Memorandum from the Office of the Inspector General

September 20, 2021

Jeremy P. Fisher

REQUEST FOR MANAGEMENT DECISION – AUDIT 2021-15779 – 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.

Curtis C Hudson

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

WJS:KDS
Attachment
cc (Attachment):
TVA Board of Directors
Andrea S. Brackett
Buddy Eller
David B. Fountain
Gregory G. Jackson
Jeffrey J. Lyash
Christopher A. Marsalis
Jill M. Matthews
Todd E. McCarter
Lindsey M. Stewart
John M. Thomas III
OIG File No. 2021-15779

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 B. Anderson
Brandon P. Roberts

Audit 2021-15779
September 20, 2021

ABBREVIATIONS

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

TABLE OF CONTENTS

APPENDICES

Audit 2021-15779 – TVA's Privacy Program

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Consolidated Appropriations Act of 2008 requires Inspectors General to conduct periodic reviews of an agency's privacy program. 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. 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. This is our sixth audit of TVA's privacy program. We previously issued reports on our audits of TVA's privacy program in 2007, 2010, 2012, 2015, and 2018.[1]

Our audit objectives were to determine if the privacy program is effective and in compliance with applicable federal regulations, federal guidance, and TVA policies.

What the OIG Found

We found several areas of the privacy program to be generally effective, including (1) completion of privacy impact assessments, (2) privacy-related training taken by network users, (3) privacy considerations during the authority to operate process, (4) system categorization, (5) privacy incident response, (6) privacy-related contract terms and conditions, and (7) desktop and laptop sanitization. However, we identified seven issues that should be addressed by TVA management to further increase the effectiveness of the privacy program. Specifically, we found:

1. Unsecured electronic restricted personally identifiable information (RPII)[2] on SharePoint and shared network drives.

---

[1] Prior audits of TVA's privacy program:

- Audit Report 2007-008T, *Privacy Protection – TVA Use of Information in Identifiable Form*, July 31, 2007.
- Audit Report 2009-12650, *Use and Protection of Personally Identifiable Information*, May 19, 2010.
- Audit Report 2012-14425, *TVA Protection of Private Information*, September 24, 2012.
- Audit Report 2014-15060, *Use and Protection of Personally Identifiable Information*, February 19, 2015.
- Audit Report 2017-15453, *TVA's Privacy Program,* June 13, 2018.

[2] 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).

2. Unsecured hard copy RPII.

3. No end user notifications for e-mail security violations.

4. No technical controls for removable media.

5. We could not confirm that all desktops and laptops utilize encryption.

6. Privacy Act notices on TVA forms did not include all required elements.

7. Not all external Web sites included privacy policies. (Note: Prior to completion of our audit, TVA Technology and Innovation took action to address the external Web sites that were missing required privacy policies.)

We also found gaps between TVA's policies and procedures and applicable federal privacy regulations and guidance.

What the OIG Recommends

We recommend the Vice President and Chief Information and Digital Officer, Technology and Innovation:

1. Implement a process to ensure appropriate access controls are in place to protect RPII on SharePoint and shared network drives.

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

3. Evaluate implementing controls for possible e-mail security violations.

4. Evaluate implementing technical controls for removable media.

5. Conduct a review to verify that RPII on Windows desktops and laptops is encrypted to TVA's encryption standards.

6. Update Privacy Act notices on TVA forms used to collect PII in accordance with TVA policy.

7. Review the privacy requirement gaps identified and determine the policies that should be updated based on risk.

EXECUTIVE SUMMARY

TVA Management's Comments

In response to our draft audit report, TVA management agreed with our recommendations. See Appendix B for TVA management's complete response.

BACKGROUND

The Consolidated Appropriations Act of 2008 requires Inspectors General to conduct periodic reviews of an agency's privacy program. 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. 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. This is our sixth audit of TVA's privacy program. We previously issued reports on our audits of TVA's privacy program in 2007, 2010, 2012, 2015, and 2018.[3]

OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objectives were to determine if the privacy program is effective and in compliance with applicable federal regulations, federal guidance, and TVA policies. Our scope was TVA's privacy program and actual practices for the use and protection of PII. A complete discussion of our objectives, scope, and methodology is included in the Appendix.

FINDINGS AND RECOMMENDATIONS

We found several areas of the privacy program to be generally effective, including (1) completion of privacy impact assessments, (2) privacy-related training taken by network users, (3) privacy considerations during the authority to operate (ATO) process, (4) system categorization, (5) privacy incident response, (6) privacy-related contract terms and conditions, and (7) desktop and laptop sanitization. However, we identified seven issues that should be addressed by TVA management to further increase the effectiveness of the privacy program. We also found gaps between TVA's policies and procedures and applicable federal privacy regulations and guidance.

[3] Prior audits of TVA's privacy program:

- Audit Report 2007-008T, *Privacy Protection – TVA Use of Information in Identifiable Form*, July 31, 2007.
- Audit Report 2009-12650, *Use and Protection of Personally Identifiable Information*, May 19, 2010.
- Audit Report 2012-14425, *TVA Protection of Private Information*, September 24, 2012.
- Audit Report 2014-15060, *Use and Protection of Personally Identifiable Information*, February 19, 2015.
- Audit Report 2017-15453, *TVA's Privacy Program,* June 13, 2018.

