



Memorandum from the Office of the Inspector General

June 13, 2007

John E. Long, Jr., WT 7B-K

REQUEST FOR FINAL ACTION – AUDIT 2007-10997 – REVIEW OF TEMPORARY SHARES
FOR SENSITIVE INFORMATION

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

Information contained in this report may be subject to public disclosure. Please advise us of any sensitive information in this report which you recommend be withheld.

If you have any questions, please contact Phyllis R. Bryan, Project Manager, at (865) 632-4043 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
Assistant Inspector General
(Audits and Inspections)
ET 3C-K

PRB:SDB

Attachment

cc (Attachment):

Steven A. Anderson, SP 5A-C
William R. Brandenburg, Jr., MP 2B-C
Maureen H. Dunn, WT 6A-K
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
Stacie A. Martin, MP 3C-C
Richard W. Moore, ET 4C-K
E. Wayne Robertson, MP 3B-C
Anthony D. Smith, WT 5A-K
OIG File No. 2007-10997



Office of the Inspector General

Audit Report

To the Chief Administrative
Officer and Executive Vice
President, Administrative
Services

REVIEW OF TEMPORARY SHARES FOR SENSITIVE INFORMATION

Audit Team
Phyllis R. Bryan
Brian S. Childs
Kyle B. Cox
Melissa M. Neusel
Sarah E. Tipton
Stephanie R. Turner

Audit 2007-10997
June 13, 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
BACKGROUND	1
OBJECTIVES, SCOPE, AND METHODOLOGY	1
FINDINGS	2
PII AND BUSINESS SENSITIVE INFORMATION	2
NON-BUSINESS INFORMATION	3
MANAGEMENT OF TEMPORARY SHARES	4
NOTIFICATION POLICY	4
INFORMATION SECURITY POLICY	4
RECOMMENDATIONS	5

APPENDIX

MEMORANDUM DATED JUNE 8, 2007, FROM JOHN E. LONG, JR., TO
BEN R. WAGNER

EXECUTIVE SUMMARY

We performed an audit of Tennessee Valley Authority (TVA) temporary share drives to determine the extent to which personally identifiable information (PII)ⁱ and/or other sensitive information is being stored on these drives. Temporary share drives are provided at geographic locations around the Valley and are used by a broad spectrum of TVA employees to support the transfer and sharing of extremely large data files. Information Services (IS) identified 20 temporary shares; however, we were only able to access 17 of the shares which were generally available to all users within TVA, including contractors with TVA IDs.

In summary, we determined:

- PII (32 instances) and other sensitive information (69 instances) were not properly secured thus exposing the information to anyone with a TVA network ID. The lack of protection of this information is a violation of TVA policy and could result in a violation of the Privacy Act.
- Shares were being used to store non-business related information (four instances) which included games, personal pictures, and other documents.
- TVA does not have a policy or guidance for management of temporary shares to address the proper use of the share (i.e., types of information that can be stored, the unsecured nature of the share), responsibilities of the users, and maintenance (i.e., maximum time frame for retention of files on the share).
- TVA Standard Programs and Processes (SPP) 12.9 on Computer Security and Privacy Incident Response, which includes procedures for notifying TVA employees and their dependents, contractors, and retirees and their dependents when PII has potentially been compromised, has yet to be implemented.
- Two business practice drafts (1) TVA Information Security Policy, which describes classification and protection of information, and (2) Acceptable Use of Information Resources (Rules of Behavior), which explicitly prohibits storage of non-TVA information on TVA servers, have yet to be implemented.

ⁱ Personally identifiable information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identify, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

As instances of questionable items were found, we notified IS personnel who coordinated with the Organization Security Officer (OSO) or the person who put the information on the share to determine the appropriate level of security to be assigned to the item. The instances identified were put on the shares by individuals across multiple TVA organizations. The high risk items like PII information were immediately secured by IS. The determination of the sensitivity of some medium to low risk items is still underway by IS and the OSO.

We recommend Chief Administrative Officer and Executive Vice President, Administrative Services, ensure:

1. OSOs and IS continue the review of the identified items and restrict access as needed.
2. The draft procedure TVA-SPP-12.9 on Computer Security and Privacy Incident Response is implemented.
3. For PII data exposures identified in this audit, general and/or individual notifications are made regarding the type of data exposed and TVA management's assessment of risk regarding the data exposures. Individual notice should be given whenever PII, such as social security numbers or other information which could be used in identity theft, is disclosed.
4. The draft business practices on Information Security Policy and Acceptable Use of Information Resources and other guidance on the use of temporary shares are implemented or developed and all TVA employees and contractors are trained on these policies.

