



Memorandum from the Office of the Inspector General

June 13, 2018

Philip D. Propes, MP 2C-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2017-15453 – 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.

If you have any questions or wish to discuss our findings, please contact Michael P. Anderson, Senior Auditor, at (865) 633-7393 or Sarah E. Huffman, Director (Acting), 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)
WT 2C-K

MPA:BSC

Attachment

cc (Attachment):

TVA Board of Directors
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Christopher A. Marsalis, WT 5D-K
Jill M. Matthews, WT 2C-K
John M. Thomas III, MR 6D-C
OIG File No. 2017-15453



Office of the Inspector General

Audit Report

To the Director, TVA
Cybersecurity

TVA'S PRIVACY PROGRAM

Audit Team

Michael P. Anderson
Melissa L. Conforti
Frank B. Lord II

Michael R. Newport
Weston J. Shepherd
Megan Spitzer

Audit 2017-15453
June 13, 2018

ABBREVIATIONS

GFP	General File and Print
HPAM	Hewlett Packard Asset Manager
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RPII	Restricted Personally Identifiable Information
SPP	Standard Programs and Processes
TVA	Tennessee Valley Authority
WI	Work Instruction

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

BACKGROUND..... 1

OBJECTIVES, SCOPE, AND METHODOLOGY 1

FINDINGS 1

 ISSUES TO BE ADDRESSED TO INCREASE THE EFFECTIVENESS
 OF THE PRIVACY PROGRAM..... 2

 TVA'S PRIVACY POLICIES NOT CONSISTENT WITH APPLICABLE
 FEDERAL REGULATIONS AND GUIDANCE..... 5

RECOMMENDATIONS 5

APPENDICES

- A. OBJECTIVES, SCOPE, AND METHODOLOGY
- B. MEMORANDUM DATED MAY 30, 2018, FROM PHILIP D. PROPES TO
 DAVID P. WHEELER



Audit 2017-15453 – TVA’s Privacy Program

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Consolidated Appropriations Act of 2008 requires Inspectors General 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 fifth review of TVA's privacy program. We previously conducted audits of TVA's privacy program in 2007, 2009, 2012, and 2014.ⁱ

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

What the OIG Found

We found areas of the privacy program to be generally effective, including (1) controls protecting privacy information on TVA-owned mobile devices, (2) privacy training taken by network users, (3) regular reviews of the privacy program by TVA management, (4) encryption controls protecting data in privacy systems, and (5) appropriate use and protection of reports in privacy systems. However, we identified several issues that should be addressed to further increase the effectiveness of the privacy program. Specifically, we found:

1. Two unencrypted laptops that were lost or stolen during our audit period were noted as containing sensitive data including PII.
2. Unsecured hard copy restricted personally identifiable information (RPII).ⁱⁱ

ⁱ 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.

ⁱⁱ RPII is information the unauthorized disclosure of which could create a substantial risk of identity theft (e.g., social security number, bank account number, certain combinations of PII).



Audit 2017-15453 – TVA’s Privacy Program

EXECUTIVE SUMMARY

3. Unsecured RPII on shared network drives.
4. Inaccurate inventory of privacy systems.
5. An information security officer of one privacy system not having completed the required privacy training.
6. Notifications of new RPII systems were not working as designed.
7. One privacy system had four shared user accounts that were no longer needed. TVA deleted these accounts after we identified them.

We also found gaps between TVA’s policies and procedures governing the privacy program and applicable federal privacy regulations and guidance.

What the OIG Recommends

We recommend the Director, TVA Cybersecurity:

1. Evaluate encrypting all laptops.
2. Take steps to ensure hard copy RPII is appropriately protected.
3. Implement a process to prevent and/or detect unsecured RPII on shared network drives.
4. Review the privacy system inventory on a periodic basis for accuracy and completeness.
5. Review the privacy requirement gaps identified and determine which policies should be updated based on risk.

TVA Management’s Comments

In response to our draft audit report, TVA management stated they provide appropriate training and provided additional information to clarify the training exception. TVA management agreed with our remaining findings and recommendations and provided additional information that they have implemented an inventory review process to ensure the privacy system inventory is accurate. See Appendix B for TVA management’s complete response.



