TVA

ANALYSIS OF PERSONNEL RECORDS IMAGING SYSTEM (PRIS) SYSTEM/BACKUP FAILURES AND PERFORMANCE REVIEW AND DEVELOPMENT (PR&D) DATA EXPOSURE

Audit 2007-039T-01

July 25, 2007

TENNESSEE VALLEY AUTHORITY
ECONOMY ~ EFFICIENCY ~ EFFECTIVENESS
1985
OFFICE OF THE INSPECTOR GENERAL

TVA RESTRICTED INFORMATION

Synopsis

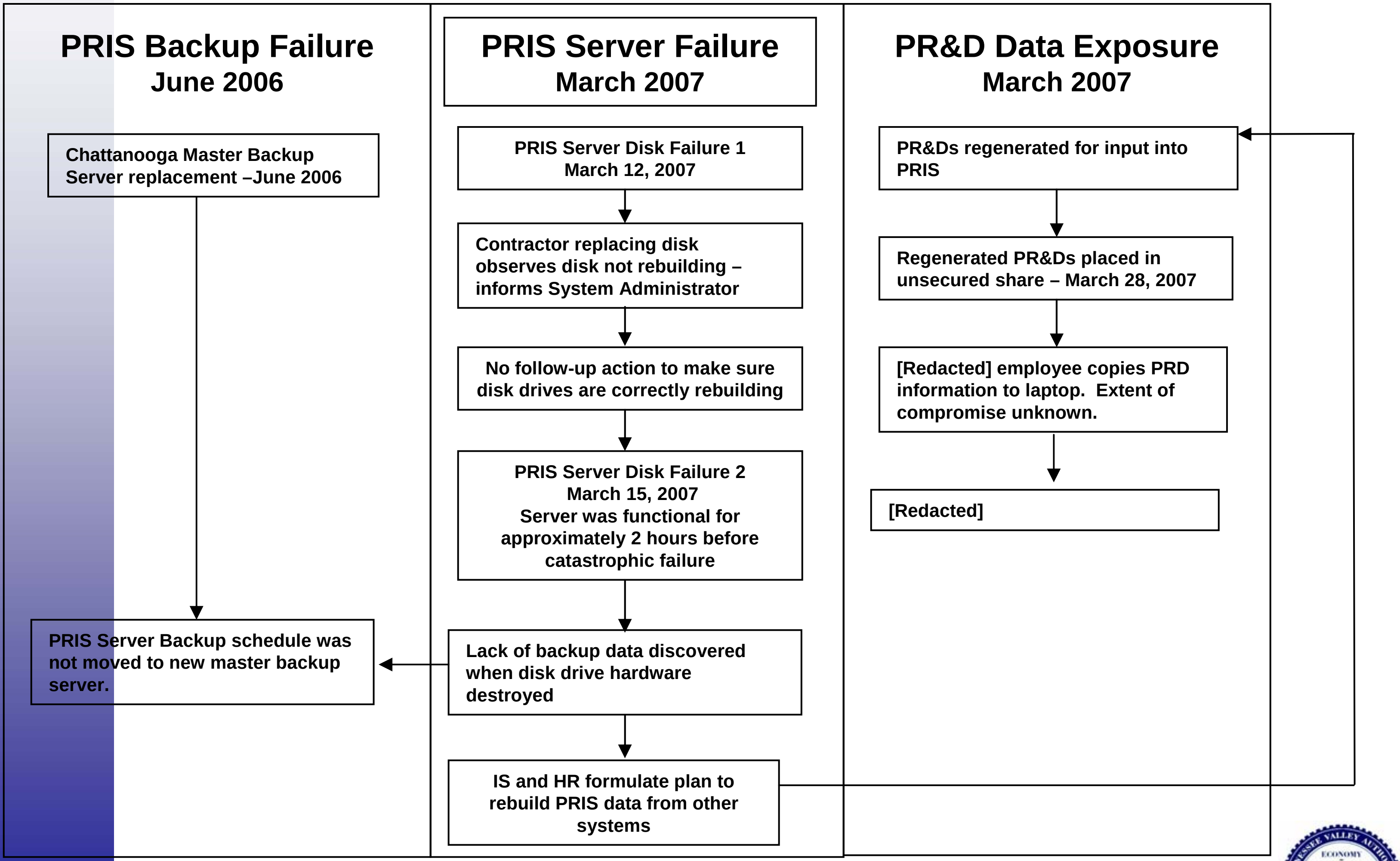
We conducted a review to determine (1) the root causes for the PRIS backup and server failures and (2) whether data recovered was adequately protected. In summary, we determined:

