



Memorandum from the Office of the Inspector General

November 7, 2024

Tammy W. Wilson

REQUEST FOR MANAGEMENT DECISION – AUDIT 2024-17478 – TVA’S PRIVACY PROGRAM

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions or wish to discuss our findings, please contact Weston J. Shepherd, Senior Auditor, at (865) 633-7386 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

WJS:KDS

Attachment

cc (Attachment):

TVA Board of Directors
Brett A. Atkins
Janda E. Brown
Kenneth C. Carnes II
Sherri R. Collins
Buddy Eller
David B. Fountain
Melissa A. Livesey
Jeffrey J. Lyash

Chris A. Marsalis
Jill M. Matthews
Todd E. McCarter
Jeannette Mills
Dustin C. Pate
John M. Thomas III
Josh Thomas
Ben R. Wagner
OIG File No. 2024-17478



Office of the Inspector General

Audit Report

To the Vice President and
Chief Information and Digital
Officer, Technology and
Innovation

TVA'S PRIVACY PROGRAM

Audit Team
Weston J. Shepherd
Jonathan S. Gibson

Audit 2024-17478
November 7, 2024

ABBREVIATIONS

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RPII	Restricted Personally Identifiable Information
SPP	Standard Programs and Processes
SORN	System of Records Notices
T&I	Technology and Innovation
TVA	Tennessee Valley Authority
VP	Vice President

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

BACKGROUND..... 1

OBJECTIVE, SCOPE, AND METHODOLOGY 2

FINDINGS AND RECOMMENDATIONS 4

DISCREPANCIES BETWEEN TVA PRIVACY SYSTEM INVENTORY AND
THE PRIVACY IMPACT ASSESSMENT INVENTORY 4

PRIVACY IMPACT ASSESSMENTS DID NOT FOLLOW TVA POLICY 5

PRIVACY CONTINUOUS MONITORING PROGRAM WAS OUTDATED..... 5

HARD COPY RESTRICTED PERSONALLY IDENTIFIABLE INFORMATION
AND A RESTRICTED AREA WERE NOT SECURED..... 6

PRIVACY IMPACT ASSESSMENT TEMPLATE DID NOT CONTAIN ALL
REQUIRED INFORMATION 7

PRIVACY POLICIES WERE NOT CONSISTENT WITH APPLICABLE LEGAL
GUIDANCE 7

APPENDIX

MEMORANDUM DATED OCTOBER 31, 2024, FROM TAMMY WILSON TO
DAVID P. WHEELER



Audit 2024-17478 – TVA’s Privacy Program

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Consolidated Appropriations Act, 2005, establishes requirements for federal agencies related to privacy. The Tennessee Valley Authority’s (TVA) privacy program includes guidelines for the proper collection, use, protection, disclosure, and disposal of personally identifiable information (PII). The program implements fundamental Federal privacy requirements found in the Privacy Act of 1974, the E-Government Act of 2002, and numerous Office of Management and Budget memoranda, which include completing privacy impact assessments (PIA),ⁱ privacy threshold analyses,ⁱⁱ and system of records notices.ⁱⁱⁱ In addition, the program establishes best practices and procedures designed to protect the personal privacy of TVA employees and other individuals about whom TVA maintains personal information. The senior privacy program manager is responsible for the day-to-day management of TVA’s privacy program.

The Consolidated Appropriations Act, 2008, requires Inspectors General to conduct periodic reviews of the agency’s implementation of these requirements. Our audit objective was to determine if TVA had designed and implemented privacy requirements in accordance with the Consolidated Appropriations Act, 2005. This is our seventh audit of TVA’s privacy program since 2007.

What the OIG Found

We determined TVA had privacy policies in alignment with the Consolidated Appropriations Act, 2005. In addition, TVA had implemented requirements from the Consolidated Appropriations Act, 2005, such as sustaining privacy protection, assuring compliance with fair information practices, proposals, congressional reporting, protecting PII, training, compliance with policies, and recording.

However, we identified six issues that should be addressed by TVA management to further comply with the requirements of the Consolidated Appropriations Act, 2005, and TVA policy.

ⁱ PIAs are conducted to identify privacy risks for systems and includes documentation on the type of PII collected, number of people affected, controls to protect PII, and privacy notices.

ⁱⁱ Privacy threshold analyses are conducted to determine the need for a full PIA and document the type of information that is used by a system.

ⁱⁱⁱ System of record notices are notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system.



Audit 2024-17478 – TVA’s Privacy Program

EXECUTIVE SUMMARY

Specifically, we identified:

1. Discrepancies between TVA privacy system inventory and the PIA inventory.
2. PIAs did not follow TVA policy.
3. The privacy continuous monitoring program was outdated.
4. Hard copy restricted personally identifiable information (RPII)^{iv} and a restricted area were not secured.
5. The PIA template did not contain all required information.
6. Privacy policies were not consistent with applicable legal guidance.

