Memorandum from the Office of the Inspector General

July 31, 2007

E. Wayne Robertson, SP 5A-C

REQUEST FOR FINAL ACTION – AUDIT 2007-008T – PRIVACY PROTECTION – TVA USE OF INFORMATION IN IDENTIFIABLE FORM

Attached is the subject final report for your review and final action. Your written comments, which addressed your management decision and actions planned or taken, have been included in the report. Please notify us when final action is complete.

If you have any questions, please contact Sylvia J. Whitehouse, Senior Auditor, at (865) 632-2640 or Jill M. Matthews, Director, Information Technology Audits, at (865) 632-4730. We appreciate the courtesy and cooperation received from your staff during the audit.

Ben R. Wagner
Deputy Inspector General
ET 3C-K

SJW:SDB
Attachment
cc (Attachment):
Steven A. Anderson, SP 5A-C
R. Clay Eckles, CTR 1P-M
Frank A. Foster, OCP 2C-NST
Nicholas P. Goschy, Jr., WT 6A-K
Tom D. Kilgore, WT 7B-K
John E. Long, Jr., WT 7B-K
Stacie A. Martin, MP 3C-C
Janice W. McAllister, EB 7A-C
Richard W. Moore, ET 4C-K
Mary E. Ragland, EB 5B-C
Edward C. Ricklefs, EB 5B-C
Emily J. Reynolds, OCP 1L-NST
OIG File No. 2007-008T

Office of the Inspector General

Audit Report

To the Vice President,
Information Services

PRIVACY PROTECTION - TVA'S USE OF INFORMATION IN IDENTIFIABLE FORM

Audit Team
Sylvia J. Whitehouse
Sarah E. Huffman

Audit 2007-008T
July 31, 2007

TABLE OF CONTENTS

APPENDIX

EXECUTIVE SUMMARY

As part of our annual audit plan, we performed an audit of the Tennessee Valley Authority (TVA) privacy program, policies, procedures governing use of information in identifiable form (IIF),[i] and privacy protection practices. The audit objectives were to determine if TVA's (1) Information Services Privacy Program Summary Report (Privacy Summary Report) on privacy policies and procedures and use of IIF was accurate and complete, (2) policies and procedures were consistent with federal privacy requirements, (3) privacy program was designed effectively to accomplish its objectives, and (4) privacy-related practices complied with policies and procedures.

We identified three areas where TVA's Privacy Summary Report to the Office of the Inspector General (OIG) needed improvement. In addition, we found:

- TVA's privacy policies and procedures were generally consistent with federal requirements. However, we noted five areas where we believe additional guidance is needed. We further noted TVA is in the process of updating its privacy policies and procedures.
- While TVA has made progress in implementing privacy program components, a focused effort is needed to strengthen the program in the following two areas: (1) complete implementation of planned privacy assessments of all systems[ii] identified with IIF, and (2) ensure privacy activities are better integrated between TVA groups who have privacy responsibilities.
- TVA needs to improve its privacy practices through (1) reviews and updates of Privacy Act Systems of Records[iii] notices and (2) implementation of best practices on systems with IIF.

At the end of our fieldwork on March 8, 2007, our review had not identified any significant IIF compromises reported to the OIG for the two-year period ending December 6, 2006, and no instances of criminal or civil liability relating to loss of personal information were reported by the Office of the General Counsel (OGC). On March 20, 2007, we issued a draft report to management for comment. During the comment period, an issue came to our attention regarding placement of IIF or other sensitive information on temporary share drives. As a result, we withdrew the original draft report until we could perform an audit to determine the extent of exposure of IIF.

---

[i] Information in identifiable form (IIF) – Defined as 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, consistent with Public Law 107–347, the E-Government Act of 2002.

[ii] The term "systems" as used in this report includes major applications, minor applications, and general support systems.

[iii] The term "Systems of Records" as used in this report refers to Privacy Act defined Systems of Records and includes all forms of records, not just records contained in information technology systems.