- The PRIS backup failure was due to (1) human error and (2) the lack of proper controls which would have detected PRIS was no longer on the master backup schedule and resulted in not having backups performed for PRIS.
- The PRIS server failure was due to hardware failures whose impact was magnified by human error.
- The PR&D data was not adequately secured when regenerated for recovery efforts.

Background

- PRIS is the official repository for TVA personnel documents such as employment applications, offer letters, disciplinary letters, performance evaluations, termination papers, etc.
- In March 2007, PRIS had two disk drive failures.
- As Information Services (IS) began work to recover the PRIS system, they discovered a system backup had not been performed.
- IS began pursuit of other options to restore the data.

Timeline



PRIS Backup Failure
June 2006

Chattanooga Master Backup Server replacement –June 2006

PRIS Server Backup schedule was not moved to new master backup server.

PRIS Server Failure
March 2007

PRIS Server Disk Failure 1
March 12, 2007

Contractor replacing disk observes disk not rebuilding – informs System Administrator

No follow-up action to make sure disk drives are correctly rebuilding

PRIS Server Disk Failure 2
March 15, 2007
Server was functional for approximately 2 hours before catastrophic failure

Lack of backup data discovered when disk drive hardware destroyed

IS and HR formulate plan to rebuild PRIS data from other systems

PR&D Data Exposure
March 2007

PR&Ds regenerated for input into PRIS

Regenerated PR&Ds placed in unsecured share – March 28, 2007

[Redacted] employee copies PRD information to laptop. Extent of compromise unknown.

[Redacted]

Objectives

- Perform a root cause analysis of the PRIS system and backup failures
- Determine if data recovered was adequately protected

Scope/Methodology

- Interviewed IS, Human Resources, and Power System Operations (PSO) personnel
- Reviewed IS Policies and Procedures
- Reviewed documentation
  - HP Service Desk (HPSD) information
  - E-mails related to the PRIS and PR&D events
  - PRD folder on temporary share server
- Fieldwork was conducted in April and May 2007
- This audit was performed in accordance with generally accepted government auditing standards.

Findings

- Root cause of the PRIS backup failure was human error and the lack of proper controls which would have detected:
  - The master backup schedule was not properly converted in June 2006; and
  - A PRIS backup did not exist.
- Root cause of the PRIS server failure was hardware failures whose impact was magnified by human error.
- The PR&D data was not adequately secured when regenerated for recovery efforts.

PRIS Backup Failure

- Cause 1: Human error and lack of controls to ensure the proper conversion of the backup schedules
  - Inadequate Planning for Conversion
    - Coordination with system administrators to verify backups was not adequate – System administrators were notified of the conversions; however, there was no explicit requirement for the administrators to verify a backup occurred after the move.
    - Lack of segregation of duties – No independent verification to ensure all backup schedules were converted to the new system instead the same person who performed the conversion also verified the conversion.
    - Test plan and result documentation not appropriately maintained.

PRIS Backup Failure (cont'd)

- Cause 2: Lack of controls to detect a PRIS backup schedule did not exist after June 2006
  - No periodic verification required to ensure the master backup schedule is consistent with the customer requirements as defined in the service level agreements
  - No automated tool to detect a server was not being backed up
    - Funds were budgeted in fiscal year (FY) 2005 to purchase an automated tool which would have identified servers not being backed up. These funds were used for infrastructure improvements to improve throughput and efficiency of backup operations.

