Memorandum from the Office of the Inspector General

May 30, 2008

E. Wayne Robertson, SP 5A-C

FINAL REPORT - SPECIAL PROJECT
REVIEW OF TVA'S PROCESS FOR HANDLING
LOST OR STOLEN COMPUTERS
OIG FILE NO. 20Z-315

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 me at (865) 632-3119 or Curtis D. Phillips, Supervisory Special Agent, at (865) 632-2584. We appreciate the courtesy and cooperation received from your staff during this review.

John E. Brennan
Assistant Inspector General
(Investigations)
ET 4C-K

CDP:JEB:MSW
Attachment
cc (Attachment):
William R. Brandenburg, Jr., MP 3B-C
Tom D. Kilgore, WT 7D-K
Ralph Edward King, WT 5A-K
Melissa A. Livesey, WT 5B-K
John E. Long, Jr., WT 7B-K
Janice W. McAllister, EB 5B-C
Gabrielle Anita Ratliff, WT 5B-K
Emily J. Reynolds, OCP 1L-NST
OIG File No. 20Z-315

Review of TVA's Process for Handling Lost or Stolen Computers

SPECIAL PROJECT – 20Z-315

May 30, 2008

Synopsis

- We initiated a special project to determine if (1) TVA's policies, procedures, and practices for handling lost or stolen computer equipment were adequate; (2) those policies, procedures, and practices were followed; and (3) the lost or stolen computers contained sensitive or restricted information. We found:
  - TVA's policies, practices, and procedures for maintaining an accurate inventory of computer equipment were not adequate. Since the August 2004 implementation of the HP Service Desk (HPSD), which contains an inventory of TVA computers, TVA has been unable to track over 5,550 computers. The inability to adequately track, as well as the lack of encryption, on these computers increases the risk for the disclosure of sensitive or restricted information.
  - The policies for handling/reporting stolen computers were not consistently followed.
  - At least one of the stolen computers contained personally identifiable information (PII)—employee social security numbers. We have not been able to confirm whether the remaining stolen computers contained sensitive or restricted information, although we believe the risk is moderate.

*"Sensitive and "restricted" information are defined in Business Practice 29. Sensitive information includes Safeguards information and restricted information includes PII.

Synopsis (continued)

- In a response to a draft of this report, management agreed with our recommendations, but disagreed with the characterization that TVA was unable to track over 5,000 computers. That response is attached.
- We disagree with management's position that they were able to track the computers in "lost" or "write-off" status. If management was able to track the missing computers, they should have recorded the correct status in HPSD, their inventory management system.

Objective, Scope, and Methodology

Objective

- The objective was to determine if:
  - TVA's policies, procedures, and practices for handling lost or stolen computer equipment were adequate
  - The policies, procedures, and practices were being followed
  - The lost or stolen computers contained sensitive or restricted information

Scope and Methodology

- Selected the period of May 1, 2006, to November 30, 2007, for the review of computers reported stolen to TVAP, information from HPSD for January and March 2008 showing the number of computers designated as "lost," and a change request for May 2006 showing the number of computers reclassified from "lost" to "write-off."
- Reviewed TVA's policy, procedures, and practices for handling computer security incidents which include the handling of computers reported stolen
- Reviewed the policy and procedures for maintaining records for personal computer life cycle in HPSD
- Consulted TVAP and HPSD to identify the universe of the lost or stolen computers
- Interviewed TVA employees who reported a computer theft to TVAP
- Interviewed Information Services (IS) senior managers responsible for HPSD

Background

How HPSD Tracks Inventory

- TVA utilizes HP Service Desk (HPSD) in conjunction with the System Management Server (SMS) to track the inventory and life cycle of computers. The system tracks configuration changes, service calls, software upgrades, and other information through the life cycle of a computer. Specifically:
  - SMS scans the network on regularly scheduled intervals to identify PCs connected to the network.
  - SMS passes the information it collects to HPSD.
  - If SMS does not find a device that was formerly on the network, it records the device as lost in SMS and maintains the record for 30 days.
  - When SMS deletes the record for the lost computer, HPSD changes the “Marked Lost Date” in its database to the current date, but continues to retain the current status of the computer.
  - After 60 days, HPSD changes the status of the computer to “lost.”
  - If the computer is reattached to the network and rediscovered by SMS, it is reentered in HPSD with a status of “production.”
  - A Change/Work Order is requested to change the status of a computer from production to “removed” when the computer is sent to Procurement to be retired (and subsequently surplused).
  - The status is changed to retired only when Procurement liquidates the computer.

