# PRIVACY IMPACT ASSESSMENT

**References:**

NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

OMB Memo M-03-22, Subject: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. http://www.whitehouse.gov/omb/memoranda_m03-22/

**General Instructions:**

*Form 20079, Privacy Impact Assessment, is to be completed for all systems of information.*

*Questions relating to the content of this form should be directed to Enterprise Information Security & Policy at 865-632-7404 or via e-mail to itsecurity@tva.gov. Associated definitions are included as an Appendix to this document.*

This form is designed to be completed for and approved by the information system's program manager. The completed form is submitted to Enterprise Information Security & Policy at ITSecurity@tva.gov.

**Tennessee Valley Authority**

**PRIVACY IMPACT ASSESSMENT (PIA)**

**TVA Information System/Electronic Collection Name:**

iComplaint

**TVA Organization/Strategic Business Unit Name:**

Equal Opportunity Compliance

## SECTION 1: IS A PIA REQUIRED?

**a. Please refer to Section 3a(1) for a table listing the various types of Personally Identifiable Information (PII). Will this TVA information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, TVA employees or retirees, TVA contractors or vendors, or TVA business partners, distributors, or direct served customers? Select one or more from the list below.**

☒ (1) Yes, from members of the general public.

☒ (2) Yes, from TVA employees or retirees, TVA contractors or vendors, and/or TVA business partners, distributors, or direct served customers.

☐ (3) No, this electronic collection does not collect, maintain, use, and/or disseminate PII.

☐ (4) This is a National Security System. See NIST Special Publication 800-59 for definition.

**b. If "No" or a National Security System, a PIA is not required. Proceed to Section 4, Review and Approval.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

## SECTION 2: PIA SUMMARY INFORMATION

**a. Why is this PIA being created or updated? Choose one:**

☐ **New TVA Information System**

☐ **New Electronic Collection**

☐ **Existing TVA Information System**

☒ **Existing Electronic Collection**

☐ **Significantly Modified TVA Information System**

**If a new or modified information system or electronic collection, enter the projected production date: _____**

**b. Does this TVA information system have a Unique Information System ID?**

☐ **Yes** **Enter the ID** [ ]

If unsure, consult the IS Account Manager to obtain the Unique Information System ID.

☒ **No**

**c. Does the TVA information system or electronic collection have a Privacy Act System of Records Notice (SORN)?**

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** **Enter Privacy Act SORN Identifier** [**TVA–5 Discrimination Complaint Files.**]

Consult the TVA Privacy Act SORNs at:

http://www.tva.gov/foia/sysofrecords.htm

☐ **No**

**d. Does this TVA information system or electronic collection have an OMB Control Number?**

Contact the Agency Clearance Officer at ITSecurity@TVA.gov for this information. This number indicates OMB approval to collect data from 10 or more persons in a 12-month period regardless of form or format.

| | | |
|---|---|---|
| ☐ **Yes** | **Enter OMB Control Number** | |
| | **Enter Expiration Date** | |

☒ **No** **No OMB Control Number required. Does not collect data from 10 or more members of the public.**

☐ **No** **Requires OMB Control Number. Collects data from 10 or more members of the public.**

**e. Authority to collect information. A Federal law, Executive Order of the President (EO), or TVA requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same. Note: Authorities can be found under the "Authority for Maintenance of the System" on the SORN.

(2) Cite the authority for this TVA information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

Tennessee Valley Authority Act of 1933, 16 U.S.C. 831–831ee; Executive Order 11478; 42 U.S.C. 2000e–16; 29 U.S.C. 633a; Title VII of the Civil Rights Act of 1964; Age Discrimination in Employment Act of 1967; Rehabilitation Act of 1973; Genetic Information Nondiscrimination Act of 2008.

**f. Summary of TVA information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this TVA information system or electronic collection and briefly describe the types of personal information about individuals collected in the system. Include how the PII is used and protected.

Required by federal regulations. See Secion 3A.1

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Release of confidential information to unwarranted soruces. Confidential passwords.