Prior to completion of our audit, TVA management took action to address and remediate three of the six findings listed above.

What the OIG Recommends

We made recommendations to TVA management for the three findings that were not addressed during the audit.

TVA Management’s Comments

In response to our draft report, TVA management agreed with our recommendations. See the Appendix for TVA management’s complete response.

^{iv} TVA has designated some PII that is more sensitive as RPII and defines RPII as information the unauthorized disclosure of could create a substantial risk of identity theft (e.g., social security number, bank account number, and certain combinations of PII).

BACKGROUND

The Consolidated Appropriations Act, 2005, establishes requirements for federal agencies to have a Chief Privacy Officer to assume the following responsibilities.

- Sustaining privacy protections
- Assuring technologies allow for continuous auditing
- Assuring compliance with fair information practices
- Evaluating legislative and regulatory proposals
- Conducting privacy impact assessments (PIA)¹
- Preparing congressional reports
- Ensuring personally identifiable information (PII) is protected
- Training employees on privacy policies
- Ensuring compliance with privacy policies

Additionally, the Consolidated Appropriations Act, 2005, requires federal agencies to (1) establish and implement procedures for information in identifiable form that is consistent with legal guidance and (2) record its use of PII with the Inspector General of the agency.

The Tennessee Valley Authority's (TVA) privacy program includes guidelines for the proper collection, use, protection, disclosure, and disposal of PII. The program implements fundamental Federal privacy requirements found in the Privacy Act of 1974, the E-Government Act of 2002, and numerous Office of Management and Budget memoranda, which include completing PIAs, privacy threshold analyses,² and System of Records Notices (SORN).³ In addition, the program establishes best practices and procedures designed to protect the personal privacy of TVA employees and other individuals about whom TVA maintains personal information. The senior privacy program manager is responsible for the day-to-day management of TVA's privacy program.

The Consolidated Appropriations Act, 2008, requires Inspectors General to conduct periodic reviews of the agency's implementation of these requirements. This is our seventh audit of TVA's privacy program since 2007.

In March 2024, we issued a management alert in which we identified nonpublic critical and sensitive information, including restricted personally identifiable

¹ PIAs are conducted to identify privacy risks for systems and includes documentation on the type of PII collected, number of people affected, controls to protect PII, and privacy notices.

² Privacy threshold analyses are conducted to determine the need for a full PIA and document the type of information that is used by a system.

³ SORNs are notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system.

information (RPII),⁴ that was accessible on TVA's SharePoint® by all TVA users. As a result of our alert, we initiated an audit of the management of access to nonpublic information in TVA's SharePoint®.⁵

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if TVA has designed and implemented privacy requirements in accordance with the Consolidated Appropriations Act, 2005. Our scope was limited to TVA's privacy program responsibilities as defined in the Consolidated Appropriations Act, 2005. To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes (SPP) and Work Instructions, including:
 - TVA-SPP-12.501, *TVA Privacy Program*.
 - TVA-SPP-12.002, *TVA Information Management Policy*.
 - TVA-SPP-12.005, *Enterprise Cybersecurity Monitoring Program*.
 - TVA-SPP-12.001, *Acceptable Use of Information Resources*.
 - TVA-SPP-12.006, *Cyber Incident Response*.
 - TVA-SPP-12.008, *Cybersecurity Policy*.
 - TVA-SPP-12.017, *Security Awareness and Training*.
 - TVA-SPP-12.800, *Risk Management Framework*.
 - TVA-SPP-12.025, *External Website and Web Services Security*.
 - TVA-SPP-31.001, *Records Management*.
 - TVA-SPP-26.09, *Website Development*.
 - TVA-SPP-12.009, *Cybersecurity Risk Management Program*.
 - Information Technology Work Instruction 12.08.06.001, *Privacy Act System of Records Notices*.
- Met with TVA's senior privacy program manager to obtain an understanding of policies, processes, and controls that have been designed and implemented to accomplish the requirements as defined in the Consolidated Appropriations Act, 2005.
- Performed a gap analysis of TVA's defined Privacy Officer Responsibilities against the responsibilities defined in the Consolidated Appropriations Act, 2005.
- Reviewed the design of TVA's policies and procedures to determine if they were in compliance with the Consolidated Appropriations Act, 2005.

⁴ TVA has designated some PII that is more sensitive as RPII and defines RPII as information the unauthorized disclosure of which could create a substantial risk of identity theft (e.g., social security number, bank account number, and certain combinations of personally identifiable information).