Background (continued)

TVA Policy—Stolen Computers

- TVA's Computer Security Incident Handling Procedure and related training material define a computer security incident to include the theft of computer equipment
- The policy also establishes the following roles and responsibilities for handling computer thefts
  - End-user reports the theft to the IT Service Center (ITSC), IT Security, TVA Police (TVAP), or OIG
  - ITSC, TVAP, or OIG reports the incident to IT Security
  - IT Security staff:
    - May serve as the Incident Commander
    - Performs an initial assessment
    - Develops an incident response plan, if necessary
    - Maintains an incident database
    - Reports the incident, as appropriate

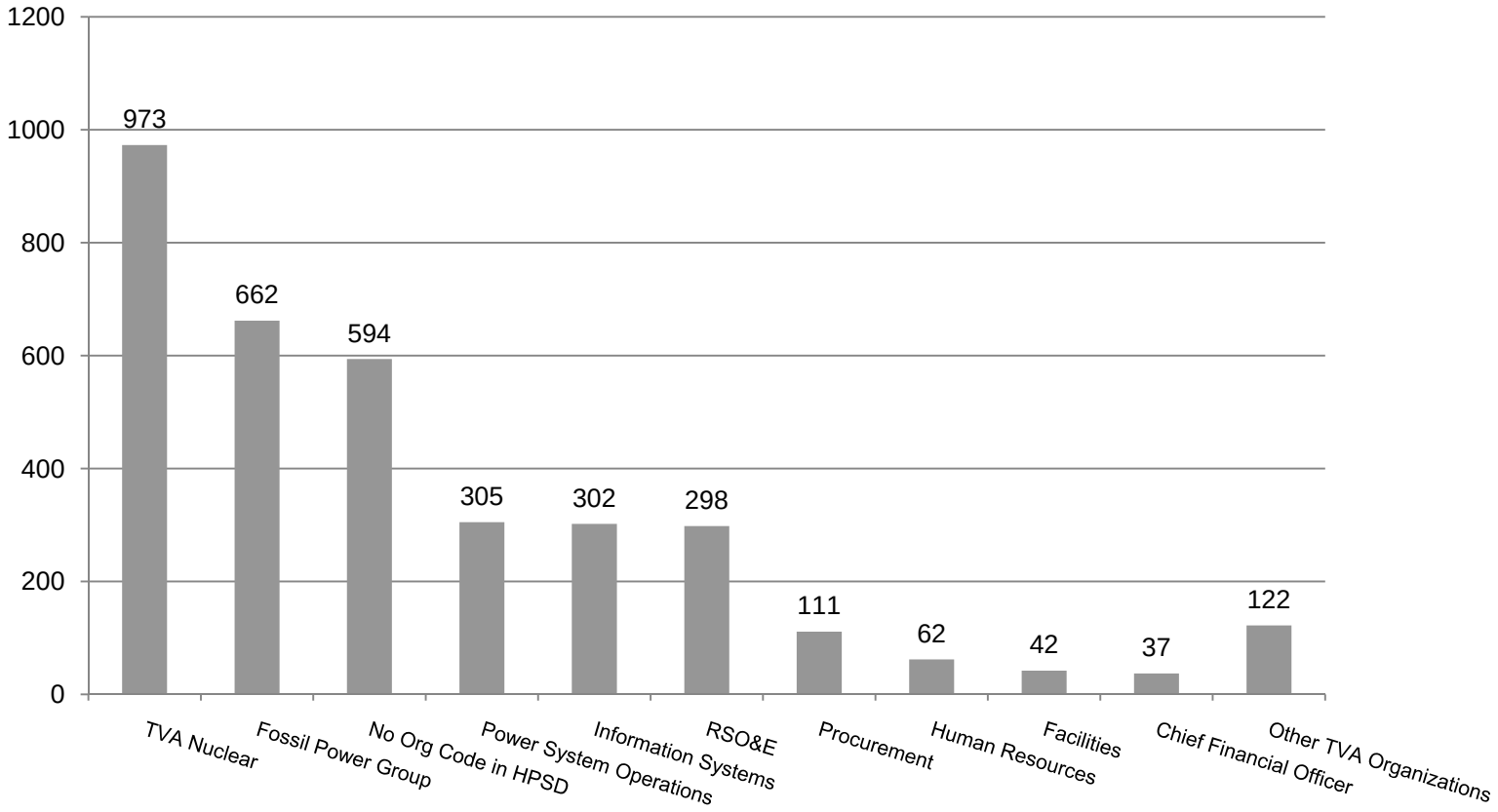
Finding 1—Inadequate Process for Tracking Computers