Audit 2017-15453 – TVA’s Privacy Program

EXECUTIVE SUMMARY

Auditor’s Response

We reviewed additional documentation provided by TVA management and determined that the information security officers had completed the required training. Accordingly, we removed our recommendation that TVA management take steps to ensure information security officers of privacy systems are appropriately trained from this report. In addition, we confirmed the privacy system inventory review process had been implemented, and no further action is required by TVA.

BACKGROUND

The Consolidated Appropriations Act of 2008 requires Inspector Generals 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 fifth audit of TVA's privacy program. We previously conducted audits of TVA's privacy program in 2007, 2009, 2012, and 2014.¹

OBJECTIVES, SCOPE, AND METHODOLOGY

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

FINDINGS

We found several areas of the privacy program to be generally effective, including (1) controls protecting privacy information on TVA-owned mobile devices, (2) privacy training taken by network users, (3) regular reviews of the privacy program by TVA management, (4) encryption controls protecting data in privacy systems, and (5) appropriate use and protection of reports in privacy systems. However, we identified several 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 governing the privacy program and applicable federal privacy regulations and guidance. Details of our findings are discussed below.

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.

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

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

1. Two unencrypted laptops that were lost or stolen during our audit period were noted as containing sensitive data including PII.
2. Unsecured hard copy restricted personally identifiable information (RPII).²
3. Unsecured RPII on shared network drives.
4. Inaccurate inventory of privacy systems.
5. An information security officer of one privacy system not having completed the required privacy training.
6. Notifications of new or modified privacy systems not working as designed.
7. One privacy system had four shared user accounts that were no longer needed. These were deleted after being identified in our fieldwork.

Two Unencrypted Laptops With PII Were Lost or Stolen

We obtained a list of privacy incidents from January 1, 2015, to May 31, 2017. From that list of 42 privacy incidents, we noted 2 involved lost or stolen laptops. Both laptops were noted to contain sensitive data including PII data, and neither laptop was encrypted. The tickets noted 1 laptop was later found, and the other was not recovered. Encrypting laptops would significantly reduce the risk of disclosure of sensitive data in cases of a lost or stolen laptop.

Unsecured Hard Copy RPII

TVA-Standard Programs and Processes (SPP)-12.002, *TVA Information Management Policy*, states that "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 conducted after-hours walkthroughs of the 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 49 unsecured documents containing PII and RPII (6 in the Knoxville office complex and 43 in the Chattanooga office complex). The unsecured documents included:

- Performance reviews.

² RPII is 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).

- Equal opportunity and compliance records.
- W-9 forms, including social security numbers.
- Pay grievance documentation.
- Employee timesheets.
- Employment applications and transcripts from schools.
- Contractor check-in information, including social security numbers.

Lack of physical control of hard copy RPII increases TVA's risk of disclosure. Accordingly, the documents should be properly secured.

Unsecured RPII Found on Shared Network Drives

TVA-SPP-12.002, *Information Management Policy*, Appendix G, Section 10 states "always utilize encryption for the storage of RPII in electronic files on IT equipment." TVA utilizes general file and print (GFP) servers for employees to store data on a shared network. However, GFP servers are not encrypted. We were informed that TVA is not currently scanning all GFP servers for unsecured RPII, and the scanning tool being used is unreliable. Based on this information, we scanned a selection of four GFP servers for unsecured agency RPII and found unsecured agency RPII on two of the four GFP servers scanned. A lack of electronic controls for TVA RPII increases TVA's risk of disclosure.

Inaccurate Inventory of Privacy Systems

The National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, requires federal agencies to establish, maintain, and update an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII. Currently within TVA, two inventories are kept for privacy systems. One is kept by Hewlett Packard Asset Manager (HPAM), which is the system of record for TVA. The other is the privacy impact assessment (PIA) list/inventory manually managed by the senior privacy program manager.

We compared the manually managed list to the system of record and found the following discrepancies:

- Four PII systems were found in HPAM that did not exist or correspond to items on the senior privacy program manager's PIA list/inventory.
- Seventeen PII systems in use at TVA that are either not categorized in HPAM or were not listed in HPAM.