⁵ Audit Report 2024-17492, *SharePoint® Access Management*, August 7, 2024

- Performed a gap analysis of TVA's policies and procedures against applicable legal and regulatory guidance.
- Reviewed the following to determine if they were in compliance with the Consolidated Appropriations Act, 2005, and TVA policies:
 - TVA's privacy continuous monitoring strategy
 - TVA's published SORNs
 - TVA's Privacy Officer involvement in legislative and regulatory proposals.
 - TVA's congressional reporting related to privacy.
 - TVA's privacy training content and completion records
 - TVA's implementation of its Privacy Breach Response Plan.
 - TVA's online privacy policies.
 - TVA's recording of its use of PII with the Inspector General.
- Selected a statistical sample 28 of 61 PIAs (with a 90 percent confidence level with a 5 percent error rate) to determine if they were completed in accordance with the Consolidated Appropriations Act, 2005, and TVA-SPP-12.501. Since this was a statistical sample, the results can be projected to the population.
- Performed after-hours walk-throughs of the Knoxville and Chattanooga office complexes to determine if hard copy RPII documents were secured in accordance with TVA policy.
- Identified and assessed internal controls to the extent necessary to address the audit objective, including:
 - Reviewed design and implementation of TVA's privacy program, training, PIAs, policies and procedures, and privacy control monitoring.
 - Reviewed design, implementation, and effectiveness of TVA's PII system inventory.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS AND RECOMMENDATIONS

We determined TVA had privacy policies in alignment with the Consolidated Appropriations Act, 2005. In addition, TVA had implemented requirements from the Consolidated Appropriations Act, 2005, such as sustaining privacy protection, assuring compliance with fair information practices, proposals, congressional reporting, protecting PII, training, compliance with policies, and recording.

However, we identified six issues that should be addressed by TVA management to further comply with the requirements of the Consolidated Appropriations Act, 2005, and TVA policy. Specifically, we found:

1. Discrepancies between TVA privacy system inventory and the PIA inventory.
2. PIAs did not follow TVA policy.
3. The privacy continuous monitoring program was outdated.
4. Hard copy RPII and a restricted area were not secured.
5. The PIA template did not contain all required information.
6. Privacy policies were not consistent with applicable legal guidance.

We discussed our findings with TVA management on August 15, 2024. Prior to completion of our audit, TVA management took action to address and remediate three of the six findings listed above.

DISCREPANCIES BETWEEN TVA PRIVACY SYSTEM INVENTORY AND THE PRIVACY IMPACT ASSESSMENT INVENTORY

We reviewed TVA's privacy system inventory and PIA inventory and identified 23 discrepancies. In addition, we noted multiple systems were incorrectly categorized in the privacy system inventory. As a result, we were initially unable to rely on the inventories. Inaccurate inventories could increase the risk of unprotected PII.

We discussed our finding with TVA management on August 15, 2024, and confirmed inventories were inaccurate. As a result, TVA took action to reconcile and update the privacy system inventory and PIA inventory. We performed additional reconciliations and confirmed the inventories were accurate.

PRIVACY IMPACT ASSESSMENTS DID NOT FOLLOW TVA POLICY

Using the privacy system inventory and PIA inventory TVA reconciled during the audit, we reviewed a sample of PIAs for completion and required elements from the Consolidated Appropriations Act, 2005, and TVA policy. We determined TVA was not following TVA-SPP-12.501, *TVA Privacy Program*, related to (1) reviewing and updating PIAs and (2) publishing PIAs on its website.

TVA policies establish requirements that PIAs are reviewed and updated when making significant changes to existing systems. Although not required by legal guidance, TVA-SPP-12.501, *TVA Privacy Program*, further requires PIAs be reviewed and updated every three years. Our review of the sampled PIAs noted 10 of 28 (36 percent) were not updated in the last three years. Reviewing PIAs help ensure privacy risks and system documentation regarding PII usage are identified and tracked.

In addition, TVA-SPP-12.501 requires systems that collect, maintain, use and/or disseminate information for members of the public to be published to the TVA privacy website. Our review of the sampled PIAs noted 8 of 28 (29 percent) were not published on the TVA privacy website. Publishing PIAs to the public website helps notify the public of PII collection, maintenance, usage, and/or dissemination.

Recommendation – We recommend the Vice President (VP) and Chief Information and Digital Officer, Technology and Innovation (T&I):

1. Review and update PIAs in accordance with requirements outlined in TVA-SPP-12.501 or review SPP requirements to determine appropriate cadence to review and update PIAs.
2. Review PIAs to identify systems that collect, maintain, use and/or disseminate information for members of the public, and publish them to the website in accordance with TVA policy.

