

	A	B	C	D	E	F	G
1	 NORTHEAST POWER COORDINATING COUNCIL, INC. 1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782						
2	Standard	Req.	NPCC Root Cause	EA Cause Code	PNC	AOC	Finding Description
3	CIP-005	R1	2	A3B2C05	X		Entity did not have all applicable Cyber Assets that were connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). There were two network switches (sw1, sw2) that were configured with VLANs that were both inside and outside of the ESP. vlan1 was inside the ESP. vlan2, vlan3 and vlan4 were outside the ESP.
4	CIP-011	R1	5	A4B1	X		Entity failed to implement its Information Protection procedures for classifying and marking eight (8) System Baseline Configuration spreadsheets that contain BES Cyber System Information as NERC Confidential.
5	CIP-011	R1	5	A4B1	X		Entity failed to implement its Information Protection procedures for classifying and marking eight (8) System Baseline Configuration spreadsheets that contain BES Cyber System Information as NERC Confidential.
6	CIP-010	R4	10	A5B2		X	Entity has implemented a program for ongoing management of Transient Cyber Assets. However, the audit team discovered several Transient Cyber Assets that were candidates to be included in the program under certain circumstances.
7	CIP-002	R1	6	A4B4		X	Based on the "misuse" scenario discussed and Entity's current operating practice, the Control Room phone System is a BES Cyber Asset.
8	CIP-002	R1	6	A4B4		X	Based on the operating capabilities of the entity control rooms, Entity should consider criterion 1.3 of Attachment 1 in its CIP-002 categorization process.
9	CIP-010	R3	10	A5B3		X	The decision criteria used to identify vulnerabilities requiring remediation are not documented.
10	CIP-010	R3	10	A5B2		X	Ensure that documentation used to demonstrate compliance accurately reflect the requirements of the standard, i.e., Doc1, Doc2 and Doc3.
11	CIP-011	R1	5	A4B1		X	Ensure third party developed documents that contain BES CSI are identified and labeled in accordance with Entity's Information Protection Program.
12	CIP-005	R1	2	A3B2C05		X	Re-evaluate the classification of layer two devices that are capable of operating at layer three and above, i.e., EACMS vs. PCA.
13	CIP-005	R1	2	A3B2C05		X	Entity should identify all Electronic Access Point (EAP) interfaces as the specific port(s) used for controlling inbound/outbound access to an ESP. The NERC Glossary of Terms states that EAPs are Cyber Asset interfaces on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
14	CIP-010	R3	10	A5B2		X	Ensure vulnerability assessments address all requirements of R3.
15	CIP-003	R1	10	A5B1		X	The organization, outline and overall construction of the Doc4 is insufficient in addressing all of the Requirements (1.1.1 through 1.1.9) and specifically CIP Exceptional Circumstances.
16	CIP-010	R3	10	A5B2		X	Ensure vulnerability assessments address all requirements of R3.
17	CIP-005	R1	2	A3B2C05		X	The ESP diagrams, which were submitted to demonstrate compliance with R1.1, were not well maintained.
18	CIP-005	R1	6	A4B4		X	Firewall rules lacked clear business justifications that reflected the current environment, and were likely too permissive .
19	CIP-010	R3	9	A4B3		X	Vulnerability Assessment action plans were not well maintained and lacked clear ownership.
20	CIP-007	R2	1	A4B5		X	The delayed patching of Device servers (caused by a prolonged procurement process), provided remote access to substation assets.
21	CIP-004	R5	6	A4B4	X		An employee that was transferred internally had access to 6 shared IDs but only 4 of the 6 passwords were reset within 30 calendar days following the date that the individual no longer required retention of that access.
22	CIP-011	R1	2	A3B2C05	X		Certain Medium Impact data that is required to be protected as "Confidential-CIP", Entity Floor Plans of Relay and Control Enclosures and Network Diagram of BES Cyber Systems (Communication Block Diagrams), were being stored in the Entity's corporate Folder. This folder does not have access properly restricted for BES Cyber System Information designated as "Confidential-CIP". The information was not properly stored in an Entity designated CIP repository in accordance with Entity procedures. The cause identified was Human Error because Information Owners believed that the Entity corporate folder had restricted access limited only to CIP cleared users.