ISSUES TO BE ADDRESSED TO INCREASE THE EFFECTIVENESS OF THE PRIVACY PROGRAM

We identified seven issues that should be addressed by TVA management to further increase the effectiveness of the privacy program. Specifically, we found:

1. Unsecured electronic restricted personally identifiable information (RPII)[4] on SharePoint and shared network drives.

2. Unsecured hard copy RPII.

3. No end user notifications for e-mail security violations.

4. No technical controls for removable media.

5. We could not confirm that all desktops and laptops utilize encryption.

6. Privacy Act notices on TVA forms did not include all required elements.

7. Not all external Web sites included privacy policies.

Unsecured Electronic RPII
TVA Standard Programs and Processes (SPP) 12.002, *TVA Information Management Policy,* requires RPII be stored in application databases with proper access controls. We searched SharePoint and identified five documents that contained unsecured RPII.

Additionally, TVA-SPP-12.002, *TVA Information Management Policy,* requires RPII on shared drives to be "restricted to those with a need-to-know by permission, settings, or passwords." We scanned five shared drives accessible by all domain users and identified unsecured RPII on one shared drive.

Ineffective technical controls for restricting access to TVA RPII increases the risk of unauthorized disclosure, which could create a substantial risk of identity theft.

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

1. Implement a process to ensure appropriate access controls are in place to protect RPII on SharePoint and shared network drives.

   TVA Management's Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

[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).

Unsecured Hard Copy RPII
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 after-hours walkthroughs of the Knoxville office complex 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 17 documents that contained RPII. 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:

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

   TVA Management's Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

No End User Notifications for E-mail Security Violations
TVA-SPP-12.002, *TVA Information Management Policy,* explains that if a possible e-mail security violation is detected, such as sending unsecured TVA RPII, the user will receive an automated e-mail message to notify the user of the possible violation and instructions for securing RPII. However, according to TVA personnel, there were no notifications for these violations. If working as designed, the end user notifications could inform users how to properly secure RPII in e-mails.

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

3. Evaluate implementing controls for possible e-mail security violations.

   TVA Management's Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

No Technical Controls for Removable Media
TVA-SPP-12.002, *TVA Information Management Policy,* states, "RPII stored . . . on removable media and portable systems and devices must be encrypted to TVA's encryption standards." According to TVA personnel, TVA has no technical controls to prevent TVA RPII being stored on unencrypted removable media, such as flash drives. Ineffective technical controls for TVA RPII on removable media increases the 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. Evaluate implementing technical controls for removable media.

   TVA Management's Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

Desktop and Laptop Encryption

TVA-SPP-12.002, *TVA Information Management Policy,* states, "RPII stored . . . on removable media and portable systems and devices must be encrypted to TVA's encryption standards." However, we identified a discrepancy between TVA's system of record for Windows laptop and desktop inventory and TVA's encryption manager. Therefore, we could not confirm that desktops and laptops utilize encryption in accordance with TVA policy. Inventory discrepancies for TVA desktops and laptops increases the risk of unauthorized RPII disclosure, which could create a substantial risk of identity theft.

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

5. Conduct a review to verify that RPII on Windows desktops and laptops is encrypted to TVA's encryption standards.

   TVA Management's Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

Privacy Act Notices on TVA Forms Did Not Include All Required Elements

TVA-SPP-12.501, *TVA Privacy Program*, requires that the name and location of the System of Records Notice (SORN)[5] be included in a Privacy Act notice on forms used to collect PII. We reviewed TVA forms used to collect PII and found 42 out of 45 TVA forms did not include the name and location of the SORN as required by TVA policy. This could result in noncompliance with federal requirements.

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

6. Update Privacy Act notices on TVA forms used to collect PII in accordance with TVA policy.

   TVA Management Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

[5] 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.

Not All External Web Sites Included Privacy Policies

TVA-SPP-12.501, *TVA Privacy Program*, requires the implementation of Federal online privacy requirements, which includes privacy policies on external Web sites. We reviewed external TVA Web sites and determined two Web sites did not have a privacy policy. Prior to completion of our audit, TVA T&I took action to address the external Web sites that were missing required privacy policies. We confirmed that the Web sites are no longer publicly accessible.

TVA'S PRIVACY POLICIES NOT CONSISTENT WITH APPLICABLE FEDERAL REGULATIONS AND GUIDANCE

We performed a gap analysis of TVA SPPs, work instructions, and other policy documents against applicable federal regulations and federal guidance. A majority of the criteria requirements were satisfied. However, we identified 8 out of 278 requirements were not reflected by current TVA policy documentation. The subject areas of identified gaps include (1) Privacy Act implementation rules, (2) privacy policies on agency Web sites, (3) agency use of third-party Web sites and applications, and (4) web measurement and customization technologies. Lack of documentation of privacy requirements could result in noncompliance with federal requirements.