Management's Response – TVA management agreed with the findings and provided completed and planned actions to implement the recommendations (see the Appendix for TVA comments). In summary, TVA has completed or plans to complete (1) a review of the remaining temporary shares; (2) implementation of the draft procedure TVA-SPP-12.9 on Computer Security and Privacy Incident Response; (3) general notification of the incidents, including employee and, as necessary, public notification; and (4) implementation of draft business practices on Information Security Policy and Acceptable Use of Information Resources, associated training and provide guidance on use of temporary shares.

Regarding individual notification, TVA management is (1) awaiting the results of its risk assessment before making a decision on individual notifications and (2) informing the contractor of the PII exposure of their database and requesting the contractor to advise TVA regarding any notifications the contractor makes.

Auditor's Response – We concur with management's proposed actions for recommendations 1, 2, and 4. Regarding recommendation 3, we believe TVA's decision to perform a risk assessment to determine the level of notification required is consistent with OMB guidance. We recommend TVA (1) issue a general notification quickly and (2) expedite the risk assessment process to ensure individual notification, if warranted, is performed in a timely manner. The OIG will conduct a follow-up review after TVA completes its risk assessment process. The review will determine whether TVA's decision regarding individual notification(s) was reasonable.

BACKGROUND

In March 2007, Information Services (IS) notified the Office of the Inspector General (OIG) of an incident in which Performance Review and Development (PR&D) forms had been stored in a temporary share on an unsecured server. The PR&D forms identified the name of the person and employee ID but did not contain social security numbers. This information was available on a temporary share drive for approximately two hours. The OIG initiated an audit (2007-039T) to review the PR&D data exposure. In the course of that audit, we identified the potential for similar data exposures on other temporary share drives.

Temporary share drives are provided at geographic locations around the Valley and are used across Tennessee Valley Authority (TVA) organizations by TVA employees and contractors to support the transfer and sharing of extremely large data files. These share drives are generally accessible to all users within TVA, including contractors with TVA IDs.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this audit was to determine the extent to which personally identifiable information (PII) and/or other sensitive information is being stored on temporary share drives. The scope of the audit covered 20 temporary shares identified by IS; however, we were only able to access 17 of the shares.

To accomplish our objective, we:

- Obtained a listing of the 20 temporary shares from IS.
- Accessed each share and opened documents to determine if they contained any PII, TVA sensitive information, contractor proprietary information, or any other questionable information. We did not perform a 100 percent review of all the nuclear shares because the five nuclear shares contained almost 2.2 million files. We stopped our review of these shares after finding numerous instances of PII or business sensitive information and recommended the Organization Security Officers (OSO) further review the shares.
- Ranked each item as high, medium, or low risk and provided the information to IS for coordination and disposition with OSOs. In general, we used the following criteria for ranking the items:
 - **High** -- Files containing PII, such as social security numbers and names or other identifying information, or Nuclear Safeguards Information.

- **Medium** -- Files potentially containing business sensitive information or labeled “sensitive,” “proprietary,” or other wording indicating distribution should be limited.
- **Low** -- Files which appeared to be personal information (pictures, documents, etc.)
- Reviewed Communications Practice 8, Accessing and Using TVA Computing Resources; the drafts of two new business practices, TVA Information Security Policy and Acceptable Use of Information Resources (Rules of Behavior); and the draft of new Standard Programs and Processes (SPP), Computer Security and Privacy Incident Response.

Fieldwork was conducted in April 2007. This audit was performed in accordance with generally accepted government auditing standards.

FINDINGS

In summary, we determined (1) PII and other sensitive information were not properly secured thus exposing the information to anyone with a TVA network ID; (2) shares were being used to store non-business related information; (3) TVA does not have a policy or guidance for management of temporary shares to address the proper use of the share; (4) TVA does not have a policy implemented regarding the level of notification required when PII has been compromised; and (5) two business practice drafts (a) TVA Information Security Policy, which describes classification and protection of information handled throughout TVA, and (b) Acceptable Use of Information Resources (Rules of Behavior), which explicitly prohibits storage of non-TVA information on TVA servers, have yet to be implemented.

The lack of protection of PII and other sensitive information is a violation of TVA policy and could result in a violation of the Privacy Act. As instances of questionable items were found, we notified IS personnel who coordinated with the OSO or the person who put the information on the share to determine the appropriate level of security to be assigned to the item. The instances identified were put on the shares by individuals across multiple TVA organizations. The high risk items like PII information were immediately secured by IS. The determination of the sensitivity of some medium to low risk items is still underway by IS and the OSOs.

