

CIP Pilot Audits Lessons Learned

November 20, 2018

- AESO team
 - Peter Wong – Director, External Compliance Monitoring
 - Daniela Cismaru – Manager, ARS Compliance Monitoring
 - Peter Tam – Senior Auditor, ARS Compliance Monitoring
 - Joan Gaerlan – Senior Auditor, ARS Compliance Monitoring
- ATCO Electric Ltd.
 - Dan Bamber – Senior Advisor, Compliance
- EPCOR Distribution and Transmission Inc.
 - Travis Robinson – Manager, Transmission Regulatory Affairs

- Background and Purpose

- CIP v5 Pilot Audits Lessons Learned

Daniela Cismaru – CIP approach, audits, assessments

Joan Gaerlan – CIP003, 004, 006, 008, and 011

Peter Tam – CIP002, 005, 007, 009, and 010

Daniela Cismaru – Audits findings

- MPs sharing their side

Dan Bamber

Travis Robinson

- Next Steps

Peter Wong

- September 2015 – AUC approves set of CIP standards
- November 2016 stakeholder session
 - Introduced the approach for monitoring CIP standards
 - Identified areas of concern, addressed them through 2017
 - TFE process defined, NERC Guidance material, clarity around IAC
- October 1, 2017 - majority of CIP requirements come into effect
- November 2017 stakeholder session
 - Details on the pilot approach for auditing CIP standards in 2018
- January – August 2018 – pilot audits
- Today – lessons learned from the pilot

- To share the lessons learned from the CIP audits completed in 2018 with the industry, so that
 - We better understand the technical requirements
 - We understand what is expected to demonstrate compliance
 - We are aware of process improvements
- Ultimately, when you are preparing for an audit, that you know how to prepare evidence to show you are compliant

CIP Compliance Monitoring Approach

- Approach

Compliance Monitoring Program (CMP) processes being used to assess MPs compliance with CIP standards

- CIP Pilot audits schedule

All companies included in Q1 and Q2 2018 scheduled audits

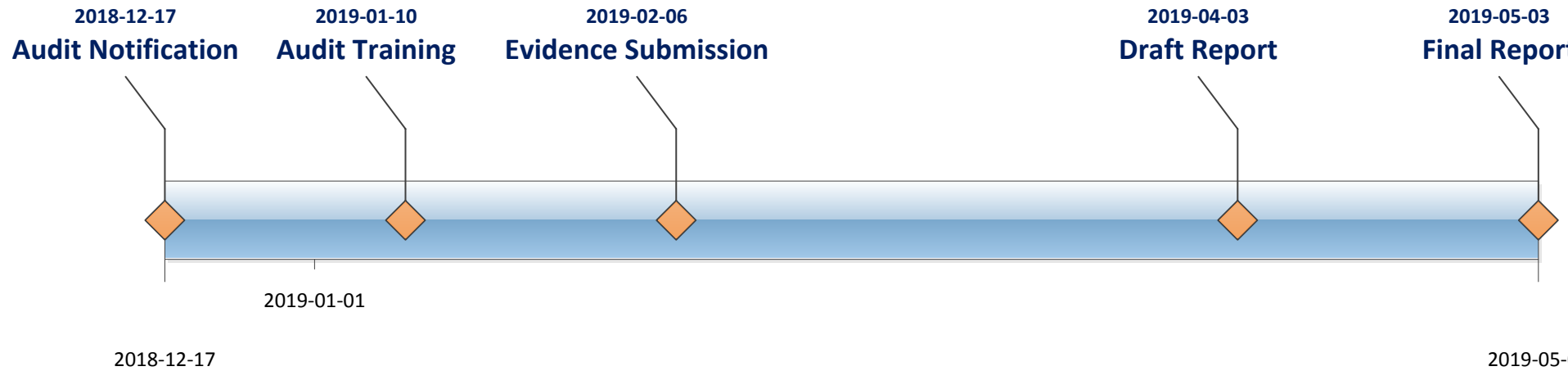
4 companies with High/Medium/Low Impact assets and 5 companies with Low Impact assets

The existing audit methodology was used

Communicated extended timelines for the audits including High/Medium Impact assets

- Considers NERC guidance, AESO ID guidance, developed processes (TFE, IAC, RFI, AA)