Other Backup Failures

- During the review, the following came to our attention:
  - September 2006 – [Redacted] requested data restore of the [Redacted] system and data was not available
    - Data regarding the [Redacted] was to be backed up to the Regional Operations Center (30 day retention) and Chattanooga (permanent retention).
    - Chattanooga backup began failing and was removed from the schedule by backup personnel because of assumption the Chattanooga backup was a duplicate.
    - Data lost for the period March through August 2006.
  - November 2006 – Manual Check found a missing backup client
    - Backup personnel were reconciling client list and found one client was missing
      - No documentation to support being dropped from backup
      - Lack of a backup caught by IS and no data loss occurred

Backup Failures

- IS Actions Taken:
  - Implemented a process to verify servers added or dropped from the master backup schedule are accurate and have proper supporting documentation
  - Developed a monitoring program for Windows servers to identify those where no backup was performed
- TVA management requested the Office of the Inspector General (OIG) perform a verification of backups. This review is currently underway (Audit 2007-039T-02).

PRIS Server Failure

- PRIS server had two hard drive failures in March 2007
  - Server was six to seven years old; normal life span for a server is five years
  - Impact from drive failures magnified by human errors
    - System Administrator was not diligent in monitoring drive replacement process
      - When first drive started failing, the system administrator did not verify the existence of a backup or request a backup be performed
      - The server hard drive configuration was considered stable; therefore, system administrator assumed the drives would rebuild automatically
      - Insufficient follow-up after drive replacement to verify (1) rebuild process was successful and (2) manual reconfiguration for this hardware type was performed to activate the hot spare
  - HPSD, an asset management tool used by IS, did not have information regarding the criticality and recovery requirements of the systems
    - HPSD did not have a Disaster Recovery level defined for PRIS.
    - The Work Agreement for FY2007 with the business unit specified a DR level of B which requires a return to service of three to seven days with no more than 24 hours of data loss. An internal IS email stated the disaster recovery work for PRIS-[Redacted] could be deleted. However, we could not locate a revised work agreement or any indication that the business unit had approved such a change.

PR&D Data Exposure

- To help in the PRIS recovery, IS regenerated PR&D forms, which did not contain social security numbers, for approximately 9,000 employees for the period 2001 – 2006.
- IS personnel failed to exercise adequate security in the handling of sensitive data.
  - Sensitive information was placed on an unsecured temporary share where it was available for about two hours
  - Sensitive information was accessed by:
    - [Redacted] employee who copied the forms.
    - IS employee who viewed the folder on the server and reported the incident to the system administrators who initiated action to restrict access to the information.
- We could not determine conclusively the extent of exposure because (1) the temporary share was available to all employees and contractors with a TVA ID, and (2) there were no logs maintained for review.

PR&D Data Exposure

- IS Actions Taken: A communiqué was issued to the IS supervising managers instituting a lock down on use of temporary shares for sensitive information and requiring 100 percent training of IS personnel in Communication Practice 8.
- Subsequently, OIG performed a review of temporary share drives in TVA to determine if determine the extent to which personally identifiable information (PII) and/or other sensitive information is being stored on these drives.
  - We identified numerous instances of PII and sensitive information stored unsecurely on temporary share drives used by a broad spectrum of TVA employees. (See Audit 2007-10997 for additional information and recommendations.)

Recommendations

1. Ensure future upgrade projects include proper planning and controls such as an independent third-party verification of data/schedule moves and proper supporting documentation be maintained.

2. Implement a process to periodically verify the master backup schedule complies with customer requirements.

3. Review and consider purchasing automated solutions that would (1) detect servers not currently included in the master backup schedule and (2) monitor information flowing on the network and stored on servers which would help identify PII.

4. Implement a process to ensure (1) HPSD information regarding the service level and disaster recovery level matches the requirements in the service level agreements; and (2) changes to service level agreements, including non-funded work, are approved by the business unit responsible for the application(s).

Recommendations (cont'd)

5. Implement/update procedures for hardware replacement to include:
   - Checking HPSD for criticality of system data
   - Checking for backups when hardware failure warnings occur
   - Verifying disk drive configurations are restored to the appropriate settings after hardware replacement/repair is completed
   - Communicate/train system administrators on changes to the procedures

6. Implement/update TVA-wide training to emphasize employee and business unit responsibilities for properly securing data which contains personally identifiable and business sensitive information. Consider:
   - Targeting business units which routinely handle social security number and other PII for more frequent training
   - Including reminders to periodically review electronic and hard copy storage to ensure information is properly secured

7. See Audit 2007-10997, Review of Temporary Shares for Sensitive Information, for additional recommendations regarding properly securing sensitive information.