Audit 2007-10997, Review of Temporary Shares for Sensitive Information, identified 32 incidents of IIF on temporary shares which were not properly secured and could have been accessed by anyone with a TVA network account. As noted in the report, we could not determine if the IIF had been inappropriately accessed since there is no usage tracking available for temporary shares. Weaknesses in any privacy program can lead to potential legal liabilities and reputation damage.

We recommend the Senior Vice President, Information Services, take actions to improve TVA's privacy program and address the identified weaknesses. Recommendations for Audit 2007-10997 are included in that report.

TVA management agreed with our recommendations and proposed actions to implement program improvements (see the Appendix for the complete response). TVA management plans to complete corrective actions by the end of fiscal year 2007, except for recommendation 7, which is scheduled for completion at the end of fiscal year 2008. We concur with TVA management’s proposed actions.

BACKGROUND

The Consolidated Appropriations Act of 2005 (the Act) was enacted in December 2004. Along with changing Tennessee Valley Authority (TVA) management structure, the Act contained a provision regarding privacy protection. Specifically, §522 of the Act required (1) a Chief Privacy Officer be designated to assume primary responsibility for privacy and data protection policy; (2) comprehensive privacy and data protection procedures be established and implemented; (3) the agency to report to the Inspector General on its use of information in identifiable form (IIF)[1] and its privacy and data protection policies and procedures; and (4) an independent review of the agency's use of IIF at least every two years.

While the applicability of §522 of the Act to TVA is not clear, TVA actions consistent with the Act and guidance issued by the Office of Management and Budget (OMB) included (1) naming the Information Services (IS) Senior Vice President as TVA's Senior Agency Official for Privacy (SAOP) in October 2005 and (2) submitting a IS Privacy Program Summary Report (Privacy Summary Report) to the Inspector General in September 2006. The Office of the Inspector General (OIG) conducted this audit as the independent review of TVA's use of IIF.

TVA's SAOP is responsible for agency-wide information privacy issues and protections and for ensuring compliance with applicable federal laws, regulations, and policies. TVA has information in identifiable form from employees, retirees, contractors, business partners, and the public.

OBJECTIVES, SCOPE, AND METHODOLOGY

This audit, which was included in our annual audit plan, evaluated TVA's use of IIF relating to TVA employees and the public and determined the:

a. Extent to which the Privacy Summary Report is accurate and accounts for TVA's current technologies, information processing, and all areas consistent with the Act;
b. Consistency of TVA's privacy policies and procedures with applicable laws and regulations;
c. Effectiveness of TVA's privacy program and data protection procedures governing the collection, use, sharing, disclosure, transfer, and security of IIF; and

[1] Information in identifiable form (IIF) – Defined as 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, consistent with Public Law 107–347, the E-Government Act of 2002.

d. Compliance of actual privacy and data collection practices with TVA's privacy procedures.

In order to meet audit objectives, we completed the following fieldwork during January and February 2007:

- Compared TVA privacy policies and procedures with federal privacy requirements from the Privacy Act of 1974, privacy provisions of the E-Government Act of 2002, and OMB implementing guides;
- Discussed privacy-related activities with staff members in several TVA groups, including IS IT Security, IS Document and Records Management, Communications, Procurement, the Office of the General Counsel (OGC), and the OIG;
- Evaluated TVA privacy-related reports and privacy program management practices;
- Reviewed TVA public and internal Web sites for privacy-related information;
- Reviewed the IS listing of privacy policies and procedures for completeness and to identify specific measures for privacy protection;
- Reviewed OIG investigative records to identify complaints concerning loss of personal information;
- Evaluated records management practices for compliance with federal privacy requirements;
- Compared the IS baseline of significant systems with IIF to the systems inventory to determine whether additional systems warrant inclusion for protecting IIF;
- Reviewed privacy protection practices and identified privacy statements for a sample of systems with IIF to identify best practices in place at TVA; and
- Identified use of continuous auditing in significant systems with IIF and methods used to mitigate risks of inadvertent release of IIF from TVA Web sites.