PII AND BUSINESS SENSITIVE INFORMATION

We found 101 instances of PII for TVA and contractor personnel and business sensitive information stored across the temporary shares. The 32 instances of PII for TVA employees and contractor employees included:

- A database with approximately 7,900 employee names, social security numbers, telephone calling card numbers, and long distance

authorization codes for the nuclear plants. Further investigation indicated this information was available on several occasions over the last few months for up to a week each time on a temporary share.

- A database with approximately 11,000 contractor employees' names, social security numbers, home addresses, telephone numbers, date of birth, disability codes, termination status, rehire status comments, etc. This database is used by a nuclear contractor to check their employees in and out of the plant. Further investigation of this information indicated the information has been available on a temporary share since 2004.
- Documents with names and social security numbers.
- Documents with names, social security numbers, and dosimeter readings.
- E-mails regarding disciplinary action and incident investigations.

All PII files were secured by IS upon notification. We could not determine if PII information had been inappropriately accessed since there is no usage tracking available for temporary shares.

We also found 69 instances of business sensitive information of TVA and contractors stored across the temporary shares. The information included:

- TVA documents or drawings marked "Sensitive" or "Business Sensitive"
- Contractor documents or drawings marked "Proprietary Information"
- Contractor proposals
- Document marked "Attorney/Client Privilege"

In addition to the documents described above, we noted numerous instances of unmarked substation drawings, nuclear plant component drawings, pictures of components in plants and substations, etc. We questioned these items as potentially sensitive information that should not be available to everyone with a TVA ID. These documents are being reviewed by the OSOs to determine if access should be restricted.

NON-BUSINESS INFORMATION

We found four incidents of shares being used to store non-business related information which included personal pictures and other documents, and Nintendo games which could be played on a Nintendo Entertainment Emulator. Current Communications Practice 8, states "Use of all computing resources in TVA is to be utilized in support of legitimate TVA business interests." A draft business practice, Acceptable Use of Information Resources (Rules of Behavior), provides explicit prohibitions including "Storage of non-TVA information on TVA servers and other electronic storage devices." According to TVA's IT Security organization, this draft business practice is in the final issuance process.

MANAGEMENT OF TEMPORARY SHARES

TVA does not have a policy or guidance for management of temporary shares to address the proper use of the share (i.e., types of information that can be stored, the unsecured nature of the share), responsibilities of the users, and maintenance (i.e., maximum time frame for retention of files on the share). As such, we observed:

1. Some temporary shares appear to have evolved from temporary to permanent storage areas. For example, five nuclear shares store over 720 GB of information and have almost 2.2 million files, some of which are over 10 years old. In addition, accounts for nuclear personnel are automatically mapped to these shares.
2. Two of the 20 temporary shares had a defined time for weekly deletion of documents. Files could remain on the other shares until the share was cleaned up by users (1) after email notification to the site that the folder is full or (2) by request from site IS personnel.
3. There was nothing to identify the shares as unsecured temporary storage areas. IS put a file on one share to identify it as unsecured after PR&D information was found on the share.

NOTIFICATION POLICY

While there is not a federal law at this time requiring notification by TVA when PII has been compromised, there is proposed legislation which would require federal agencies to notify individuals when their PII has been compromised. TVA has drafted a SPP which defines the process for responding to computer security and privacy incidents. TVA-SPP-12.9 on Computer Security and Privacy Incident Response contains (1) guidelines for establishing the response team, which includes an Office of the General Counsel representative; (2) a risk assessment methodology for determining under what circumstances a general notification and/or individual notification is warranted; and (3) steps to be performed when notifying. According to TVA's IT Security organization, this SPP is in the final issuance process.

INFORMATION SECURITY POLICY

TVA has drafted a Business Practice to establish TVA's Information Security Policy. This business practice is intended to supersede the outdated Protection of Sensitive Information and Records policy issued on December 10, 1996. The draft business practice describes the classification and protection mechanisms for information handled throughout TVA. According to TVA's IT Security organization, this draft business practice is in the final issuance process.

RECOMMENDATIONS

We recommend Chief Administrative Officer and Executive Vice President, Administrative Services, ensure:

1. OSOs and IS continue the review of the identified items and restrict access as needed.
2. The draft procedure TVA-SPP-12.9 on Computer Security and Privacy Incident Response is implemented.
3. For PII data exposures identified in this audit, general and/or individual notifications are made regarding the type of data exposed and TVA management's assessment of risk regarding the data exposures. Individual notice should be given whenever PII, such as social security numbers or other information which could be used in identity theft, is disclosed.
4. The draft business practices on Information Security Policy and Acceptable Use of Information Resources and other guidance on the use of temporary shares are implemented or developed and all TVA employees and contractors are trained on these policies.