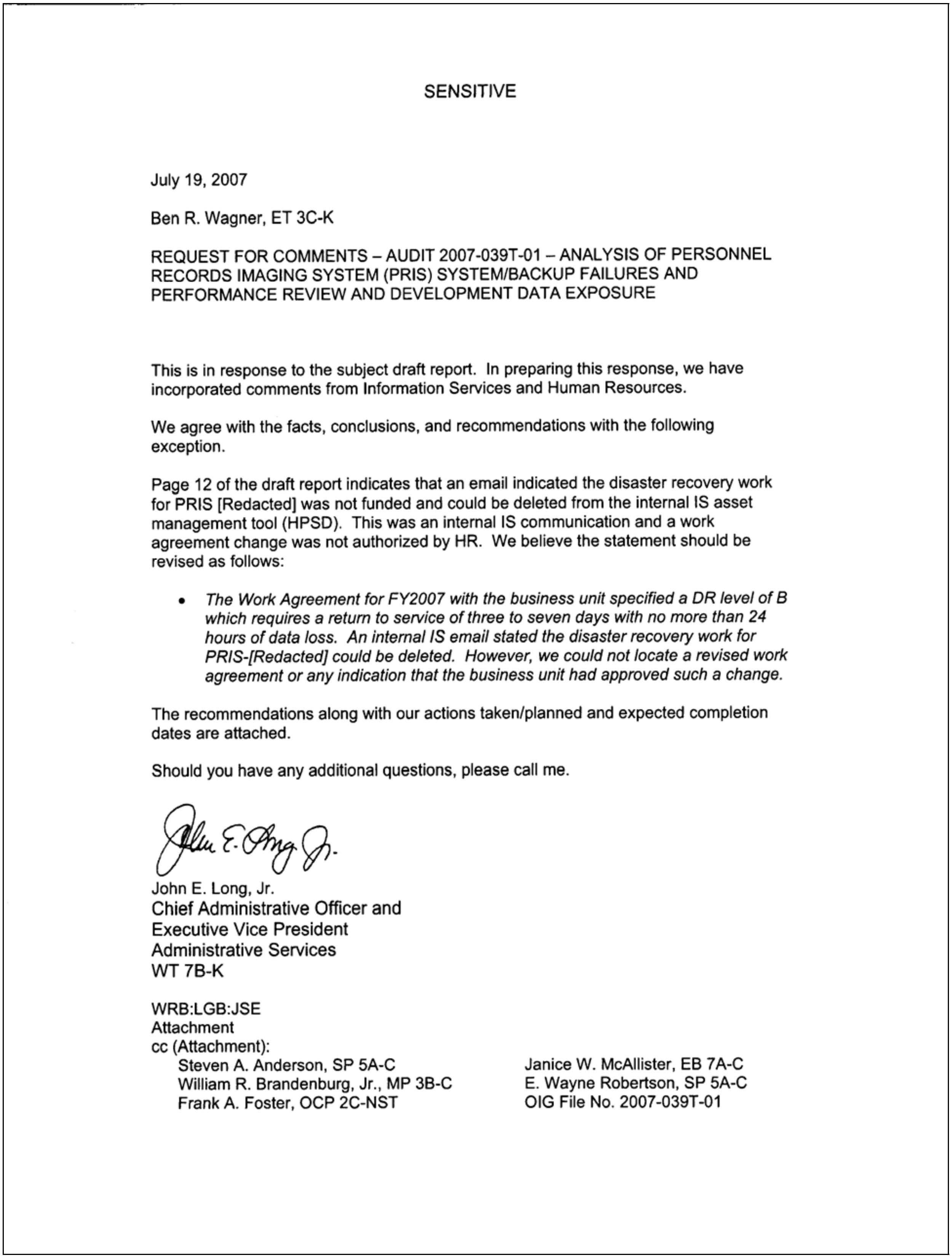
Recommendations (cont'd)

TVA Management's Comments (See Appendix for entire response)

The Executive Vice President, Administration, and Chief Administrative Officer, agreed with our facts, conclusions, and recommendations with one exception. Management provided revised wording regarding the PRIS-[Redacted] work agreement discussed on page 12 of the report.