**g. With whom will the PII be shared through data exchange (including hardcopy, electronic files, and system-to-system connections), both within TVA and outside of TVA (e.g., other Federal Agencies, contract vendors)? Indicate all that apply and include type of data exchange.**

☒ **Within TVA**. Specify

Equal Opportunity Compliance (EOC) staff

☒ **Other Federal Agencies**. Specify

Equal Employment Opportunity Commission (EEOC)

☐ **State and Local Agencies**. Specify

☐ **Contractor** (enter name and describe the language in the contract that safeguards PII.) Specify.

☒ **Other** (e.g., commercial providers, colleges). Specify.

Micropact (iComplaint vendor - host)

**h. Do other information systems share information or have access to information in this information system?**

☐ **Yes**. Specify

☒ **No**.

**i. Do individuals have the opportunity to object to the collection of their PII which is part of this system?**

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can object to the collection of PII. Include consequences, if any, if an individual objects.

(2) If "No," state the reason why individuals cannot object.

29 CFR 1614

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

☐ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent. Include consequences, if any, if an individual withholds their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

29 CFR 1614

**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

☒ **Privacy Act Statement**

☐ **Privacy Advisory**

☐ **Other**

☐ **None**

Describe each applicable format.

Hard and/or electronic copy of the EEO process Rights and Responsibilities. TVA Act of 1933. 16 U.S.C. Section 831dd, Executive Order 11478, 42 U.S.C. Section 2000e-16, 42 U.S.C. Section 633 (a).

**NOTE:**

**Sections 1 and 2 above are to be posted to the TVA Privacy Impact Assessment web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**Only those Privacy Impact Assessments that pertain to the general public are posted on the TVA Privacy Impact Assessment web site.**

**A TVA organization/strategic business unit can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**

## SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

**a. For the questions in subparagraphs 3.a.(1) through 3.a.(6), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.**

(1) **What PII will be collected or maintained in this system?** Indicate all individual PII or PII groupings that apply in the table below.

| | | |
|---|---|---|
| ☒ Age | ☒ Maiden Name | ☐ Personnel records/information** |
| ☐ Biometrics (e.g., fingerprints, DNA, blood type, etc.)** | ☒ Mailing/Home Address** | ☐ Photograph of Individual(s) |
| ☒ Birth Date** | ☐ Marital Status** | ☐ Place of Birth** |
| ☐ Change of address with court-ordered non-disclosure** | ☒ Medical Information | ☐ Professional affiliations |
| ☒ Change of home address | ☐ Medical records/information (includes psychiatric or psychological records/ information, and xrays)** | ☐ Property Title Numbers |
| ☐ Child Information** | ☐ Military Records** | ☒ Race/Ethnicity |
| ☐ Citizenship | ☐ Mother's Maiden Name** | ☒ Religious Preference |
| ☐ Criminal information** | ☐ Mother's Middle Name** | ☐ Security Clearance** |
| ☒ Disability Information** | ☒ Name | ☐ Social Security Number (SSN)** |
| ☐ Driver's License** | ☒ National or ethnic origin | ☐ Spouse Information** |
| ☐ Education Information** | ☒ Occupation or title | ☐ Taxpayer ID Number (not SSN) |
| ☐ Emergency Contact | ☐ Other | ☐ Truncated SSN (e.g., last 4)** |
| ☒ Employee ID number | ☐ Other ID Number | ☐ TVA Travel Card number** |
| ☐ Employment Information** | ☐ Other Names Used (Alias) | ☐ TVA Travel Card security code** |
| ☐ Family status/information** | ☐ Passport Number** | ☐ Vehicle ID (VIN) |
| ☐ Financial Information** | ☐ Personal affiliations | ☐ Weight |
| ☒ Gender | ☐ Personal bank account number and/or bank routing number** | ☒ Work cell phone number |
| ☐ Geographic indicator (e.g., plant or site) | ☒ Personal Cell Telephone Number | ☒ Work email address |
| ☒ Home Telephone Number | ☐ Personal credit card number** | ☒ Work FAX number |
| ☐ IP address | ☐ Personal credit card security code** | ☒ Work mailing address |
| ☐ Law Enforcement Information** | ☒ Personal Email Address | ☐ Work pager number |
| ☐ Legal Status** | ☐ Personal pager number | ☒ Work telephone number |

**Restricted PII (RPII)

If "Other," specify or explain any PII grouping selected.