23	CIP-007	R5	14	A3	X		A TFE was not filed with the Entity by the CIP version 6 effective date in Area1 (Date1) for devices that could not meet the requirement to limit the number of unsuccessful authentications, or generate alerts after a threshold of unsuccessful attempts was reached. Subsequently, a TFE was filed with the Entity on Date2. The device types covered by the TFE are Device1, Device2, Device3, Device4, and Device5.
24	CIP-007	R4	6	A4B4	X		Server Device1, which is one of two servers that make up the Entity Physical Access Control System (PACS), was not reporting in to the Device2 system. Consequently, event logs were not retained for the 90 consecutive days required. It was discovered that, during the initial roll-out, Device1 was not installed correctly on this asset. Once the project was completed and the CIP v5 program was running, multiple changes were made to the servers where the security controls were validated. During these validations, random samples were used to test controls and this server was never selected for testing. Human error was identified as the cause in the following areas: 1) The initial confirmation and implementation, 2) The testing done on a per change basis, 3) The quarterly certifications.
25	CIP-010	R1	14	A3	X		Software was removed from a Cyber Asset without proper authorization of baseline configuration change. The cause of this condition was human error.
26	CIP-010	R1	10	A5B2	X		The baseline configuration documentation was not updated within 30 calendar days after a change. Software on an EACMS device that was part of an Intermediate System was upgraded on Date1. On Date 2 it was discovered that the baseline configuration documentation had not been updated with the new version.
27	CIP-007	R5	2	A3B2C05	X		Entity did not change known default passwords, per Cyber Asset capability at Medium Impact Substations. Entity's states that Entity has made a business decision to not change the default passwords on Cyber Assets within Substations (Doc1). This was confirmed by the SME. CIP Standard 007-6 Requirement 5.4 does not allow for exceptions based on business decisions.

	A	B	C	D	E	F	G
1	 NORTHEAST POWER COORDINATING COUNCIL, INC. NPCC, Inc. 1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782						
2	Standard	Req.	NPCC Root Cause	EA Cause Code	PNC	AOC	Finding Description
28	CIP-005	R2	2	A3B2C05	X		Entity does not utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access (IRA) does not directly access an applicable Cyber Asset. Entity's IRA implementation is based on client VPN tunnel connections originating outside of the ESP to an Applicable Cyber Assets inside of the ESP. IRA sessions could be established from IT assets on the corporate network via an ESP firewall VPN as well as from the control systems vendor via a dedicated VPN router. Entity's implementation does not include an Intermediate System (jump host) outside of the ESP. As a result, Entity did not utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access (IRA) does not directly access an applicable Cyber Asset.
29	CIP-007	R2	1	A4B5	X		Entity did not include at least 3 Applicable Cyber Assets in their patch management process. A comparison between switch firmware versions and those currently offered by the vendor demonstrated that 3 sw3 switches (Medium Impact BCAs) were not receiving current firmware updates. These switches were not included in Entity's patch management process.
30	CIP-002	R1	6	A4B4		X	The operators' VOIP phone system is currently categorized as a Cyber Asset not a BES Cyber System. However, Entity's operating practices do not provide for an independent assessment of emergency orders given over the phone system. So the phone system may be susceptible to misuse. Consequently, it should be categorized as a BES Cyber System and protected accordingly to mitigate potential misuse scenarios.
31	CIP-010	R4	9	A4B3		X	Entity's TCA management plan appeared to be implemented in an on-demand manner as opposed to an on-going manner, as stated in evidence.
32	CIP-005	R1	2	A3B2C05		X	Entity has not clearly identified Electronic Access Points.
33	CIP-010	R3	10	A5B2		X	Ensure the documented cyber vulnerability assessment process addresses all applicable systems as required by CIP-010-2, R3.
34	CIP-005	R1	2	A3B2C05		X	Entity had not clearly identified Electronic Access Points (EAP). Rather, Entity had identified entire Cyber Assets as EAPs instead of the network interfaces.