TVA Management's Comments – In response to our draft report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

PRIVACY CONTINUOUS MONITORING PROGRAM WAS OUTDATED

The Consolidated Appropriations Act, 2005, requires “technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices.” TVA had a privacy continuous monitoring program in place that had not been

updated since the last audit.⁶ However, during our current audit, the program underwent significant changes and we were unable to test the effectiveness of TVA's privacy continuous monitoring program due to timing of implementation. Privacy continuous monitoring helps maintain awareness of privacy risks, assess privacy controls, and ensure compliance with privacy requirements.

Recommendation – We recommend the VP and Chief Information and Digital Officer, T&I:

3. Verify completion of continuous monitoring of privacy controls in accordance with the privacy continuous monitoring program.

TVA Management's Comments – In response to our draft report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

HARD COPY RESTRICTED PERSONALLY IDENTIFIABLE INFORMATION AND A RESTRICTED AREA WERE NOT SECURED

TVA-SPP-12.002, *TVA Information Management Policy*, states "RPII shall be properly secured at all times when not in use and/or under the control of a person with a need-to-know to limit the potential for unauthorized disclosure." We performed walkthroughs of TVA's Knoxville and Chattanooga office complexes to identify unsecured hard copy records containing RPII on individuals' desks, in unlocked filing cabinets, and on or around printers. During our walkthroughs, we found 46 instances of unsecured documents that contained RPII.

We also found a badge reader for a restricted area was allowing inappropriate physical access to all TVA employees. Prior to the completion of our audit, TVA management took action to address the inappropriate physical access. Ineffective physical controls for hard copy RPII increases TVA's risk of unauthorized disclosure, which could create a substantial risk of identity theft.

Recommendation – We recommend the VP and Chief Information and Digital Officer, T&I:

4. Take steps to ensure hard copy RPII is appropriately protected.

TVA Management's Comments – In response to our draft report, TVA management agreed with our recommendations. See the Appendix for TVA management's complete response.

⁶ Audit Report 2021-15779, *TVA's Privacy Program*, September 20, 2021.

PRIVACY IMPACT ASSESSMENT TEMPLATE DID NOT CONTAIN ALL REQUIRED INFORMATION

The Consolidated Appropriations Act, 2005, requires TVA's Privacy Officer conduct a PIA of proposed rules on the privacy of information in an identifiable form, including the type of PII collected and the number of people affected. We reviewed TVA's template used for completing PIAs and determined it did not include the number of people affected. We discussed our finding with TVA management on August 15, 2024, and, as a result, TVA took action to update the template to include the number of people affected. We reviewed the updated template and confirmed changes were implemented.

PRIVACY POLICIES WERE NOT CONSISTENT WITH APPLICABLE LEGAL GUIDANCE

The Consolidated Appropriations Act, 2005, requires agencies "establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public" that are consistent with legal guidance. We performed a gap analysis of TVA SPPs, work instructions, and other policy documents against applicable criteria. A majority of the criteria requirements were satisfied. However, we identified 3 out of 277 requirements were not reflected by current TVA policy documentation. The subject areas of the identified gaps included TVA's online privacy policy and Privacy Act requests. We discussed our finding with TVA management on August 15, 2024, and, as a result, TVA took action to update policy documentation to address the identified gaps. We reviewed the updated policies and confirmed changes were implemented.

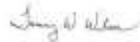
October 31, 2024

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2024-17478 – TVA's PRIVACY PROGRAM

Our response to your request for comments regarding the subject report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Weston Shepard, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.



Tammy Wilson
Vice President and Chief Information & Digital Officer
Technology and Innovation

KCC: BAA
cc (Attachment): Response to Request

Kenneth C. Carnes
Dustin C. Pate
Brett A. Atkins
Sherri R. Collins
Joshua Linville
Jessica A. Anthony
Stephen K. Avans
Julie S. Farr
Faisal Bhatti
Bradley E. Bennett

David B. Fountain
Gregory G. Jackson
Melissa A. Livesey
Todd E. McCarter
Christopher A. Marsalis
Jeannette Mills
Melissa R. Crane
Courtney L. Stetzler
Kacy K Kirtley
OIG File No. 2024-17478

Audit 2024-17478 – TVA's Privacy Program
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

	Recommendation	Comments
1	We recommend the Vice President and Chief Information & Digital Officer, T&I. Review and update PIAs in accordance with requirements outlined in TVA-SPP-12.501 or review SPP requirements to determine appropriate cadence to review and update PIAs.	Management agrees.
2	Review PIAs to identify systems that collect, maintain, use and/or disseminate information for the public, and publish them to the website in accordance with TVA policy.	Management agrees.
3	Verify completion of continuous monitoring of privacy controls in accordance with the privacy continuous monitoring program.	Management agrees.
4	Take steps to ensure hard copy RPII is appropriately protected.	Management agrees.