TVA Management's Response – The Chief Administrative Officer and Executive Vice President, Administrative Services, agreed with the findings and provided proposed corrective actions to address our recommendations (see the Appendix). In summary:

1. OSOs and IS completed the review of the temporary shares. An additional 169 instances of PII were identified. This information has been moved to a secure, hidden share. TVA will be conducting a risk analysis on this information. IS will institute a plan to monitor and review all share drives for sensitive information. Details of this plan will be completed by July 31, 2007.
2. TVA is in the process of converting TVA level SPPs to TVA Procedures. TVA-SPP-12.9 will become a TVA procedure on Computer Security and Privacy Incident Response. Once converted, the procedure will go through the standards review process and is expected to be deployed by September 30, 2007.
3. Even though the PII information was accessible within TVA by those with an authorized TVA ID, there is no evidence to suggest that this data has been acquired by an unauthorized person or disclosed outside of TVA. TVA will conduct a risk analysis for all identified instances of PII and will tailor its response to the nature and scope of the risk and ensure the

response complies with any applicable federal regulations. These assessments are expected to be completed for the original instances by June 29, 2007, and the remaining instances by July 31, 2007.

Regarding notifications, TVA stated they (1) do not plan to issue individual notification of the exposure of sensitive information unless the risk assessments indicate a need to do so; and (2) will issue general, broad notification of the incidents, including employee and, as necessary, public notification. For the contractor database containing PII, TVA plans to notify the contractor and ask them to inform TVA of any general or individual notification the contractor makes.

4. The draft business practices are currently in the IS review and comment phase. The remaining implementation activities include: OSO, IT Council, and SBU review, comment resolution, and deployment activities (communication, publication, and training). The expected completion date for full deployment is June 30, 2007.

The continued use of temporary shares is being evaluated by IS. Based on this evaluation, appropriate guidance on the proper management and use of temporary shares will be developed and is expected to be issued to business units by June 30, 2007.

Auditor's Response – We concur with management's proposed actions for recommendations 1, 2, and 4. Regarding recommendation 3, we believe TVA's decision to perform a risk assessment to determine the level of notification required is consistent with OMB guidance. We recommend TVA (1) issue a general notification quickly and (2) expedite the risk assessment process to ensure individual notification, if warranted, is performed in a timely manner. The OIG will conduct a follow-up review after TVA completes its risk assessment process. The review will determine whether TVA's decision regarding individual notification(s) was reasonable.

SENSITIVE

June 8, 2007

Ben R. Wagner, ET 3C-K

REQUEST FOR COMMENTS - DRAFT AUDIT 2007-10997 - REVIEW OF TEMPORARY SHARES FOR SENSITIVE INFORMATION

We agree with the findings in the subject audit report issued on May 4, 2007. With regard to the four recommendations, the following observations and actions are planned:

Recommendation: Organizational Security Officers (OSOs) and Information Services (IS) continue the review of identified items and restrict access as needed.

Action: As a result of a comprehensive review of non-TVAN temporary share drives, the Office of the Inspector General (OIG) identified 104 instances of sensitive information stored on the temporary share drives by a broad spectrum of TVA employees. All instances identified as high-risk items (46) were secured immediately by IS. The remaining 77 items categorized as medium or low were turned over to the business unit OSOs for coordination. The OSOs handled each item by contacting the owner of the file. The file owner either deleted the file or moved it to a storage location with proper security. The 104 items, including those handled by business unit OSOs, were tracked utilizing HP Service Desk. As of May 10, all 104 items had been handled and the HP Service Desk tickets were closed.

In addition to the temporary shares reviewed by the OIG, we have completed a comprehensive review of the remaining shares that were used by TVAN. A joint team of IS and TVAN representatives reviewed and dispositioned the data utilizing the same technique used by the OIG and IS during the original audit. As of May 25, 169 instances of personal information in identifiable form (PII) were identified on 5 temporary shares. This information has been moved to a secure, hidden share. We will be conducting a risk analysis on this information.

As we continue to monitor and review temporary share drives, IS will also institute a plan to monitor and review all share drives for sensitive information. Details of this plan will be completed by July 31, 2007.

Recommendation: The draft procedure TVA-SPP-12.9 on Computer Security and Privacy Incident Response is implemented.