35	CIP-005	R1	2	A3B2C05		X	The LAN extension interfaces between the primary and backup control center ESPs are not configured to transmit routable communication and so they do not meet the NERC Glossary definition of an Electronic Access Points (EAP). However, Entity has categorized the interfaces as EAPs. Technically since these interfaces are considered EAPs and are associated with Control Centers, Entity is required to implement one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications, which they have not done.
36	CIP-008	R2	10	A5B2		X	Cyber Security Incident Response Plan exercise reports lacked details of the discussions and proposed steps as they relate to the Plan. Also, the exercise frequency exceeded the 15 month requirement by two months.
37	CIP-003	R4	10	A5B2		X	Requirement 4 of CIP-003-6 requires the Responsible Entity to implement a documented process to delegate authority. Although the Delegation Form that was provided as evidence was acceptable, the procedure defining the process needs to be updated to Version 5.
38	CIP-003	R1	10	A5B1		X	Auditors noted that during examination of various program documents several contained terminology referencing CIP Version 3 Standards and Requirements, incomplete sentences and did not contain approval signatures by the responsible program manager. These issues call into question the validity of these documents which could lead to Potential Noncompliances in the future.
39	CIP-010	R3	9	A4B3		X	Whenever a cyber vulnerability assessment is performed, ensure that the documented scope of work is reconciled against the work that is actually completed.
40	CIP-005	R1	2	A3B2C05	X		The entity had firewall rules that were overly permissive, allowing inbound connections from four class C subnets to any device in the substation (blank destination address in Device configuration) as well as outbound connections from any device in the substation (blank source address in Device configuration) to four class C subnets. The entity stated it could not deploy detailed firewall rules, i.e., one rule per BCA for every inbound/outbound traffic flow, as the Device devices would run out of memory and cause a performance issue with substation/control center communications. Entity could not provide evidence to support this claim (performance impact tests records, vendor documentation, etc.) As a result, Entity did not provide a valid reason granting access to "ANY" source and/or destination addresses at Medium Impact Substations.
41	CIP-007	R1	5	A4B1	X		Entity13 notified the audit team that its configuration monitoring tool (Device1) identified discrepancies between the actual network accessible logical ports on 23 Device2 Cyber Assets and the documented baseline configurations. However, Device1 did not present the discrepancies for processing (by IT operators) in the daily exception reports. Therefore, Entity had network accessible logical ports that were needed, but were not documented or justified as required by R1.1.
42	CIP-005	R1	14	A3	X		Entity failed to identify four Electronic Access Points (EAP) on four High Impact BES Cyber Assets. These unidentified EAPs provided External Routable Connectivity (ERC) into the main ESP from non-ESP networks. The potential noncompliance ended when the Entity moved these connections fully inside the main ESP. The connections between the four network switches are now fully contained within the main ESP. As a result, the network switches covered by the potential noncompliance no longer contain EAPs. The root cause of this potential noncompliance was Entity did not identify these connections as providing ERC to the main ESP. Entity stated that this was due to a human error that occurred when reconciling ESPs and VLANs.
43	CIP-002	R1	2	A3B2C05	X		Requirement 1 of CIP-002-5.1 requires the Responsible Entity to identify high and medium impact BES Cyber Systems at each asset, and identify those assets that contain low impact BES Cyber Systems. In this case, Entity's procedures were based on Version 3 of the CIP Standards. Therefore, their identification process for BES Cyber Systems was not correct.
44	CIP-002	R2	6	A4B4	X		Requirement 2 requires the Responsible Entity to review the identifications made in Requirement 1 and have its CIP Senior Manager or delegate approve the identifications required by Requirement 1 at least once every 15 calendar months. In this case, Entity had not made the identifications necessary for Requirement 1 and therefore did not have the CIP Senior Manager review and approve the identifications required by CIP-002-5.1.
45	CIP-003	R3	7	A4B1C04	X		Requirement 3 of CIP-003-6 requires the Responsible Entity to identify a CIP Senior Manager by name, and document any change within 30 calendar days of the change. In this case, Entity's earliest designation of a CIP Senior Manager was five months after required by the Standard based on the effective date of the Standard.