- TVA's policies, procedures, and practices for maintaining an accurate inventory record of personal computers in HPSD were not adequate. Since the August 2004 implementation of the HPSD, TVA has been unable to track over 5,550 computers.
  - IS personnel agreed their inventory process was not working correctly and stated a significant number of the computers classified as "lost" were misclassified
  - IS implemented HPSD in August 2004 to maintain an inventory and track the lifecycle of PCs on the network. Since that time:
    - IS moved 5,031 PCs from a "lost" status to a "write-off " status in May 2006.
      - Management defined "lost" status as PCs no longer connected to the network.
      - Management used the "write-off" status to record a one-time move of PCs from "lost" as management began to disposition for lifecycle management.
    - At the end of March 2008, HPSD reflects 3,014 computers in "lost" status and 2,536 in "write-off" status for a total of 5,550.

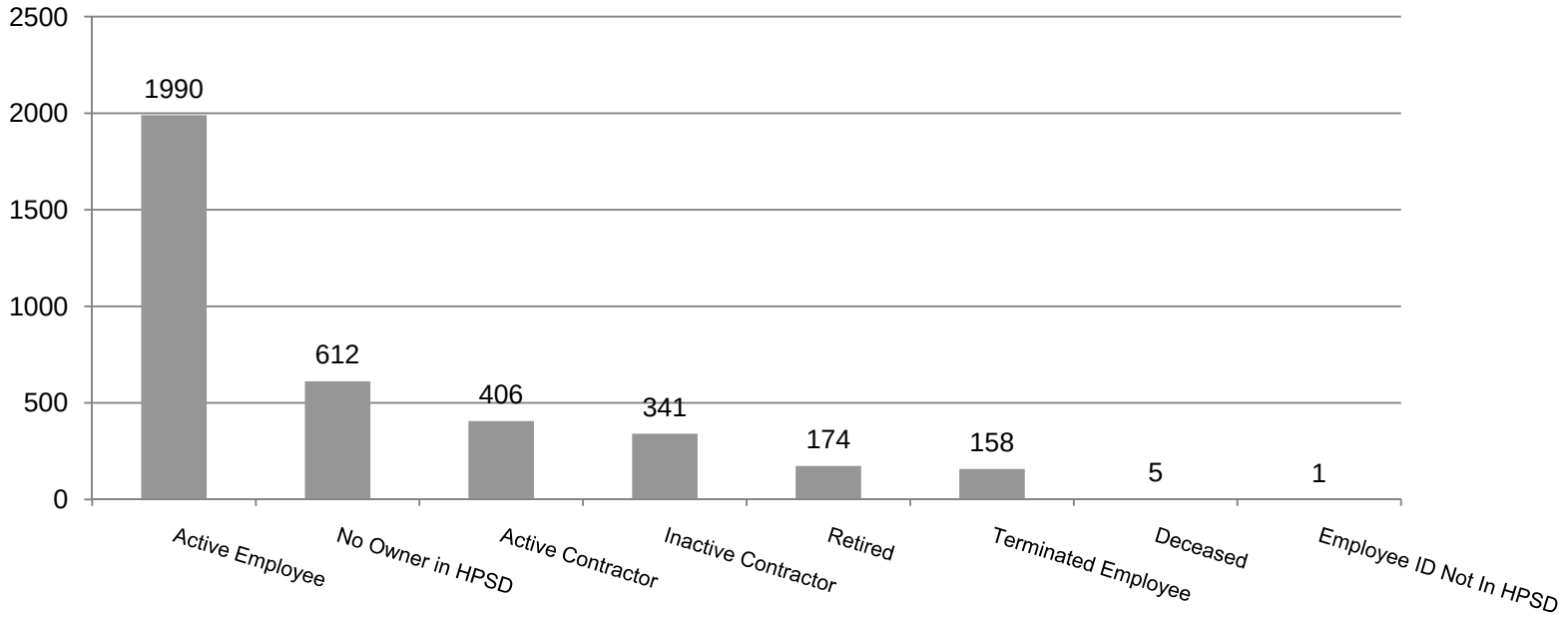
Finding 1—Inadequate Process for Tracking Computers (continued)