Lack of an accurate and complete inventory of privacy systems increases TVA's risk of PII disclosure.

Information Security Officer of One Privacy System Did Not Take the Required Training

As a result of a prior audit,³ TVA implemented additional privacy training for designated information security officers of privacy systems entitled “Protecting Personally Identifiable Information.” We selected five privacy systems from the inventory of all privacy systems for further testing. Two of the five selected privacy systems have information security officers designated.⁴ We reviewed training records for the two information security officers and determined one of the two did not take the required training. Proper training of security officers helps ensure they are aware of their roles and responsibilities in helping to secure privacy systems.

Subsequent to our draft audit report, TVA management provided additional documentation showing the one information security officer did take the required training. We reviewed the documentation and concur that the information security officer did complete the required training.

Notifications of New Systems and Changes to Privacy Systems Not Working as Designed

The senior privacy program manager is notified of a new system or revisions to an existing system through TVA’s change management system by an e-mail that is triggered when the employee inputting the revisions notes it could have a privacy impact. As a result of a recommendation from a prior audit,⁵ TVA management implemented a process in which they keep a manual log of all notifications from the change management system that could affect privacy and whether or not the change required a new or updated privacy threshold analysis or PIA.

We compared a report of RPII related changes from TVA’s change management system from January 1, 2015, to June 17, 2017, with the log kept by the senior privacy program manager and found 32 discrepancies. We determined the discrepancies were due to a failure of the change management system’s e-mail notification feature that should send an e-mail to the senior privacy program manager. TVA management informed us the cause of the system failure was the e-mail feature did not transfer when an upgrade of the change management system occurred.

We were made aware that the e-mail notifications were resolved during fieldwork. We reviewed e-mail evidence and concur that the notification is now working as designed.

³ Audit Report 2009-12650, *Use and Protection of Personally Identifiable Information*, May 19, 2010.

⁴ The remaining three systems either (a) were scheduled to be authorized in fiscal year 2018 or (b) will not be authorized. Therefore, these systems do not have an information security officer designated.

⁵ Audit Report 2014-15060, *Use and Protection of Personally Identifiable Information*, February 19, 2015.

Four Shared User Accounts No Longer Needed

The National Institute of Standards and Technology Special Publication 800-53 IA-2 requires information systems to uniquely identify and authenticate organizational users or processes acting on behalf of organizational users. We reviewed the user listings for five privacy systems to determine if any did not identify unique users (also known as shared accounts). The use of shared accounts introduces risk by limiting individual accountability of actions performed. We found one system that had four shared user accounts that TVA confirmed were no longer needed. Those accounts were deleted after being identified in our fieldwork.

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

We performed a gap analysis of TVA SPPs against applicable privacy requirements required of federal agencies. We found 106 of 259 federal privacy requirements were not reflected by current TVA policy documentation. The specific requirements not reflected by current TVA policy documentation have been shared with TVA management. Lack of documentation of privacy requirements could result in noncompliance with federal requirements.

RECOMMENDATIONS

We recommend the Director, TVA Cybersecurity:

1. Evaluate encrypting all laptops.
2. Take steps to ensure hard copy RPII is appropriately protected.
3. Implement a process to prevent and/or detect unsecured RPII on shared network drives, specifically GFP servers.
4. Review the HPAM privacy system inventory on a periodic basis for accuracy and completeness.
5. Review the privacy requirement gaps identified and determine which policies should be updated based on risk.

TVA Management's Comments – In response to our draft audit report, TVA management stated they provide appropriate training and provided additional information to clarify the training exception. TVA management agreed with our remaining findings and recommendations and provided additional information that they have implemented an inventory review process to ensure the HPAM privacy system inventory is accurate. See Appendix B for TVA management's complete response.