	A	B	C	D	E	F	G
1	 NORTHEAST POWER COORDINATING COUNCIL, INC. NPCC, Inc. 1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782						
2	Standard	Req.	NPCC Root Cause	EA Cause Code	PNC	AOC	Finding Description
46	CIP-007	R5	5	A4B1	X		Entity discovered 91 accounts with passwords that had not been changed in the last 15 months. This Device1 is used for identification and authentication to nine Cyber Assets of the Device2. It does not natively record the date of last password change. With the Device1 technology currently in place, it is not technically possible to enforce user password changes. Although Entity has a procedure for tracking password changes, this procedure was not applied to the Device1 accounts.
47	CIP-005	R2	2	A3B2C05	X		An Intermediate System is logically located inside of an identified ESP. The network diagram indicates that the Jumpbox host (Device1), an identified Intermediate System, is inside of the Network1 ESP. The NERC Glossary of Terms for Intermediate System states that they must not be located inside the Electronic Security Perimeter. The Jumpbox is located in a DMZ that was defined as being inside of the ESP. R2.1 - There is Interactive Remote Access that does not utilize an Intermediate System. Users located outside of the Network1 ESP are being provided Interactive Remote Access to a Proxy Server (Device2) that is located inside of the ESP without utilizing an Intermediate System. The access originates from the corporate network. Additionally, Interactive Remote Access is permitted from an asset outside of the ESP (Device3) to a cyber asset inside (Device4) of the Network1 ESP (Doc13) without utilizing an Intermediate System (Doc15). As a result, there is Interactive Remote Access that does not utilize an Intermediate System. This allows the Cyber Asset outside of the ESP initiating Interactive Remote Access to directly access an applicable Cyber Asset inside of the ESP. R2.3 - There is Interactive Remote Access that does not require multi-factor authentication. Entity personnel were able to connect from a cyber asset outside of the ESP (Device5) to the Device6 which is an applicable cyber asset inside of the Network1 ESP. This connection offered the user the ability to bypass multi-factor authentication and only use a single factor static passcode. As a result, there are Interactive Remote Access sessions that do not require multi-factor authentication.
48	CIP-010	R3	10	A5B2	X		Entity did not have a documented process to perform an active vulnerability assessment. Doc1 includes the process for paper vulnerability assessment but did not include the process for performing an active vulnerability assessment. Analysis and discussion with Entity SMEs during the interview process confirmed these facts. As a result, Entity did not document one or more processes to perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment.
49	CIP-002	R1	6	A4B4	X		R1 requires the Responsible Entity to identify high and medium impact BES Cyber Systems at each asset, and identify those assets that contain low impact BES Cyber Systems. In this case, Entity did not know they had medium impact BES Cyber Systems. Entity stated the "top-down assessment approach which documents only the identified BES Cyber Assets and not other equipment at the asset is a potential weakness in the previous assessment process", thus resulting in missing the Cyber Assets.
50	CIP-002	R2	6	A4B4	X		R2 requires the Responsible Entity to review the identifications in R1 and have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months. In this case, Entity did not know they had medium impact BES Cyber Systems. Consequently they did not have BES Cyber Systems on their list. They were unable to annually review and approve it as required by R2 for the period from Date1 to the close of this audit on Date2. PNC Cause: Entity failed to develop the required list of BES Cyber Systems. Thus there was nothing to review or approve as required by R2.
51	CIP-005	R1	6	A4B4	X		There are firewall rules that are no longer valid yet have not been disabled or removed as well as firewall rules that do not include the reason for granting access. The Entity had firewall rules that were no longer used (i.e. printer no longer in service) as well as firewall rules where the reason for granting access was documented as "unknown". As a result, Entity could not provide a valid reason granting access for each inbound and outbound access permission configured on the EAP (Medium Impact BES Cyber Systems).
52	CIP-010	R3	5	A4B1	X		Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems but has not documented the planned date of completion of the action plan and/or the execution status of the mitigation plans. The Cyber Vulnerability Assessment (CVA) action plans did not document the planned completion date and/or status of each of the CVA findings deemed applicable by Entity1. Additionally, for many items, the Entity was unsure of the status/planned completion date.
53	CIP-002	R2	6	A4B4		X	The initial BES Cyber System list was created but not approved by CIP-002-5.1's effective date. Additionally, the following year's approval missed the 15 month frequency by one month.
