Simulator Security

Discovery

- On 03/30/12, a Clinton licensed operator accessing historical information from the Simulator Plant Process Computer (PPC), identified that the sequence of events (SOE) log from previous scenarios could be accessed.

- It was determined that this historical data was not being deleted (or written over) when the simulator initial conditions (IC) are reset, as expected. The initial corrective action was to manually delete the associated SOE files.

Initial Actions Taken

- Fleet Training Director call that evening determined that this condition was applicable to all of the Mid-West Simulators.
  - All simulators were placed in an exam security state and were disconnected from all external networks until the simulator PPC vulnerabilities were identified, assessed, and actions put in place to correct the issue.
  - The simulator Information Technologist (IT) group and fleet simulator peer group were informed and a short-term fix was implemented at Clinton, Quad Cities, and Dresden that deletes the historical data files from the Simulator PPC.

Initial Actions Taken

•The method was completed at Clinton and shared with each site’s Simulator Coordinator for implementation.

•Braidwood and Bryon were determined not to be affected by the SOE issue.

•The training director peer group concluded that no exam security compromise had occurred.

Initial Actions Taken

- Clinton station performed a prompt investigation to capture the event and communicate the actions taken.
  - Each of the Mid-West sites' simulators is affected by this interface with the simulator PPC.
  - The Mid-Atlantic sites have not completed the simulator PPC upgrade and do not have the ability to access historical data from the simulator "at the controls" area.
  - Determined that historical PPC computer point access would require a deliberate series of commands and specific knowledge of when exam material was being created and validated. (Malicious Intent required)

NRC Interface

- Dresden and Quad Cities Station identified their issue via a white paper that specified that the simulator PPC SOE message log file does not get cleared out upon IC reset as expected. (Due to ILT Exams in progress.) These papers were presented to NRC Region 3.
- During the NRC's recent 71111.11 inspection, Dresden station was given a preliminary Licensee Identified Violation of 10 CFR 55.49 "Integrity of Examinations and Tests" for the potential simulator exam security issue.

CAP

Individual Site Assessment of Event	
Site	IR(s)
Braidwood	1350393
Byron	1350674
Clinton	**1348127**, 1349731
Dresden	1348182
LaSalle	1350492
Limerick	1350863
Oyster Creek	1349638
Peach Bottom	1350941
Quad Cities	1348733
Three Mile Island	1349463
ACE	1351002

Completed Actions

- Corporate IT developed a plan and timeline to address these issues and long-term strategies to automatically delete these files.
  - The Fleet Simulator IT group has created a solution that automatically removes all files when the initial conditions are reset following a simulator scenario. This has been implemented at all Exelon sites.

ACE Actions

- Revise TQ-AA-306 and TQ-AA-1252 to require the Simulator Coordinator and the IT-SA to both screen simulator design changes for potential impact on exam security and ensure that vendor documents (if applicable) address exam security.

- Revise simulator design change “template” scoping documentation or contract wording to include exam security information review.

- Communicate to Sim Coordinators via the Center of Excellence to ensure exam security reviews are addressed and documented for all changes currently in progress. Information in progress tracking mechanisms should be discussed with vendors.

- Communicate to all vendors currently performing simulator design changes to communicate to the Simulator Coordinator and IT-SA on all issues and exam security information. Information in progress tracking mechanisms should be discussed with the site.

- Evaluate the site specific simulator exam security checklist for revision. Verify that during exam related activities in the simulator all remote LAN accessibility is disconnected.

- Provide informal training to all Simulator Coordinators on Site and Corporate IT roles and responsibilities to include interface expectations.

- Issue a Yellow NER for the event discussed in ACE 1351002.