We conducted this audit in accordance with generally accepted *Government Auditing Standards.*

FINDINGS

In summary, we determined:

- TVA's Privacy Summary Report to the OIG needed improvement in three areas.

- TVA's privacy policies and procedures were generally consistent with federal requirements. However, we noted: (1) five areas where we believe further guidance is needed, and (2) TVA is in the process of updating its privacy policies and procedures.
- While TVA has made progress in implementing privacy program components, a focused effort is needed to strengthen the program in the following two areas: (1) complete implementation of planned privacy assessments of all systems[2] identified with IIF, and (2) ensure privacy activities are better integrated between TVA groups who have privacy responsibilities.
- TVA needs to improve its privacy practices through (1) reviews and updates of Systems of Records[3] notices and (2) implementation of best practices on systems with IIF.

At the completion of our fieldwork on March 8, 2007, our review indicated there were no significant IIF compromises reported to the OIG for the two-year period ending December 6, 2006, and no instances of criminal or civil liability relating to loss of personal information were reported by the OGC. However, as discussed further below, an issue came to our attention subsequent to our review indicating IIF was available on temporary share drives to anyone with a TVA network account. Weaknesses in a privacy program could result in compromise of private information, which may lead to potential legal liabilities and reputation damage.

PRIVACY REPORT COMPLETENESS

In the September 2006 Privacy Summary Report to the OIG, IS provided a list of 60 privacy and data protection policies and procedures. In a separate document, IS identified 50 significant systems with IIF making up the TVA baseline. The Privacy Summary Report could be improved by including:

- Four areas related to privacy protection policies and procedures that were not included in the Summary Report: oversight by the IT Security Executive Committee, Acceptable Use Requirements for the TVA Corporate Network, the new IS procedure on Privacy Impact Assessments, and TVA's Systems of Records.
- Three systems related to electronic deposits, personnel records, and contractor personnel that IS confirmed contained IIF but were not

[2] The term “systems” as used in this report includes major applications, minor applications, and general support systems.

[3] The term "Systems of Records" as used in this report refers to Privacy Act defined Systems of Records and includes all forms of records, not just records contained in information technology systems.

considered in developing the system baseline. During our audit, IS agreed to include the three systems in plans for privacy assessments.

- Current technologies to be used in protecting or transmitting IIF. Projects to implement encryption on desktops and servers and access controls using smart card technology were either in progress or in planning stages.

CONSISTENCY WITH FEDERAL REQUIREMENTS

TVA and IS privacy and data protection policies and procedures that we evaluated were consistent with the majority of federal requirements. However, we believe further or more explicit guidance, based on Privacy Act requirements and OMB guidelines, is needed in the following areas: (1) identifying contracts subject to privacy requirements; (2) requiring machine-readable privacy policies on contractor-hosted Web sites; (3) maintaining the minimal information about individuals necessary to accomplish agency purposes; (4) prohibited disclosure practices, such as selling or renting names and addresses; and (5) processes for notifying individuals of pending releases. IS reported revisions were being reviewed to incorporate privacy components in two TVA-wide policies and three procedures.

PRIVACY PROGRAM EFFECTIVENESS

While TVA has made progress in implementing privacy program components, a focused effort is needed to strengthen the program in the following two areas: (1) completion of all planned privacy assessments of systems with IIF and (2) better integration between TVA groups who have privacy responsibilities.

Since naming TVA's SAOP, IS has made progress in implementing planned privacy program components. Notable accomplishments include implementing privacy training as part of TVA's annual required security awareness and training program, establishing methodologies for identifying and assessing systems with IIF, and initiating security categorizations of information systems. IS completed TVA's first privacy assessment in September 2006. Continued progress is needed to ensure TVA's privacy program completes the implementation necessary for achieving optimal systems protections. More specifically, completing privacy assessments of systems with IIF will be required for TVA to identify best practices and implement the measures necessary to adequately protect such systems and the data they contain. During our audit, we were provided a tentative schedule for completing the assessments of 53 systems during fiscal year 2007.