54	CIP-003	R4	7	A4B1C04	X		The change in delegation from Employee1 to Employee2, was not documented within 30 days, as required by the Standard. Employee1 had resigned effective Date1. His replacement (Employee2) was appointed on Date2. The new delegation became effective Date3. Although the delegation was properly documented, Entity had exceeded the 30 day requirement.
55	CIP-005	R1	2	A3B2C05	X		Certain CIP version 5 definitions from the NERC Glossary of Terms were not fully understood by SMEs.
56	CIP-005	R2	2	A3B2C05		X	Certain CIP definitions from the current NERC Glossary of Terms are not fully understood by SMEs. e.g., Electronic Access Point, Intermediate System.
57	CIP-005	R1	6	A4B4	X		There are inbound and outbound access permissions that do not include a valid reason for granting access to "ANY" protocol. Entity16 had at least 18 firewall rules that allowed any port or service. In some instances, the entity had not contacted one of its vendors since Date1 to see if port ranges could be identified and reduced. In other cases, firewall management traffic flow rules between applicable cyber assets inside the Network ESP and assets outside the ESP were configured for "ANY" protocol. Management traffic port ranges were excessive and should be reduced. As a result, Entity did not have a documented reason for granting access rules that allow "ANY" protocols to enter or exit the ESP.
58	CIP-010	R1	10	A5B1		X	There was lack of consistency between documentation used to support compliance with CIP-007-6 (ex: ports and service documentation) and baseline configurations.
59	CIP-010	R4	2	A3B2C05	X		The BES CSI authorization form was used to authorize TCA usage instead of the TCA usage form. Lack of understanding of the appropriate form to use could lead to future compliance issues.
60	CIP-011	R1	2	A3B2C05		X	Entity did not follow Doc for handling BES Cyber System Information released to third parties.

	A	B	C	D	E	F	G
1	 NORTHEAST POWER COORDINATING COUNCIL, INC. NPCC, Inc. 1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782						
2	Standard	Req.	NPCC Root Cause	EA Cause Code	PNC	AOC	Finding Description
61	CIP-007	R3	9	A4B3	X		CIP-007-6, R3.3 requires responsible entities to implement a documented process for testing antivirus signatures. Although Entity has a documented process, it has not implemented this process. The documented process for testing malicious code signatures or patterns prior to general deployment (Doc) was not being followed. Signature updates for anti-malware software were deployed to BCAs without first being tested on test machines as stated in policy. Employees were not aware of the policy requirement to test anti-malware software signature updates prior to general deployment. As a result, Entity has not implemented the process to test malicious code signature or pattern updates prior to general deployment.
62	CIP-003	R3	7	A4B1C04		X	Having a single person with a "Concentration of Duties" creates a single point of failure in many processes that could lead to future compliance issues.
63	CIP-007	R5	11	A5B3C01	X		Entity was unable to demonstrate that default passwords were changed, and/or password length & complexity requirements were met for Medium Impact Cyber Assets. Entity's Department1 performed a site inspection at Area2 substation and reviewed 3 cyber assets for compliance with applicable requirements. Entity determined that only 1 (Device1) of the 3 sampled assets had default passwords changed. Entity identified other issues related to default passwords not being changed (Part 5.4) and password length & complexity not being correctly configured (Part 5.5). As part of the Entity internal Doc process, these issues are currently under-review to determine timeline, root cause, extent of condition across X-states and mitigation actions. The passwords for the applicable cyber assets at the Area2 substation have been subsequently changed.
