Cyber Security Control Testing: Centralized Control System
Draft V0.0 December 13, 2019

The following control tests are designed to verify that implementation of cyber security protections for the Centralized Control System are in compliance with the PPPL Cyber Security Program Plan (CSPP) and best practices for protection of PPPL Information Technology systems and data.

Cyber Control Family	Test	Test Results
Risk Management	Categorize the system based on FIPS 199 (Low, Moderate) and assign to the appropriate cyber security system and subsystem	Moderate risk designation agreed after discussions held on Jan 8 2020.
Risk Management	Produce an inventory of IT hardware and software components to be included in this system	A complete inventory will be produced as part of the FDR documentation.
Risk Management	Define interconnects required with other internal and external networked systems.	Interface definitions are included as part of the requirements and specification documents for these systems and will be included in design reviews.
Privacy	List known categories of PPPL data to be stored in the Centralized Control System, including future enhancements/additions.	Process data? Also being sent to OPC but does that qualify for this or covered by that system
Privacy	Perform standard DOE Privacy Needs Assessment, and if required, full Privacy Impact Assessment	
Access Control	Verify vlan assignment and proper network segmentation for all servers	
Access Control	Verify the use of PPPL Active Directory for user accounts, administrator accounts, and account passwords.	
Access Control	Review system and application administrator accounts for least privilege.	

Cyber Security Control Testing: Centralized Control System
Draft V0.0 December 13, 2019

Access Control	Review use of any non-AD local, system, or service accounts in servers or vendor application.	Local accounts for the Rockwell software (FactoryTalk View and Studio 5000) will be managed by PI&C
Access Control	Review need for firewall access controls, including for remote (offsite) access	No offsite access is planned at this time.
Audit and Accountability	Review system logging implementation and need for forwarding to central server and/or splunk	The data server will act as a central log server and will have the splunk agent installed.
Audit and Accountability	Review application logging implementation and need for forwarding to central server and/or splunk	The data server will act as a central log server and will have the splunk agent installed.
Awareness Training	Review plans for user security awareness training and policy for restricting storage of Protected PII and other sensitive data	Users will be required to take PPPL Cyber training. There is no plan to store PII or other sensitive data on the system.
Security Assessment and Authorization	Determine the need for PSO cyber authorization approval and obtain approval if needed	NEED MORE INFO - not sure of implications
Configuration Management	Verify configuration of the server OS and use of standard configuration baseline or best practices	There is no server OS, Windows 10 on rack-mount PC. Updates will be managed by IT
Configuration Management	Verify configuration of web server(s) and use of standard configuration baseline or best practices	There are no plans for web server use
Configuration Management	Verify configuration of application and use of standard configuration baseline or best practices	Application is custom and there is no standard available. Best practices will be used in its development and the system will undergo period cyber security scans. Software Quality Assurance procedures will be followed where applicable for an A3 system.

Cyber Security Control Testing: Centralized Control System
Draft V0.0 December 13, 2019

Configuration Management	Review vendor system/application change management process	Will use scn.pppl.gov for change management process (applications). IT must give access to Developers/admins of FLARE
Contingency Planning	Verify periodic PPPL backups of system and user data are in place.	Periodic Clonezilla backups of systems (by I&C group) and Netbackup with appropriate backup policy set for experimental data
Contingency Planning	Review and update contingency plan for system rebuild/disaster recovery capabilities.	Clonezilla will provide bare metal restoration capability, incremental backups by netbackup will ensure system and experimental data are retrievable
Identification and Authentication	Verify all default vendor/system passwords are identified and changed.	**Defer**. Once purchased and on hand.
Identification and Authentication	Verify implementation of 2-factor authentication for system administrators.	
Identification and Authentication	Verify implementation of 2-factor authentication for users and application administrators.	
Media Protection	Review vendor policy for encryption and protection of data at rest, data on backup devices, etc. (FIPS 140-2 compliant?)	No PIII will be present in system, experimental and configuration data has no requirement for this at this time.
Physical and Environmental Protection	Review physical location of servers, physical access controls, use of UPS and/or dual power feeds, backup power capabilities, fire protection, etc.	Panel in control room, locked with unique key, access controlled by procedure. The control cabinet has a UPS power feed
Planning	Update cyber system security plan with system description, drawings, etc	**Defer** After FDR, and build-out
Risk Assessment	Perform network vulnerability scanning according to policy	OK, will ask to be added to periodic cyber security scans

Cyber Security Control Testing: Centralized Control System
Draft V0.0 December 13, 2019

Risk Assessment	Perform application vulnerability scanning according to policy	OK, will ask to be added to periodic cyber security scans
System and Communications Protection	Verify use of encrypted protocols for administrator and user web-based access (HTTPS), remote login access (e.g. RDP), etc	No plans to utilize remote access
System and Communications Protection	Verify use of encrypted protocols (e.g. latest version of TLS) for in transit network communications between web server, application server, file server, and database server.	Data transfers between control systems nodes will take place on NSTX Control Systems VLAN. Data will be transmitted one way to OPC server.
System and Communications Protection	Verify use of AES-256 encryption for data at rest	No PII, no requirement for encryption.
System and Information Integrity	Verify deployment of anti-malware protections on servers	Unclear what we need here
System and Information Integrity	Review server patching policy and procedures	No servers in use in system.
System and Information Integrity	Review application patching policy and procedures	OK. Will follow best practices for patching control, experimental data servers and operator terminals for experimental devices.
System and Information Integrity	Review intrusion detection/prevention policy and capability	Cabinet will have door switches to monitor any access events, and uniquely keyed fasteners to prevent entry,
PPPL Custom	Verify format of user/admin emails generated by application(s) for phishing recognition including sender/recipient and email content	No email capability is envisioned for the system.