Although we found some coordination between groups handling TVA's privacy responsibilities, that coordination needs to be improved. Activities related to privacy protection and compliance with privacy requirements include: managing and safeguarding information systems; records

management; exemptions to releases of information under the Freedom of Information Act; contracting actions; training all personnel; handling and tracking legal actions; and investigating privacy-related allegations such as identity theft. These functions are managed in different TVA groups, including IS Architecture, Planning, & Compliance; Communications; Human Resources; Procurement; TVA Police; Nuclear Security; the OGC; and the OIG. However, we did not find privacy-related responsibilities clearly documented for all areas, and an integrated view of TVA privacy efforts describing the relationships between the groups performing privacy protection functions did not exist. An effective privacy program will also clearly communicate responsibilities of security officers, systems owners, records liaisons, and all personnel to help ensure systems are adequately protected and compliance is consistently met over time.

We reviewed allegations reported to the OIG in the last two years and identified no significant IIF compromises as of December 6, 2006. In addition, we determined no instances of criminal or civil liability relating to loss of personal information were reported by the OGC. However, subsequent to our draft report dated March 20, 2007, an issue came to our attention regarding placement of IIF or other sensitive information on temporary share drives. We withdrew the draft report pending an audit of this issue to determine the extent of exposure. Audit 2007-10997, Review of Temporary Shares for Sensitive Information, identified 32 incidents of IIF on temporary shares which were not properly secured and could have been accessed by anyone with a TVA network account. As noted in that report, we could not determine if the IIF had been inappropriately accessed since there is no usage tracking available for temporary shares.

CONSISTENCY OF PRACTICES WITH PROCEDURES

TVA needs to improve the consistency of privacy practices with procedures through (1) reviews and updates of Systems of Records notices and (2) implementation of best practices on systems with IIF. We found IS submitted required reports on privacy, matching programs, and altered Systems of Records. In addition, we identified practices in place for protecting sensitive printed and electronic documents, including documents containing IIF, submitted for processing in TVA's file management system. Although we did not perform an in-depth review of these practices, we found no significant concerns relating to document management in TVA’s file management system.

We found IS had not updated the Systems of Records notices since 1999, although a revision in routine uses was published in 2003. We further found IS had not conducted reviews of TVA Systems of Records notices to ensure their accuracy or reviews of routine use disclosures and exemptions

consistent with OMB guidance.[4] We believe as a best practice such reviews should be conducted periodically, and the systems notices should be updated. We did not attempt to determine whether any new or revised Systems of Records are required for TVA information systems because IS' planned assessments will include this determination.

Based on our review of systems best practices, we determined additional measures may be warranted on internal systems accessible to general TVA users. All tested systems containing IIF restricted user access, but other protection measures were not consistently in place. Approximately one-half of the systems we tested provided a privacy notice when either general or privileged users logged on to the system. Although we found no specific requirement for posting privacy notices in internal systems, implementation is generally a low-cost solution to help remind users the system contains private information and requires special protection. Other protection measures, including monitoring transactions, reviewing activity logs, and continuous auditing techniques, were present in some systems but not widely used. None of the tested systems had implemented encryption technologies, although we noted TVA's encryption project is in progress.

RECOMMENDATIONS

We recommend the Senior Vice President (SVP), IS, consider the following program improvements:

1. Ensure future privacy reports to the OIG include all privacy protection policies and procedures and current technologies to be used in protecting or transmitting IIF.
2. Complete revisions of policies and procedures, including addressing areas identified in this report and clearly identifying privacy-related responsibilities.
3. Complete all planned privacy assessments of systems with IIF.
4. Enhance integration of privacy compliance and protection efforts managed among TVA groups to ensure activities are adequately coordinated.
5. Update TVA's Systems of Records to include revisions and ensure descriptions are accurate.
6. Conduct and document periodic reviews of TVA's Systems of Records.