- Q1 Audit – schedule example



- Audit Notifications

The audit notifications sent in advance

- Sent **70+ days in advance** of the evidence submission date (the current process requires 30 days)

- Audit Scope

All CIP requirements applicable to each company based on the registered functional entities and a subset of the power system applicable requirements

- CIP Audit period

Q1 – October 1, 2017 to December 31, 2017

Q2 – October 1, 2017 to March 31, 2018

- All asset categories (High/Medium/Low Impact)

- Duration of the audits

No changes for the companies with only Low Impact assets

- Forecasted/Actual - 3 months

Companies with High/Medium/Low Impact assets

- Forecasted – 5 months
- Actual – anywhere in between 4 to 6 months

Overall length of the Pilot Audits

- February to mid-August 2018

Flexibility on determining the length of the audits will be maintained

- Initial Evidence Submission

Normal process and timelines used for initial submissions

The received evidence pertains to all requirements included in the audit scope

- Shortages

Inconsistent evidence

Poor/unreliable data

Documented processes with no evidence of implementation

- Reasons for not providing information during initial evidence submission

Different interpretation of the requirement and/or evidence required

Waiting for auditors to submit sampling request

Data gathering issues and/or unavailability of evidence

Confidentiality concerns

- Impact of evidence's shortages

Increased number of IRs

Extensions to IRs

Delays in finalizing the audits

- Observations

The volume of evidence was significantly higher than expected

Direct correlation between the number of assets and the volume of evidence

Direct correlation between the MP's internal structure and the volume of evidence

Direct correlation between the quality of initial evidence and the duration of the audit

- Statistics

High/Medium Impact Assets (volume)	Low Impact Assets (volume)	Number of documents	Number of pages	Previous audits (volume)
3.5 GB	16.26 MB	Approx. 800	Approx. 25000	20% of 2018 audits

- Submission mechanisms

SharePoint Online

- Mainly used by the MPs with High/Medium Impact assets, to ensure alignment with CIP-011 (BCSI)
- Generally reliable and user friendly; training provided by the AESO; issues addressed timely

We will continue using SharePoint in future audits

- Steps to improve the initial evidence submission

The AESO is reviewing the RSAWs to see whether additional guidance should/could be provided (mid-March 2019)

Suggestion to MPs – where possible, consolidate your documentation; use the “Evidence Description” to provide clear references/guidance

- Normal process with adjusted timelines used

RSAWs

As the mechanism for evidence submission and documenting the assessments

TFE

The approved TFEs were considered based on the date of approval

Applicability Assessments/RFI

Formal AESO positions and clarifications were considered

Timelines

Some extension of finalizing the assessments due to quality of evidence initial submissions, IRs responses and clarifications

- Planning on continuing using the current methodology and adjust the timelines when necessary

- Information Requests

The usual process and timelines used

- Quality of Responses

Good things

- The MPs made an effort to provide good, quality responses
- Small number of requests for extensions
- The MPs reached out to auditors for clarifications

Shortages

- Incomplete responses
- Conflicting information; retracted/changed information
- Unsorted data with insufficient and/or incorrect guidance on how to extract the information requested

- Observations

Clear correlation between the quality of initial evidence and the number of IRs

- The lower the quality of initial evidence submission, the higher the number of IRs

The duration of the audit clearly linked to the number of IRs and the quality of the IRs responses

The volume of information submitted in response to IRs varied anywhere from 10% to 700% of initial evidence submission

Total # of IRs	# IRs for H/M	# IRs for L	Volume	# of Extension Days
261 vs. 100	249	12	1.1 GB	37

- Challenges

Reissuing IRs due to incorrect and/or incomplete responses

IRs numbering

- The high number of IRs & several auditors working on an audit at the same time posed a challenge in properly identify the IRs
- The current IR naming convention made referencing previous IRs quite difficult

The AESO has requested input from the impacted MPs

- Developed a process to ensure unique IR identifier
- IR identifier/name will contain the # if questions included

- Submission Mechanisms

SharePoint Online

We will continue using SharePoint in future audits

- Steps to mitigate the high number the IRs

The AESO is reviewing all the RSAWs to see if additional guidance should/could be provided (posted by mid-March 2019)

Suggestion to MPs – focus on developing and submitting timely and quality evidence

- Observed discrepancies between the MPs and the AESO's understanding and application of certain terms
- Compliance has worked closely with the technical and legal groups within the AESO to ensure establishing an unique position and a consistent application throughout the audits