64	CIP-010	R1	2	A3B2C05	X		Baseline configurations did not reflect the actual running configurations. For applicable Medium Impact BES Cyber Assets, Entity did not include logical network accessible ports in configuration baselines. For BES Cyber Asset Device1, port [A] was listed as open and listening in CIP-007-6 R1.1 documentation but not listed as open and listening in the BES Cyber Asset baseline for CIP-010-2 R1. The port was not actually open. Entity indicated that the CIP-007-6 R1 port listing covers a group of BES Cyber Assets (Device1 systems) and that the port may not actually be open on each individual BES Cyber Asset in the group. Entity stated that the grouping for CIP-007-6 R1 was not granular enough and included BES Cyber Assets that were not exactly alike. Entity stated that they would be reevaluating their grouping strategies for BES Cyber Assets to ensure each group only contains BES Cyber Assets that are exactly alike. For Medium Impact BES Cyber Assets, the baselines did not include logical network accessible ports. Entity stated that they thought that this requirement (1.1.4) only applies to BES Cyber Assets with External Routable Connectivity (ERC). The audit team reviewed the applicability of this requirement and confirmed that it applies to all Medium Impact BES Cyber Assets (no ERC exclusion). Entity acknowledged that this was an oversight on their part and would be identifying logical network accessible ports in the baselines for Medium Impact BES Cyber Systems going forward.
65	CIP-010	R4	2	A3B2C05	X		Entity could not demonstrate that Removable Media usage on applicable Cyber Assets was authorized. Additionally, Entity could not demonstrate that methods to mitigate malicious code had been implemented. For Section 3.1, Entity did not provide evidence of authorization for removable media usage on 8 EMS workstations (High Impact BCAs) inside of the Network ESP. Entity stated that the authorization documentation was completed but could not be located due the fact that the employee responsible for retaining the documentation was no longer with the organization. Entity did provide documentation that implied that Removable Media usage was authorized but could not provide the actual Authorization Form required by their documented process. For Section 3.2, Entity's documented process for Removable Media Handling, Doc2, does not specify that the method(s) to detect malicious code on Removable Media must use a Cyber Asset other than a BES Cyber System or Protected Cyber Asset. Entity did not know that this is a requirement and as a result, did not include this in their documented process.
66	CIP-005	R1	6	A4B4	X		There are inbound and outbound access permissions that do not include a valid reason for granting access to "ANY" protocol. Additionally, there are firewall rules that allow outbound communications from any IP on any protocol to any IP (Doc1). These rules are overly permissive. The port ranges were excessive and could be reduced. As a result, the entity did not have a documented reason for granting access rules that allow "ANY" protocols to enter/exit the ESP. The entity states that the root cause for this issue is the lack of adequate information on the ports and services needed for communication with the Device1 server. This server was a legacy device, purchased by a previous owner of the Function1 facility. The Device1 firewall (Device2) was installed on Date1. It is a medium impact EACMS with the EAP used for communication from the Device3 workstation to the Device1 server. The overly permissive rules presented could be exploited by a threat actor to establish a remote desktop session from the Device1 server (outside the ESP) to the Device3 workstation (inside the ESP).
67	CIP-005	R2	2	A3B2C05	X		There are Interactive Remote Access paths that do not require multi-factor authentication. The entity's two factor challenge only occurred when connecting to their business network through VPN. This configuration offers a user the ability to bypass multi-factor authentication and only use a single factor if already connected to the business network locally. Access to the Intermediate system used to access a BCA from inside the business network (outside the ESP but inside the corporate network) did not require MFA (Multi-factor authentication). As a result, there are Interactive Remote Access sessions that do not require multi-factor authentication. The entity states the root cause was a misunderstanding of the CIP definition of Remote Access and not applying it to the internal Business network accessing the BCA in the ESP. The scope of this noncompliance is one medium impact EACMS asset: Device1, the server used as the IRA intermediate system. An individual with access to the business network could gain access to the Intermediate system and initiate an IRA session without requiring MFA

	A	B	C	D	E	F	G
1	 NORTHEAST POWER COORDINATING COUNCIL, INC. NPCC, Inc. 1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782						
2	Standard	Req.	NPCC Root Cause	EA Cause Code	PNC	AOC	Finding Description
68	CIP-007	R2	5	A4B1	X		R2 For two Cyber Assets (Device1 and Device2), Entity did not evaluate security patches for applicability that have been released since the last evaluation, at least once every 35 days. Additionally, For the Manufacturer controlled switches, Entity did not apply an applicable patch or create a dated mitigation plan for the applicable patch within 35 calendar days of the evaluation completion. Occurrence 1 – R2.2 Specifically, for the Device1 and Device2, Entity did not check with the BCA vendor to check for security patches and did not include these BCAs in their overall patch management program. Occurrence 2 – R2.3 Specifically, for two network switches controlled by Entity vendor Manufacturer, (BES Cyber Asset ID Asset3, Asset4), Entity did not apply an applicable patch or create a dated mitigation plan for the applicable patch within 35 calendar days of the evaluation completion. The vendor Manufacturer will only install patches during an outage. In this case, the outage was scheduled to occur 40 days after the patch notification but was delayed for market purposes. The update was ultimately performed 54 days from the notification that the patch was approved. The documented security patch was available on Date2 was not applied until Date3. During this 19-day time period, Entity did not have a dated mitigation plan.