Action: TVA is in the process of restructuring corporate level practices and procedures. The restructuring effort will include the conversion of TVA level SPPs to TVA Procedures. TVA-SPP-12.9 is an enhanced procedure for responding to computer security and privacy incidents. It supersedes existing guidance issued by IT Security in 2003 entitled *Computer Security Incident Handling*. This SPP will become a TVA Procedure on Computer Security and Privacy Incident Response. Once converted, the procedure will go through the standard review process and is expected to be deployed by September 30, 2007.

SENSITIVE

Ben R. Wagner
Page 2
June 8, 2007

Recommendation: For PII data exposures identified in this audit, general and/or individual notifications are made regarding the type of data exposed and TVA management's assessment of risk regarding the data exposures. Individual notice should be given whenever PII data, such as social security numbers or other information which could be used in identity theft, is disclosed.

Action: Even though the PII information was accessible within TVA by those with an authorized TVA ID, there is no evidence to suggest that this data has been acquired by an unauthorized person or disclosed outside of TVA.

TVA will conduct a risk analysis for each of the 201 identified instances and will tailor its response to the nature and scope of the risk and ensure that the response complies with any applicable federal regulations. An IS review team, with legal advice from the Office of the General Counsel (OGC), began the risk assessment process for each of the OIG 32 identified instances of PII data on May 14. The risk assessment of the original 32 instances is expected to be completed by June 29, 2007. The team will also complete a risk assessment of the 169 instances identified in the latest review. This assessment is expected to be completed by July 31, 2007.

Planned Notification Action:

We will provide individual notification if the risk assessments indicate a need to do so. After discussion of legal requirements with OGC and reviewing OMB guidance, to the extent appropriate, we do not plan to issue individual notification of the exposure of sensitive information at this time. However, TVA will issue general, broad notification of these incidents, including employee and, as necessary, public notification. The following outlines the communication plan.

- TVA Procurement will notify [Redacted] that an [Redacted] database containing PII data was accessible internally at TVA to all TVA employees with an authorized TVA ID. TVA will ask [Redacted] to inform TVA of any general or individual notification they make.
- TVA will notify employees of the PII data exposure utilizing a broad statement to all employees.
- TVA will issue the new Business Practices referenced above to address information security, rules of behavior, and rules for use and management of temporary share drives.
- TVA will develop a public notification plan to be carried out as necessary in parallel with the broad employee notification.

Recommendation: The draft business practices on Information Security Policy and Acceptable Use of Information Resources and other guidance on the use of temporary shares are implemented or developed and all TVA employees and contractors are trained on these policies.

SENSITIVE

Ben R. Wagner
Page 3
June 8, 2007

Action: The draft business practice on Information Security Policy defines an enhanced TVA policy for safeguarding information in documentary (hard copy) and electronic forms consistent with current applicable laws, standards, directives, and industry best practices. It will supersede the *Protection of Sensitive Information and Records Policy* issued in December 1996 and the IT Position Statement on the *Minimum Requirements for the Electronic Transfer of Sensitive Information* issued in December 2005. The Acceptable Use of Information Resources defines the set of rules that describes responsibilities and expected behavior with regard to information and information system usage. This practice will replace several IT Security Position Statements and parts of other TVA level business practices. These practices are currently in the IS review and comment phase. The remaining implementation activities include: OSO, IT Council, and SBU review, comment resolution, and deployment activities (communication, publication, and training). The expected completion date for full deployment is June 30, 2007.

The findings of this investigation have shown that the handling of sensitive information is a TVA-wide issue. On May 16, I issued a letter to the TVA Business Council advising them of the audit findings and enlisting their support to emphasize the importance of handling and protecting sensitive information within their organizations. The new practices and TVA Procedure described above will be targeted for TVA-wide training. Additionally, the IT Security and Privacy Annual Training module will be modified to emphasize the personal accountability and proper handling of sensitive information. The annual IT Security and Privacy training activity is required for every TVA employee and contractor with an NT ID on their training anniversary date and all new employees during new employee orientation.

The continued use of temporary shares is being evaluated by Information Services. Based on this evaluation, appropriate guidance on the proper management and use of temporary shares will be developed and is expected to be issued to business units by June 30, 2007.

Please let me know if you have questions or would like to discuss these issues further.



John E. Long, Jr.
Chief Administrative Officer and
Executive Vice President
Administrative Services
WT 7B-K

cc: Maureen H. Dunn, WT 6A-K
Tom Kilgore, WT 7B-K
E. Wayne Robertson, MP 3B-C
EDMS, WT CA-K