Auditor's Response

We concur with management's proposed actions to implement processes to reduce the risk of future server and backup failures. We have revised the wording on page 12 based on management's response to the draft report.



SENSITIVE

July 19, 2007

Ben R. Wagner, ET 3C-K

REQUEST FOR COMMENTS – AUDIT 2007-039T-01 – ANALYSIS OF PERSONNEL RECORDS IMAGING SYSTEM (PRIS) SYSTEM/BACKUP FAILURES AND PERFORMANCE REVIEW AND DEVELOPMENT DATA EXPOSURE

This is in response to the subject draft report. In preparing this response, we have incorporated comments from Information Services and Human Resources.

We agree with the facts, conclusions, and recommendations with the following exception.

Page 12 of the draft report indicates that an email indicated the disaster recovery work for PRIS [Redacted] was not funded and could be deleted from the internal IS asset management tool (HPSD). This was an internal IS communication and a work agreement change was not authorized by HR. We believe the statement should be revised as follows:

- *The Work Agreement for FY2007 with the business unit specified a DR level of B which requires a return to service of three to seven days with no more than 24 hours of data loss. An internal IS email stated the disaster recovery work for PRIS-[Redacted] could be deleted. However, we could not locate a revised work agreement or any indication that the business unit had approved such a change.*

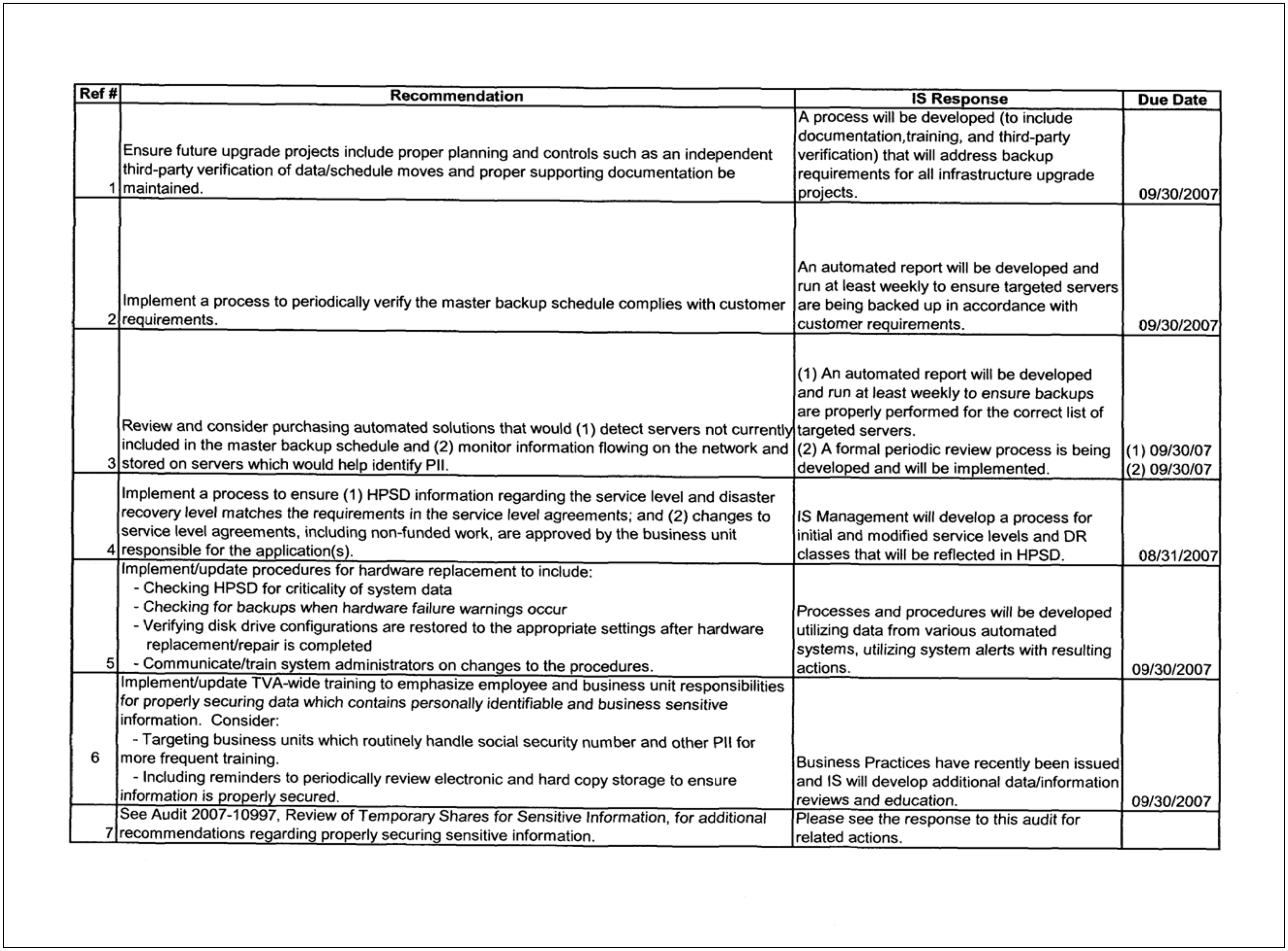
The recommendations along with our actions taken/planned and expected completion dates are attached.

