Memorandum from the Office of the Inspector General

November 20, 2007

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

FINAL REPORT – AUDIT 2007-11198 – REVIEW OF RISK ASSESSMENT PERFORMED ON PERSONALLY IDENTIFIABLE INFORMATION

Attached is the subject final report for your review. This report does not include any recommendations and is to be used for informational purposes only. Accordingly, no response is necessary.

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.

Robert E. Martin
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
Peyton T. Hairston, Jr., WT 7B-K
Tom D. Kilgore, WT 7B-K
Janice W. McAllister, EB 7A-C
Richard W. Moore, ET 4C-K
Emily J. Reynolds, OCP 1L-NST
OIG File No. 2007-11198

Review of Risk Assessment Performed on Personally Identifiable Information (PII)

Audit 2007-11198

November 20, 2007

Synopsis

- In summary, we found the (1) risk assessment methodology was consistent with National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidance, and (2) the conclusions reached were reasonable.

Background

- OIG Audit 2007-10997, Review of Temporary Shares for Sensitive Information, found 32 instances of PII not properly secured on temporary share drives thus exposing the information to anyone with a TVA network ID.
- Information Services (IS) and Organization Security Officers (OSO) conducted subsequent reviews of the Nuclear temporary share drives and found 169 additional instances of PII.
- In response to our findings, TVA management conducted a two-phase risk analysis on PII found stored on temporary share drives to determine the appropriate level of disclosure to individuals affected. Phase I reviewed the PII found during the OIG audit, and Phase II reviewed the PII identified during the IS/OSO review. Phases I and II utilized the same risk assessment methodology.
- TVA issued a general notification on the PII exposure but determined, based on the risk assessment, individual notification was not needed.

Background

- To determine the risk level for each occurrence of PII, TVA used the following risk model:

  Overall Risk = Weighted Threat Likelihood x Magnitude of Impact

- An Overall Risk Rating of:
  - "Low" would not require individual notification.
  - "Moderate" would not require individual notification unless there were verifiable instances of data capture and probable intent to misuse data.
  - "High" would require individual notification.

Objective, Scope & Methodology

Objective

- Review the risk assessment methodology used to evaluate PII identified during OIG and IS reviews of temporary shares and determine if IS' conclusions regarding risk exposure of PII were reasonable.

Scope & Methodology

- Interviewed IS personnel.
- Performed a walkthrough of the process used by the IS PII Assessment Team.
- Identified applicable criteria related to risk assessment and PII data breach response.

Objective, Scope & Methodology

Scope & Methodology (cont'd)

- Compared the risk assessment methodology to (1) NIST SP 800-30, Risk Management Guide for Information Technology Systems and (2) OMB guidance.
- Evaluated a sample of seven risk scores against supporting interview documentation.
- Reperformed risk ranking calculations for (1) our sample and (2) all Phase I interviews.
- Fieldwork was conducted between August and November 2007.
- This audit was performed in accordance with generally accepted government auditing standards.

Finding

- In summary, we determined the (1) risk assessment methodology was consistent with NIST and OMB guidance, and (2) the conclusions reached were reasonable.
  - The Risk Model used (Overall Risk = Weighted Threat Likelihood x Magnitude of Impact) is consistent with the NIST SP 800-30 guidance. In addition, this model is consistent with OMB guidance which recommends using a risk-based approach to determine whether notification of a breach is required.
  - The criteria TVA developed for rating Threat Likelihood and Magnitude of Impact appeared reasonable.
  - TVA determined, based on the risk model, that none of the occurrences reached the risk level of high which would have required individual notification. In our review of a sample of the risk rating assignments, we noted one of the seven sampled was not calculated correctly; however, when the rating was recalculated it did not change the overall risk rating for that occurrence. Therefore, we believe the conclusions reached based on the risk ratings and methodology used were reasonable.