Auditor's Response – We reviewed additional documentation provided by TVA management and determined that the information security officers had completed the required training. Accordingly, we removed our recommendation that TVA management take steps to ensure information security officers of privacy systems are appropriately trained from this report. In addition, we confirmed the HPAM privacy system inventory review process had been implemented, and no further action is required by TVA.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our objectives were to determine if the Tennessee Valley Authority's (TVA) privacy program is effective and in compliance with applicable federal regulations, federal guidance, and TVA policies and procedures. Our audit 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:

- Discussed the privacy program in detail with TVA's senior privacy program manager to obtain an understanding of the program.
- Reviewed applicable TVA Standard Programs and Processes (SPP) and Work Instructions (WI), including:
 - TVA-SPP-12.501, *TVA Privacy Program*.
 - TVA-SPP-12.002, *TVA Information Management Policy*.
 - TVA-SPP-12.001, *Acceptable Use of Information Resources*.
 - TVA-SPP-12.006, *Cyber Incident Response*.
 - TVA-IT-WI-12.08.03.003, *Privacy Impact Assessment*.
 - TVA-IT-WI-12.06.012, *PII Incident Notifications*.
 - TVA-IT-WI-12.08.06.001, *Privacy Act System of Records Notices (SORNs)*.
 - TVA-SPP-11.316, *Employee Discipline*.
- Obtained and reviewed applicable federal privacy regulations and guidance.
- Compared applicable federal privacy regulations and guidance to TVA's privacy program SPPs and WIs.
- Compared a change management system report of changes that affected privacy from January 1, 2015, to June 17, 2017, to a manual log maintained by the senior privacy program manager to determine completeness.
- Obtained and reviewed the two inventories TVA keeps for privacy systems containing restricted personally identifiable information (RPII) to determine the completeness of the information in each system.
- Reviewed four TVA general file and print servers to determine if unsecured RPII was being stored on those servers. We selected one server each from the Knoxville and Chattanooga office complexes and one server each from a fossil plant and nuclear plant.
- Reviewed controls around handling of RPII on mobile devices to determine compliance with TVA-SPP-12.002, *TVA Information Management Policy*.
- Selected 5 TVA systems containing RPII and reviewed (1) training records to determine if security officers are appropriately trained, (2) user listings to determine if shared accounts were being used, (3) sample reports provided by system owners to determine if RPII was being handled appropriately, and (4) encryption (both at rest and in transit) of the data. We selected the 5 systems (from a population of 53 privacy systems) based on criticality and risk to TVA.

- Reviewed annual cyber security awareness training to determine if privacy requirements were included.
- Determined if TVA's privacy program is regularly reviewed by TVA management.
- Performed after-hours walkthroughs of the Knoxville and Chattanooga office complexes to determine if hard copy RPII documents were being appropriately secured.
- Reviewed resolution of privacy incidents from January 1, 2015, to May 31, 2017, to determine adequate steps have been performed to mitigate loss of data.

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.

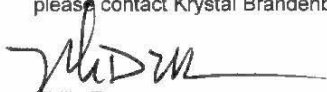
May 30, 2018

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2017-15453 – 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 Michael Anderson, Sarah Huffman, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg.



Philip Propes
Chief Information Security Officer
Information Technology
MP 2C-C

cc (Attachment):

Robert Arnold, MP 2C-C
Andrea Brackett, WT 5D-K
Krystal Brandenburg, MP 3C-C
Robertson Dickens, WT 9C-K
Jeremy Fisher, MR 6D-C
David Johnson, SP 2A-C
Dwain Lanier, MR 6D-C

Melissa Livesey, WT 5B-K
Christopher Marsalis, WT 5D-K
Jill Matthews, ET 4C-K
Philip Propes, MP 3B-C
John Thomas, MR 6D-C
OIG File No. 2017-15453

AUDIT 2017-15453
TVA's Privacy Program
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Recommendation		Comments
1	Evaluate encrypting all laptops.	Management agrees.
2	Take steps to ensure hard copy RPII is appropriately protected.	Management agrees.
3	Implement a process to prevent and/or detect unsecured RPII on shared network drives, specifically GFP servers.	Management agrees.
4	Review the HPAM privacy system inventory on a periodic basis for accuracy and completeness.	Management agrees. TVA reviews the inventory on a weekly basis and has provided additional information to the OIG.
5	Take steps to ensure information security officers of privacy systems are appropriately trained.	Management agrees. TVA provides appropriate training and has provided additional information to the OIG to clarify the training exception.
6	Review the privacy requirement gaps identified and determine which policies should be updated based on risk.	Management agrees.