[4] Appendix I to OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, states Systems of Records should be reviewed every two years to ensure accuracy, and reviews of routine use disclosures and exemptions should take place every four years to ensure reported uses are compatible with agency purposes and exemptions are still needed.

7. Implement privacy notices on all internal systems with IIF accessible to general users from the TVA corporate network and consider implementing other measures as appropriate to protect systems with IIF.

Recommendations for Audit 2007-10997 are included in that report.

Management's Response – The SVP, IS, agreed with our recommendations and proposed actions to implement program improvements (see the Appendix for the complete response). IS plans to complete corrective actions by the end of fiscal year 2007, except for recommendation number 7, which is scheduled for completion at the end of fiscal year 2008.

Auditor's Response – We concur with TVA management's proposed actions.

July 30, 2007

Ben R. Wagner, ET 3C-K

REQUEST FOR COMMENTS - DRAFT AUDIT 2007-008T - PRIVACY PROTECTION - TVA'S USE OF INFORMATION IN IDENTIFIABLE FORM

In response to your memorandum of June 6, 2007, Information Services (IS) provides the attached comments to the subject audit report.

If you have questions or need additional information, please contact Bill Brandenburg at 423-751-2049.

E. Wayne Robertson
Vice President
Information Services
SP 5A-C

WRB:JSE
Attachment
cc (Attachment):
Steven A. Anderson, SP 5A-C
R. Clay Eckles, CTR 1P-M
Frank A. Foster, OCP 2C-NST
Nicholas P. Goschy, Jr., WT 6A-K
John E. Long, Jr., WT 7B-K
Stacie A. Martin, MP 3C-C
Mary E. Ragland, EB 5B-C
Edward C. Ricklefs, EB 5B-C
Anthony D. Smith, WT 5A-K
EDMS, WT CA-K

Memo Audit 2007 008T Privacy Protection 073007.doc

Privacy Protection, TVA's Use of Information in Identifiable Form (IIF)
OIG Audit 2007-008T - Information Service Audit Response

Recommendation	Agreement/ Disagreement	Actions Taken/Planned	Date Taken/ Planned
1. Ensure future privacy reports to the OIG include all privacy protection policies and procedures and current technologies to be used in protecting or transmitting IIF.	Agreement	Recommendations will be incorporated into FY 2007 report.	09/28/07
2. Complete revisions of policies and procedures, including addressing areas identified in this report and clearly identifying privacy-related responsibilities.	Agreement	Recommendations will be incorporated into future policy and procedures documents.	09/28/07*
3. Complete all planned privacy assessments of systems with IIF.	Agreement	Privacy assessments are underway. FY 2007 to date progress: 17 assessments have been conducted with 5 reports complete, 12 in draft, and 38 requests for assessment meetings are issued to contacts or have been scheduled.	09/28/07
4. Enhance integration of privacy compliance and protection efforts managed among TVA groups to ensure activities are adequately coordinated.	Agreement	Recommendations will be incorporated into future policy and procedure documents.	09/28/07*
5. Update TVA's Systems of Records to include revisions and ensure descriptions are accurate.	Agreement	Developed action plan to review all contacts and systems, issue letter of request for review, schedule reviews as needed, update list of Record Systems, republish updated list to Federal Register, and update FOIA Web site.	09/30/07
6. Conduct and document periodic reviews of TVA's Systems of Records.	Agreement	Perform bi-annual reviews of Record Systems list or when changes in law necessitate.	09/30/07
7. Implement privacy notices on all internal systems with IIF accessible to general users from the TVA corporate network and consider implementing other measures as appropriate to protect systems with IIF.	Agreement	Where technically feasible, these recommendations will be implemented and handled via the Privacy Remediation effort. Alternate methods will be considered where measures recommended are not technically feasible.	9/30/08

*Date for policy update. IT Security may not own all related procedures requiring updates. The issued policy will provide guidance for needed updates to associated requirements agency-wide.