Should you have any additional questions, please call me.

John E. Long Jr.

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

WRB:LGB:JSE
Attachment
cc (Attachment):
Steven A. Anderson, SP 5A-C
William R. Brandenburg, Jr., MP 3B-C
Frank A. Foster, OCP 2C-NST
Janice W. McAllister, EB 7A-C
E. Wayne Robertson, SP 5A-C
OIG File No. 2007-039T-01



Ref #	Recommendation	IS Response	Due Date
1	Ensure future upgrade projects include proper planning and controls such as an independent third-party verification of data/schedule moves and proper supporting documentation be maintained.	A process will be developed (to include documentation,training, and third-party verification) that will address backup requirements for all infrastructure upgrade projects.	09/30/2007
2	Implement a process to periodically verify the master backup schedule complies with customer requirements.	An automated report will be developed and run at least weekly to ensure targeted servers are being backed up in accordance with customer requirements.	09/30/2007
3	Review and consider purchasing automated solutions that would (1) detect servers not currently included in the master backup schedule and (2) monitor information flowing on the network and stored on servers which would help identify PII.	(1) An automated report will be developed and run at least weekly to ensure backups are properly performed for the correct list of targeted servers. (2) A formal periodic review process is being developed and will be implemented.	(1) 09/30/07 (2) 09/30/07
4	Implement a process to ensure (1) HPSD information regarding the service level and disaster recovery level matches the requirements in the service level agreements; and (2) changes to service level agreements, including non-funded work, are approved by the business unit responsible for the application(s).	IS Management will develop a process for initial and modified service levels and DR classes that will be reflected in HPSD.	08/31/2007
5	Implement/update procedures for hardware replacement to include: - Checking HPSD for criticality of system data - Checking for backups when hardware failure warnings occur - Verifying disk drive configurations are restored to the appropriate settings after hardware replacement/repair is completed - Communicate/train system administrators on changes to the procedures.	Processes and procedures will be developed utilizing data from various automated systems, utilizing system alerts with resulting actions.	09/30/2007
6	Implement/update TVA-wide training to emphasize employee and business unit responsibilities for properly securing data which contains personally identifiable and business sensitive information. Consider: - Targeting business units which routinely handle social security number and other PII for more frequent training. - Including reminders to periodically review electronic and hard copy storage to ensure information is properly secured.	Business Practices have recently been issued and IS will develop additional data/information reviews and education.	09/30/2007
7	See Audit 2007-10997, Review of Temporary Shares for Sensitive Information, for additional recommendations regarding properly securing sensitive information.	Please see the response to this audit for related actions.	

APPENDIX
Page 2 of 2