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

7. Review the privacy requirement gaps identified and determine the policies that should be updated based on risk.

   TVA Management's Comments – TVA management agreed with the recommendation. See Appendix B for TVA management's complete response.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objectives were to determine if the Tennessee Valley Authority's (TVA) privacy program is effective and in compliance with applicable federal regulation, federal guidance, and TVA policies. Our scope was TVA's privacy program and actual practices for the use and protection of personally identifiable information (PII). To achieve our audit objectives, 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.*
  - Information Technology Work Instruction 12.08.06.001, *Privacy Act System of Records Notices.*
- Discussed the privacy program and requirements in detail with TVA's senior privacy program manager to obtain an understanding of the program.
- Judgmentally selected 3 out of 50 TVA systems that contain restricted personally identifiable information (RPII) data. The three systems were selected based on risk and auditor knowledge of RPII data types contained in the systems. For the three sample systems, we reviewed (1) privacy impact assessments (PIAs) to determine if the PIAs included all required elements, (2) approvals required for systems that contain social security numbers, and (3) encryption of the data. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Compared listing of PIAs to TVA's inventory of systems that contain RPII to determine if PIAs were completed for all systems that contain RPII.
- Reviewed TVA's privacy Web site to determine if PIAs were listed in accordance with TVA-SPP-12.501, *TVA Privacy Program.*
- Reviewed annual cyber security awareness training to determine if privacy requirements were included and was completed in accordance with timing requirements in TVA policies.
- Reviewed training for individuals in essential roles related to privacy to determine if training was completed in accordance with TVA-SPP-12.501, *TVA Privacy Program.*
- Reviewed training documents to determine compliance with TVA's Privacy Breach Response Plan.

- Judgmentally selected 3 out of 59 authority to operate (ATO) documents. The three ATO documents selected were for TVA systems categorized as containing PII or RPII. We reviewed the three ATOs to determine (1) if PIAs were incorporated in ATOs, (2) if PIAs were reviewed in conjunction with ATO updates, and (3) accuracy of system categorization. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Reviewed system security and privacy plans to determine if privacy controls were incorporated.
- Reviewed privacy incidents to determine if the incidents were handled in accordance with TVA's Privacy Breach Response Plan.
- Judgmentally selected 7 out of 6,117 contracts. The seven contracts that we selected were based on risk of vendors that hold, store, or process TVA PII data. We reviewed the contracts' terms and conditions to determine if the contracts included required terms and conditions related to TVA PII data. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Compared inventories of retired desktops and laptops to inventory of retirement tickets to determine if desktops and laptops were sanitized appropriately.
- Conducted searches in SharePoint to identify unsecured RPII.
- Judgmentally selected five shared network drives out of a total of 109 shared network drives. The five drives selected were selected because they were accessible by all domain users. We reviewed each server to determine if any contained unsecured RPII. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Performed after-hours walk-throughs of the Knoxville office complex to determine if hard copy RPII documents were being appropriately secured.
- Conducted walk-through of e-mail alerting capabilities to determine if alerting controls in place were in accordance with TVA-SPP-12.002, *TVA Information Management Policy.*
- Reviewed e-mail options to determine if message encryption was available to end users.
- Compared TVA's system of record for laptop and desktop inventory and inventory for TVA's encryption manager to determine if all desktops and laptops were encrypted.
- Reviewed TVA forms used to collect PII to determine if the forms included all required elements.
- Reviewed TVA public-facing Web sites to determine if privacy policies were incorporated in accordance with TVA-SPP-12.501, *TVA Privacy Program.*
- Obtained and reviewed applicable federal privacy regulations and guidance.

- Compared applicable federal privacy regulations and guidance to TVA's policies and procedures.
- Obtained an understanding of information system controls associated with TVA's privacy program, such as inventory of systems that contain RPII, encryption, annual cybersecurity and privacy training, and data monitoring. We identified these controls as significant to the audit objective and included them in our audit testing.

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.

September 17, 2021

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2021 – 15779 TVA'S PRIVACY PROGRAM

Our response to your request for comments regarding the subject draft 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 Josh Thomas.

Jeremy Fisher
Vice President and Chief Information Officer
Technology and Innovation
SP 3A-C

ASB:BAB JRT
cc (Attachment): Response to Request
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
David Harrison, MP 5C-C
Gregory Jackson
Benjamin Jones, SP 3L-C
Todd McCarter, MP 2C-C
John Thomas, MR 6D-C
Joshua Thomas
OIG File No. 2021-15779

Audit 2021-15779
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 and Digital Officer, T&I: Implement a process to ensure appropriate access controls are in place to protect RPII on SharePoint and shared network drives.	Management agrees
2	Take steps to ensure hard copy RPII is appropriately protected.	Management agrees
3	Evaluate implementing controls for possible E-mail security violations.	Management agrees
4	Evaluate implementing technical controls for removable media.	Management agrees
5	Conduct a review to verify that RPII on Windows desktops and Laptops is encrypted to TVA's encryption standards.	Management agrees
6	Update Privacy Act notices on TVA forms used to collect PII in accordance with TVA policy.	Management agrees
7	Review the privacy requirement gaps identified and determine the policies that should be updated based on risk.	Management agrees