/or disseminate information? Check all that apply:

- TVA employees
- TVA contractor
- Members of the public

3. Is the information collected directly from the individual?

- Yes     No    How is the information collected? Information is from PLUS

4. What type of personally identifiable information (PII) can be/is collected, maintained, used, and/or disseminated?

Check all that apply: (Per the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.)

- |  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> Home Phone             | <input type="checkbox"/> Financial Information         | <input type="checkbox"/> Biometric Information  |
| <input type="checkbox"/> Home Address                      | <input type="checkbox"/> Clearance Information         | <input type="checkbox"/> Citizenship  |
| <input checked="" type="checkbox"/> Home Email             | <input type="checkbox"/> Mother's Maiden Name          | <input type="checkbox"/> Driver's License Number  |
| <input checked="" type="checkbox"/> Employment Information | <input type="checkbox"/> Date of Birth                 | <input type="checkbox"/> Username/Password  |
| <input checked="" type="checkbox"/> Work Address           | <input type="checkbox"/> Place of Birth                | <input type="checkbox"/> Passport Number  |
| <input checked="" type="checkbox"/> Work Phone             | <input type="checkbox"/> Criminal History              | <input type="checkbox"/> Other:   |
| <input checked="" type="checkbox"/> Work Email             | <input type="checkbox"/> Social Security number (SSN)  | <div style="border: 1px solid black; width: 150px; height: 15px; margin-left: 10px;"></div> |
| <input checked="" type="checkbox"/> Name                   | <input type="checkbox"/> Medical or Health Information |   |

If none of the above data elements are checked, stop and submit this PTA as-is to TVA Privacy Office at [privacy@tva.gov](mailto:privacy@tva.gov). Otherwise, please continue completing the remaining questions in the document.

### Privacy Notice and Transparency

5. Legal authority to collect, use, maintain, and share data in the system:

Tennessee Valley Authority Act of 1933, 16 U.S.C. 831-831ee; 5 U.S.C. 552a; and 28 U.S.C 534

6. Does the system have a SORN? (If PII in the system is retrieved using one or more of the identifiers listed in Question 4, a System of Records Notice (SORN) is required.)

- Yes     No

List name(s) of applicable SORN(s): TVA-37 Police Records

7. How are individuals notified as to how their information will be collected, maintained, used, and/or disseminated within this system?

Privacy Impact Assessments, Privacy Act Statements, System of Records Notice (SORNs)



8. What consent options do individuals have regarding specific uses or sharing of their information?

Individuals are not provided consent for specific uses or sharing of their information.

**DATA MINIMIZATION**

9. Are only the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose collected, used and retained?

- Yes  No

10. What are the retention periods for the information in the system?

Individual records are retained only as long as the individuals are active employees or contractors. Detailed reports on notification contacts are retained in TEENS for a minimum of 90 days, but often much longer. Reports can be deleted manually.

**DATA QUALITY**

11. How is data quality (i.e., accuracy, relevance, timeliness, and completeness) ensured throughout the data lifecycle and business processes associated with the use of the information? Check all that apply.

- Information is collected directly from individuals (preferred method of collection, whenever possible)

If collected via a form, please list form(s) name and number here:

[Empty text box]

- Cross referencing information entries with other systems  Third party information verification
- Character limits on text submissions  Numerical restrictions in text boxes
- Other: [Empty text box]

12. How is inaccurate or outdated information checked for and corrected?

The data in TEENS matches the source systems (PLUS/ValleyConnect).

**Access and Redress**

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

The individual would go through PLUS to have any information corrected, amended, or deleted.

**Internal and External Sharing**

14. Explain how the information in the system is limited to the uses specified in the notices discussed above.

The system is limited to TVA authorized users. The use of PII is solely for the purpose(s) specified in the notices above.

15. With which (if any) internal TVA systems is the information shared?

PLUS, Valley Connect

16. With which (if any) organizations external to TVA is information shared?

None.

17. Does the system have any associated websites/applications including an external TVA website or third-party owned or managed website or application (e.g., Facebook, YouTube, Twitter, Flickr, etc.)?

Yes     No

Please describe and provide link: <https://tva.mir3.com/jsp/security/showLogin.jsp>

i. Does the website or application allow individuals to submit comments, feedback or messages?

- Yes
- Yes, but the feature will be turned off
- No

ii. Does the website or application allow individuals to submit comments, feedback or messages?

- Yes, but TVA does not have access to any system information.
- Yes, TVA has access to the collected information, but only single-session technologies are used.
- Yes, TVA has access to the collected information, and multi-session technologies are used.
- No

### SECURITY

18. What privacy orientation or training is provided to authorized users of the system or individuals with access to the system?

[Redacted]

19. Has a FIPS 199 determination been made?

[Redacted]

20. What is the FIPS 199 determination? Check one for each.

[Redacted]



21. What types of technical safeguards are in place to protect the information?

[Redacted]

22. What types of physical safeguards exist to protect the information?

[Redacted]

23. What types of administrative safeguards exist to protect the information?

[Redacted]

24. What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage?

All monitoring, recording, and auditing safeguards to prevent and detect unauthorized access or inappropriate usage is applied through TVA Cybersecurity.

25. Discuss any other potential privacy risks to the information within the system and safeguards that are in place to mitigate those risks.

None.

Please submit completed form to: **TVA Privacy Office**  
[privacy@tva.gov](mailto:privacy@tva.gov)