NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Loss of EMS – IT Communications Disabled

Primary Interest Groups
Generator Operator (GOP)
Reliability Coordinator (RC)
Transmission Operator (TOP)
Transmission Owner (TO)

Problem Statement
Transmission System Operators lost abilities to authenticate to the EMS system, resulting in a loss of monitoring and control functionality for more than 30 minutes.

Details
Scheduled control center server maintenance was being performed, which required the local authentication server to be taken out of service. By design, control center EMS application authentication should have rerouted automatically to a remote authentication server when the local server was taken out of service. Contrary to expectations and design, the automatic rerouting of authentication traffic did not occur and the EMS application was impacted.

As a result, maintenance on the local authentication server was curtailed and was brought back on-line. Once local authentication was re-established, full EMS functionality was available.

The root cause analysis determined that a specific firewall policy allowing authentication failover from the local authentication server to the remote authentication server was inadvertently deleted.

Corrective Actions
The following corrective actions were implemented:

- IT and business teams worked together to develop a test plan template to ensure that application functionality would be retained and supporting infrastructure components would function as designed.
- The IT Change Management process was immediately modified to ensure that comprehensive test plans are executed regardless of change classification. The past practice for work believed to be low risk was to allow test plans as a streamlined process when implementing a change. The prior streamlined process for low-risk firewall policy changes required only that an engineering analytical review be performed. IT personnel were retrained on a revised Change Management process that included, but was not limited to, use of comprehensive test plans for all change classifications.
- A redundant local authentication server was installed at the primary control center.

Lesson Learned

- EMS network design should, where possible, include a redundant local authentication server on the same internal network as the primary local authentication server. Having the primary and redundant local authentication servers on the same internal network (i.e., behind the same firewall) eliminates the dependency on a firewall rule for internal communications to both the primary and redundant local authentication servers.
- The IT Change Management process should consider applying the following principles:
  - Apply a thorough test process that is reviewed with the client for all changes that could affect EMS function.
  - Test the design redundancy or back-out plan prior to implementing a change.
  - Test plans need to be comprehensive and include regression-level testing.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the Bulk-Power System. NERC requests your input on this lesson learned by taking the short survey provided in the link below:

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	NPCC – Event Analysis
Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	20131001
Date Published:	October 29, 2013
Category:	Communications

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.