(2) Approximately how many people are affected by this information system's collection of PII?

200/YR

(3) What is the source for the PII collected (e.g., individual, existing TVA information systems, other Federal information systems or databases, contractor systems, commercial systems)?

(a) What PII is being collected from the individual?

Describe.

See section 3A.1

(b) What PII is being collected from other TVA files and databases?

Describe.

See section 3A.1

(c) What PII is being collected from sources other than the individual and TVA files and databases?

Describe.

N.A.

(d) If PII is being collected from sources other than the individual and TVA files and databases, how will the information be verified as current, accurate, and complete?

Describe.

N.A.

(4) How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Face-to-Face Contact
☒ Telephone Interview
☒ Fax
☒ Email
☐ Web Site
☒ Information Sharing from System to System
☐ Other (Describe)

(5) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)? Elaborate on why the collection of PII is necessary.

Describe.

29 CFR 1614 - verification and Identification

(6) What is the intended use of the PII collected (e.g., mission-related use, administrative use)? Elaborate on the intended use of the PII.

Describe.

| Mission-related use. Processing of EEO counseling/formal complaints. |
|---|

**b. Does this TVA information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)**

☐ **Yes**

☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

| |
|---|

**c. Does this TVA information system or electronic collection provide the capability to conduct surveillance on individuals via identifying, locating, monitoring, and/or tracking?**

☐ **Yes**

☒ **No**

If "Yes," explain what risks are introduced by this capability and how this risk is mitigated.

| |
|---|

**d. Who has or will have access to PII in the TVA information system or electronic collection? Indicate all that apply.**

☐ **Users** ☐ **Developers** ☐ **System Administrators** ☐ **Contractors**

☒ **Other** (Describe)

| EOC staff and others as applicable to specific cases. |
|---|

**e. How will the PII be secured?**

(1) **Physical Controls.** Indicate all that apply.

☐ Security Guards ☐ Cipher Locks ☐ Identification Badges

☐ Combination Locks ☐ Key Cards ☐ Closed Circuit Television

☐ Safes ☒ Other (Describe)

| EOC staff access only - via restricted server. Locked file cabinets. |
|---|

(2) **Technical Controls.** Indicate all that apply.

- ☒ User Identification
- ☐ Biometrics
- ☒ Password
- ☒ Firewall
- ☒ Intrusion Detection System (IDS)
- ☒ Virtual Private Network (VPN)
- ☒ Encryption
- ☐ TVA Public Key Infrastructure Certificates
- ☒ External Certificate Authority (CA) Certificate
- ☐ TVA ID/Access Card
- ☐ Other (Describe)

(3) **Administrative Controls**. Indicate all that apply.

- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Encryption of Backups Containing Sensitive Data
- ☒ Backups Secured Off-site
- ☐ Other (Describe)

**g. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?**

Describe.

Same - see section F.2

**h. For existing TVA information systems or electronic collections, what measures have been put in place to address identified privacy risks?**

Describe.

Privacy Act Statement.

**i. For new TVA information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?**

Describe.

Existing System

**j. Does this TVA information system or electronic collection have a public-facing web presence?**

☐ **Yes**.

☒ **No**.

If "Yes,"

(1) Please provide the URL of the web site(s).

N.A.

(2) If PII is collected online from individuals, is there a link to the TVA privacy policy on each page or major entry point associated with the collection.

☐ **Yes**

☒ **No**

If no, describe.

N.A.

(3) Does the privacy policy include information pertaining to the security of the management, operational and technical controls for ensuring the security and confidentiality of individually identifiable information records?

☒ **Yes**

☐ **No**

If no, describe.

(4) Does the information system provide content (e.g., www.tvakids.com) to children under the age of 13 and collect PII from these visitors?

☐ **Yes**

☒ **No**

If yes, describe PII being collected.

N.A.

If yes, does the privacy policy contain requirements of the Children's Online Privacy Protection Act (COPPA)?

N.A.

☐ **Yes**

☒ **No**

(5) Is machine readable technology (e.g., Platform for Privacy Preferences [P3P]) adapted to automatically alert users about whether privacy practices match their personal privacy preferences?

☐ **Yes**

☒ **No**

If no, describe.

N.A.