69	CIP-007	R5	5	A4B1	X		For five BCAs managed by Vendor Manufacturer (all network switches), Entity was not able to demonstrate that the BCAs are compliant with the requirements for the standard. Entity was not able to get the required information to demonstrate compliance from the vendor. Occurrence 1 R5.2 For five Manufacturer2 managed BCAs, Entity was unable to provide evidence demonstrating that all known enabled default or other generic account types were identified and inventoried. Occurrence 2 R5.3 For five Manufacturer managed BCAs, Entity was unable to provide evidence demonstrating that individuals who have authorized access to shared accounts are identified. Occurrence 3 R5.4 for five Manufacturer managed BCAs, Entity was unable to provide evidence demonstrating that known default passwords have been changed. Occurrence 4 R5.5 For five Manufacturer managed BCAs, Entity was unable to provide evidence demonstrating that password length and complexity requirements are either technically or procedurally enforced
70	CIP-010	R1	2	A3B2C05	X		For the equipment controlled by Manufacturer, the baseline configuration did not include logically accessible network ports. For the PACS and the Intermediate System, Entity1 did not develop baseline configurations. Occurrence 1 For five BCAs managed by Manufacturer (all network switches), the baseline configuration did not include logically accessible network ports. Entity was not able to demonstrate that the BCAs are compliant with the requirements for the standard. Entity was not able to get the required information to demonstrate compliance from the vendor. Occurrence 2 For nine PACs cyber assets and one Intermediate System, Entity did not develop baseline configurations. It appears Entity did not identify these devices as being subject to the NERC CIP standards. This PNC will be filed under CIP-010-2 R1, however, as the cyber assets were not identified, they may not be receiving the protections afforded by the CIP standards.
71	CIP-002	R1	6	A4B4		X	Based on Entity's current operating practice, and the "misuse" scenario discussed with NPCC, the operators' phone system should be identified as a BES Cyber Asset.
72	CIP-005	R1	2	A3B2C05		X	Entity has not clearly identified Electronic Access Points (EAP). Rather, Entity has identified entire Cyber Assets as EAPs instead of the network interfaces
73	CIP-005	R1	6	A4B4	X		Entity failed to include a reason for granting access of inbound and outbound access permissions. The audit team discovered 1 access permission that did not include a reason and 2 access permissions that did not include a clear reason for access. Specifically, the documentation for firewall rule #X1 (NP-View ID#) on FW1 did not include a reason for granting access. Additionally, the documentation for firewall rule #X2 and rule #X3 (NP-View ID#) on firewall FW1 described the directional flow of traffic which does not adequately explain the reason for granting access
74	CIP-007	R5	9	A4B3	X		Tools used to enforce password complexity procedures were configured incorrectly. Specifically, the tools were configured to allow a minimum password length of six characters instead of eight characters as required by the Standard. The password configuration spreadsheet used by Entity to store shared passwords and to evaluate password compliance had several password length validations (formulas) that were configured to check for a minimum of six (6) characters instead of eight (8). Entity does have other procedural controls to ensure that password lengths are compliant with the standard and all password lengths validated in the sample set met the minimum length specified in the standard. This issue is related to an incorrectly configured tool used in the procedural control to enforce password complexity.
75	CIP-003	R1	7	A4B1C04		X	Having a concentration of duties may result in a single point of failure and could lead to future compliance issues.
76	CIP-007	R3	6	A4B4		X	Ensure Entity's CIP-007 R3 testing procedure is consistent with the testing being performed. i.e signature testing done by vendors.
77	CIP-010	R1	10	A5B1		X	The process to develop baseline configurations was not clearly documented.