

**CYBER SYSTEMS
ASSESSMENT TEMPLATE**

AM-CE-P034-R1075

Rev. 2

This document contains specific content that has been or will be used as "Evidence of Compliance" for regulatory audits. Any person(s) making revisions to this document shall contact the T&S Engineering Manager, T&S Compliance Analyst and the Exelon NERC Compliance and Security NERC

Cyber Systems						
Component Classification Categories						
Criticality	I		X			High Impact BES Cyber Systems
	II			X		Medium Impact with External Routable Connectivity (ERC) BES Cyber Systems ^③ and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Assets (PCA)
	III				X	Medium Impact without ERC BES Cyber Systems ^③ and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Assets (PCA)
	IV					X All other Cyber Systems and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Assets (PCA)
Duty Cycle	Heavy Load	N/A	N/A	N/A	N/A	
	Normal Load	N/A	N/A	N/A	N/A	
Service Condition	In Service	X	X	X	X	
	Spare	N/A	N/A	N/A	N/A	
Condition Monitoring Tasks		Task Frequencies			Failure Codes^①	Comments
None	N/A	N/A	N/A	N/A		
Time Directed Tasks		Task Frequencies			Failure Codes^①	Comments
On-Site Assessments for Paper Vulnerability Assessment (with ERC)	N/A	1Y ^②	N/A	N/A		
On-Site Assessments for Paper Vulnerability Assessment (without ERC)	N/A	N/A	1Y ^②	N/A		
Failure Finding Tasks		Task Frequencies			Failure Codes^①	Comments
None	N/A	N/A	N/A	N/A		
Condition Directed Tasks		Task Frequencies			Failure Codes^①	Comments
None	N/A	N/A	N/A	N/A		

① For items covered under the CIP Reliability Standards, time-based activities are performed according to minimum assessment activities and the maximum required intervals prescribed in the tables of applicable CIP standard.

② For items defined under the CIP Reliability Standards, interval for the utility's On-Site Assessments for Paper Vulnerability Assessment is 1Y with no grace to ensure compliance with the maximum required interval of 15 calendar months for the utility's Paper Vulnerability Assessment.

③ As defined per NERC Standard CIP-002 BES Cyber System Categorization reliability standard.

FAILURE MODE

FAILURE CAUSES

MAINTENANCE TASKS

**INTENTIONALLY
BLANK**

**CYBER SYSTEMS
ASSESSMENT TEMPLATE**

TASK	DEFINITION
Paper Vulnerability Assessment (without ERC)	Tasks to be executed as detailed in the NERC CIP Vulnerability Assessment Procedure (RC-AC-PCD3-013) and governed by the NERC CIP Vulnerability Assessment Process (RC-AC-PCS3-011)
Paper Vulnerability Assessment (with ERC)	Tasks to be executed as detailed in the NERC CIP Vulnerability Assessment Procedure (RC-AC-PCD3-013) and governed by the NERC CIP Vulnerability Assessment Process (RC-AC-PCS3-011)

**CYBER SYSTEMS
ASSESSMENT TEMPLATE**

Cyber Systems

Cyber Systems Assessment Template documents the tasks and frequencies for executing cyber system assessments as established in Exelon's NERC CIP Compliance Process NERC CIP Vulnerability Assessment Process (RC-AC-PCS3-011) and NERC CIP Vulnerability Assessment Procedure (RC-AC-PCD3-013). This assessment template has been developed to address NERC CIP equipment that is owned and maintained by ComEd. Aspects of the Preventive Maintenance Process including Run-to-Failure Analysis, Duty Cycle, Operating Environment, Failure Modes, Failure Causes and Equipment Failure Analysis Feedback are not applicable. In addition, tasks described within this document are assessment activities and not to be considered as operational preventive or predictive maintenance tasks.

References:

- CIP-002 - Cyber Security - BES Cyber System Categorization
 - CIP-005 - Cyber Security - Electronic Security Perimeter(s)
 - CIP-006 - Cyber Security - Physical Security of BES Cyber Systems
 - CIP-007 - Cyber Security - System Security Management
 - CIP-010 - Cyber Security - Configuration Change Management and Vulnerability Assessments
 - RC-AC-PCD3-013 NERC CIP Vulnerability Assessment Procedure
 - RC-AC-PCS3-011 NERC CIP Vulnerability Assessment Process
-

Boundary Definitions

The boundary of the Vulnerability Assessment for the purpose of this document is defined to include the on-site assessments, data gathering, and analysis of assessment activity in addition to finalizing the Vulnerability Assessment Report and Remediation Plans for all applicable ComEd owned equipment.

Failure Experiences

n/a

**CYBER SYSTEMS
ASSESSMENT TEMPLATE**

Vendor Recommendations

n/a

Disposition of Vendor Recommendations

n/a

Basis for Maintenance Tasks

Maintenance tasks and intervals established to comply with NERC CIP-010 Cyber Security - Configuration Change Management and Vulnerability Assessments so that Cyber Systems are kept in working order.

**CYBER SYSTEMS
ASSESSMENT TEMPLATE**

Revision 0		Date 10/31/2016
Writer	Kevin Swiat (ComEd)	
Reviewer(s)	Bill Pakosz (ComEd), Pooja Rajoria (ComEd), Mike Scannell (ComEd), Jeff Nagel (ComEd), John Hansen (TSC)	
Approver(s)	Michael Moy (ComEd) Preventive Maintenance UFAM	
Reason Written	Initial maintenance template development.	

Revision 1		Date 3/17/2017
Writer	Kevin Swiat (ComEd)	
Reviewer(s)	Jeff Nagel (ComEd), John Hansen (TSC)	
Approver(s)	Michael Moy (ComEd) Preventive Maintenance UFAM	
Reason Written	Revise note to specify that tasks contained within the document are assessment activities and not to be considered as operational preventive or predictive maintenance tasks.	

Revision 2		Date 3/17/2019
Writer	Kevin Swiat (ComEd)	
Reviewer(s)	Jeff Nagel (ComEd Testing Group); Kyle Spesard (ComEd Testing Group); Kash Dave (ComEd Testing Group); Olive Millan (ComEd Testing Group); Irfan Khan (ComEd R&PE); John Hansen (NERC CMT)	
Approver(s)	Michael Moy (ComEd) Preventive Maintenance UFAM	
Reason Written	Updated "Cyber Systems" and "Development History" tab header to be "Assessment Template"; Added document number and page numbers to all tab footers; Updated documents to reference Exelon's NERC Compliance Management Team (NERC CMT); Updated Task Definitions to reference the NERC CIP Vulnerability Assessment Process and Procedure for details; Modified "Maintenance Basis" tab label to be "Basis"; Revised basis statement at top of "Basis" tab to reference the NERC CIP Vulnerability Assessment Process and Procedure; Added reference to RC-AC-PCS3-011 NERC CIP Vulnerability Assessment Process; Completed 2-year periodic review.	