(6) Does the web site utilize tracking and customization activities involving persistent cookies or any other means (e.g. web beacons) to track visitors' activity on the Internet?

☐ **Yes**

☒ **No**

If yes, describe the need for and use of persistent tracking technology.

(a) If the web site employs persistent tracking technology, is there a notice or link describing its use?

☐ **Yes**

☒ **No**

If yes, please provide the URL for the notice.

N.A.

**j. Who is hosting this information system or electronic collection?**

☐ **TVA**

☒ **Vendor (includes other government agencies)**

If hosted by a vendor, please provide vendor name and contract number.

On file

## SECTION 4: REVIEW AND APPROVAL

| | Name | Title | Phone # | Date |
|---|---|---|---|---|
| Prepared by: | Chris Marsalis | Senior Privacy Program Manager | 865-632-2467 | 09/25/2013 |
| Approved by: (Info System/Electronic Collection Owner) | Vyrone A. Cravanas | Senior Manager, Equal Opportunity Compliance | (865) 632-8340 | 08/15/2013 |

Please submit the completed form to Enterprise Information Security & Policy at ITSecurity@tva.gov.

**APPENDIX A - Publishing the PIA**
For use by EISP only

**Publishing:**

Only Sections 1 and 2 of this PIA will be published on the TVA Privacy Impact Assessment Web Site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

Only those Privacy Impact Assessments that pertain to the general public are posted on the TVA Privacy Impact Assessment web site.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the TVA organization/strategic business unit may restrict the publication of Sections 1 and/or 2.

**Unique PIA Number:** _____

**Date posted to the TVA PIA Web Site:** _____

## APPENDIX B - Definitions

**Aggregation of Data** - Aggregation of data is the taking of various data elements and then turning them into a composite of all the data to form another type of data such as tables or data arrays or collecting data into a single database.

**Application -** A hardware/software system implemented to satisfy a particular set of requirements.

**Availability -** Ensuring timely and reliable access to and use of information.

**Confidentiality -** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Consolidation -** Consolidation means combining data from more than one source into one system, application or process. Existing controls for the individual parts should remain or be strengthened to ensure no inappropriate access by unauthorized individuals. However, since individual pieces of data lose their identity, existing controls may actually be diminished (e.g., a summary census report may not point at the individual respondent but rather at a class of respondents, which makes it less personal).

**Data Aggregation -** Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

**Electronic Collection of Information -** Any collection of information enabled by IT.

**General Support System -** An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications and people.

**Identifiable Form -** Identifiable form means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

**Information in Identifiable Form -** Information in identifiable form is information in an information technology (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, e.g., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors.

**Information System -** The term information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

**Integrity -** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Low Sensitivity Information -** Information that is not classified as National Security Information having a low impact rating for the confidentiality or integrity of security objectives. Information suitable for public release or information that has already been made publicly available is also included in this category.

**Moderate Sensitivity Information -** Information not classified as National Security Information having a moderate impact rating for the confidentiality or integrity of security objectives. Designation of information as Moderate Sensitivity Information does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA for information designated as Moderate Sensitivity Information will be reviewed and processed in the same manner as other Freedom of Information (FOI) requests.

**National Security Information -** Information that has been determined pursuant to Executive Order (E.O.) 12958 as amended by E.O. 13292, or any predecessor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked (Secret, Top Secret, etc.) to indicate its classified status when in documentary form. National Security Information is synonymous with Classified Information.

**Personal Information -** Personal information is information about an identifiable individual that may include but not be limited to: race, national or ethnic origin, religion, age, marital or family status, education, medical, psychiatric, psychological, criminal, financial, or employment history, any identification number, symbol or other particular assigned to an individual, name, address, telephone number, fingerprints, blood type or DNA.

**Personally Identifiable Information -** Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

**Privacy Act Statements -** When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

**Privacy Impact Assessment -** PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Restricted Personally Identifiable Information (RPII) -** Restricted PII is information the unauthorized disclosure of which could create a substantial risk of identity theft (i.e., social security number, bank account number, or combination of two or more items of personally identifiable information, etc.).

**Security Categorization** - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets or individuals.

**System of Records Notice (SORN)** - Public notice of the existence and character of a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

**TVA Information System** - A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.