- In the attached response, management disagreed with the characterization that TVA was unable to track over 5,000 computers. Management advised the “lost” and “write-off” status were used only for lifecycle purposes and they would introduce a “not connected” status to better reflect the status of computers. Management further stated they had properly dispositioned 1,428 computers.
- We disagree with management’s position that they were able to track the computers in “lost” or “write-off” status. If management was able to track the missing computers, they should have recorded the correct status in HPSD, their inventory management system.

Summary of Computers with Lost Status by Organization Effective January 2008



Summary of Computers with Lost Status by Employee Status Effective January 2008



Finding 1—Inadequate Process for Tracking Computers (continued)

Reasons for Lost Status

- According to Senior IS managers, computers drop out of inventory or become misclassified for several reasons
  - They were returned to stock for reissuance
  - HPSD contains duplicate entries
  - HPSD was not updated correctly when computers were retired and sent to surplus
  - They were actually lost or stolen
  - They are held in Radiological Controlled Areas
  - Some of the computers may never have been on the network, such as:
    - Those held at the nuclear sites because they contain “Safeguards” information
    - Those behind firewalls in a process control environment
    - Those used as data acquisition devices

Finding 1—Inadequate Process for Tracking Computers (continued)

Planned Improvements to Inventory Process

- During our field work, IS initiated a review of the HPSD inventory process and developed a plan to improve the process. The plan addressed:
  - Improvements in the receiving process to ensure computers are recorded correctly in HPSD
  - Improvements to the retirement process to ensure computers sent to surplus are accurately recorded in HPSD
  - Improvements in the tracking and recovery process for computers disconnected for more than 30 days from the network
  - Clean up HPSD for cases where receiving procedures were not followed
  - Reconcile HPSD with surplus computer inventory, and work with owners to locate the remaining computers

Finding 2—Noncompliance with Procedures for Handling Stolen Computers

- TVA policies, procedures, and practices for handling computers reported as stolen were not followed
  - TVAP received reports that 26 computer-related items, such as laptops, desk-tops, PDAs, & computer screens, were stolen during the period May 1, 2006, to November 30, 2007
  - TVAP confirmed they generally did not notify IT Security when they received a report of a stolen computer
  - IT Security specialists did not recall TVAP notifying IT Security of any computer thefts
  - IT Security did not include the theft of computers in their computer security incident database and recalled receiving notification involving the theft of only one computer during the review period (May 2006 to November 2007) and they conducted an assessment of the information on the computer

Finding 2—Noncompliance with Procedures for Handling Stolen Computers (continued)

Planned Improvements for Handling Stolen Computers

- TVA is planning to roll out an encryption project which will help secure information on computers if they are lost or stolen
- IT Security has a draft policy on Computer Security and Privacy Incident Response which better defines the roles and responsibilities of those involved. However, the policy has been in draft for several years.
- After being contacted during this project ,TVAP distributed an e-mail to all TVAP Commanders reminding them to notify IT Security of all reported computer thefts
- IT Security is planning an awareness article for all TVA employees to be published in Inside TVA

Finding 3—PII and Sensitive Information on Stolen/Lost Computers

- One of the laptops reported stolen contained employee social security numbers because the user saved copies of employee service reviews completed prior to the implementation of employee identification numbers
- There is a moderate risk other sensitive or restricted information was disclosed on the computers reported stolen because:
  - The stolen computer users included a RAD Protection Manager, Nuclear Electrical Engineers Manager, Nuclear Electrical Maintenance Manager, and a Commercial Analyst
- The inability to track over 5,550 computers substantially increases TVA's risk for the disclosure of sensitive or restricted information. However, until a complete review of the computers classified as "lost" is conducted, we do not have sufficient information to know the extent of that risk.

Recommendations

- IS should:
  - Implement the planned improvement for the inventory process in HPSD
  - Implement the laptop encryption project
  - Initiate a project to locate the computers listed as lost in HPSD and perform a risk assessment to determine if any of the truly lost computers contained sensitive or restricted information
  - IS should develop a process to follow-up when the status of computer equipment moves to lost.
- Enterprise IT Security should:
  - Follow up and conduct a risk analysis on the computers reported as stolen
  - Finalize the draft policy on Computer Security and Privacy Incident Response
- TVA Management agreed with these recommendations and their planned actions are attached.

May 2, 2008

John E. Brennan, ET 4C-K

SPECIAL PROJECT
REVIEW OF TVA'S PROCESS FOR HANDLING
LOST OR STOLEN COMPUTERS
OIG FILE NO. 20Z-315

Our response to your request for a management decision regarding the findings of the subject report is attached. While we agree with the recommendations set forth in the subject report, we disagree with the OIG's characterization that Information Services is unable to track over five thousand PCs. As we've stated on numerous occasions, the statuses of "lost" and "write-off" were statuses available to us in our inventory tracking tool that were used for lifecycle purposes but were not indicative of their actual state. We will be introducing a "not connected" status to better reflect the status of these PCs. As of the date of this response, Information Services has properly dispositioned 185 of these PCs since the release of this report in addition to the 1,243 PCs that have been properly dispositioned since the beginning of this investigation. As stated in our detailed response, we will be working to properly disposition the remainder of these PCs.

We would also like to thank Curtis Phillips and you for the professionalism and cooperation in conducting this investigation. If you have any questions, please contact me or Gabrielle Ratliff, 865-632-7055.

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

WRB:JWM:JSE
Attachment
cc (Attachment):
William R. Brandenburg, Jr., MP 3B-C
Tom D. Kilgore, WT 7D-K
Ralph E. King, WT 5A-K
Melissa A. Livesey, WT 5B-K
John E. Long, Jr., WT 7B-K
Janice W. McAllister, EB 7D-C
Curtis D. Phillips, ET 4C-K
Gabrielle A. Ratliff, WT 5B-K
EDMS, WT CA-K

Appendix

Special Project
Review of TVA's Process For Handling Lost or Stolen Computers
OIG File No. 20Z-315

Recommended Action Step	Resp Dept	Lead	Action Planned	Estimated Complete
Implement planned improvement for the inventory process in HPSD.	IO	Sam Boozer	Management agrees. Planned improvements will be documented and implemented.	05/30/2008
Implement the laptop encryption project.	IO	Bill Brandenburg	Laptop encryption of My Documents folder was implemented on 3/26/2008. Any laptop that has been connected to TVA network since 3/26 has had the My Documents folder encrypted.	03/28/2008 - complete
Initiate a project to locate the computers listed as lost in HPSD and perform a risk assessment to determine if any of the truly lost computers contained sensitive or restricted information.	IO/EITS	Sam Boozer/Gabrielle Ratliff	Management agrees. A project has been initiated to perform and complete these tasks.	06/30/2008
IS should develop a process to follow-up when the status of computer equipment moves to lost.	IO	Sam Boozer	Management agrees. A process will be established.	05/30/2008
Follow-up and conduct a risk analysis on the computers reported as stolen.	EITS	Gabrielle Ratliff	Management agrees. EITS is working on streamlining the reporting of missing and/or stolen computer equipment so that the appropriate notifications are made in a consistent manner. EITS will issue an awareness article for all TVA employees.	05/30/2008
Finalize the draft policy on Computer Security and Privacy Incident Response.	EITS	Gabrielle Ratliff	TVA SPP 12.9 - Computer Security and Privacy Incident Response has been finalized and was sent to Human Resource Services on 4/15/2008 to be published.	05/05/2008