- Control Centre

Control center is a Medium Impact BCS if it controls and monitors 1500 MW generation from generating units located at two or more locations

Industry practice - a centralized control room controls and monitors several generating units/AGF (commonly used for windfarms located in different jurisdictions)

Pending the AESO decision whether the term applies to locations and/or control centers that are not located in AB

Compliance expectations and approach will be communicated after the decision is formally communicated by the AESO

- Location

A number of the criteria in CIP-002 Attachment 1, as well as the definition of a control centre rely on the concept of a “location”

It appears that “location” could be interpreted differently

Compliance is advocating for the development of an ID

- Policies, Programs, Processes, Procedures

None of these terms are defined in the NERC or AESO glossary

The AESO's expectations for these terms is based on common industry usage and the intent in the standards, including NERC guidance

It is apparent that there is no common understanding of what is meant by each of these terms

Compliance has initiated an internal dialogue on this matter and it is advocating strongly for the development of an ID

- Industrial Complex vs Power Plant

The “Industrial Complex” and “Power Plant” are not defined terms

It is apparent that there is no common understanding of what is meant by each of these terms

Compliance has initiated an internal dialogue on this matter and a formal position is in the development

- CIP-004 R1 Applicability to Contractors

The wording of CIP-004 R1 part 1.1 indicates that it applies to “the Responsible Entity’s personnel...”, whereas other requirements in CIP-004 do not use the word “personnel”; the term “individuals” is mainly used, unless specifically stating “contractors” and “service vendors” as people to whom the requirement applies

The AESO position is that the requirement applies to Contractors
Compliance is advocating for the development of an ID

- CIP-005 R1 and CIP-007 R1 Firewall Rule and Logical Port Justification

CIP-005 R1.3 requires “inbound and outbound access permissions, including the **reason** for granting access...” Similarly, CIP-007 R1.1 requires the market participant “enable only logical network accessible ports that have been **determined to be needed...**”

Compliance is advocating for the development of an ID to provide guidance on “need” and “reasons”

- CIP-006 Physical Access Control, Monitoring and Logging

CIP-006 requirements imply that physical access should be controlled, monitored and logged at all times

Provisions for controlling, monitoring and logging physical access when PACS is not available to carry out its function is deemed necessary

Compliance is advocating for the development of an ID

- CIP-006 R1.5/ R1.7 Alarming or Alerting

CIP-006 R1.5 and R1.7 requires RE to “issue an alarm or alert in response to detected unauthorized access ... within 15 minutes of detection”

Compliance is advocating for the development of an ID to increase the emphasis on timely guidance

- CIP-007 Security Patch Management

CIP-007 R2 Part 2.1 requires market participants to have a patch management process for tracking the patch sources

Not all patch sources were tracked because the incorrect assumption made by MPs that they are not subject to the requirement

Compliance is advocating for the development of an ID

- CIP-009 R1 Part 1.5 Data Preservation

CIP-009 R1 Part 1.5 requires market participants to have one or more processes to preserve data per cyber asset capability for determining the cause of a cyber security incident that triggers activation of the recovery plan(s)

The AESO observed that the processes do not sufficiently address preserving data per cyber asset capability

Compliance is advocating for the development of an ID

- CIP-011 Information Protection

CIP-011 R1 requires documentation and implementation of methods for identifying BCSI and procedures for protecting and securely handling BCSI in storage, transit and use

Some programs lacked a comprehensive assessment of what constitutes BCSI

Compliance is advocating for the development of an ID

Clarifications (cont.)

- Compliance is supporting the ID development
- Until then, the RSAWs will be updated to include guidance on these matters (mid-March 2019)

- Observed shortcomings

Documentation deficiencies

- Processes too high level; not addressing the “how”
- Process addressing a particular requirement not clearly referenced
- Not addressing all applicable systems/ access types
- Not addressing all sub-requirements
- Not covering all departments/ groups/ locations/ physical security perimeters (PSP)s in scope

- AESO expectations

Documentation

- Documented processes addressing the “how”
- Clear references to documented process addressing a particular requirement
- All applicable systems/ access types addressed
- All sub-requirements addressed

Note:

This includes processes involving different circumstances/ scenarios such as PACS outages/ unavailability, equipment being moved, etc., not just under normal circumstances

- All departments/ groups/ locations/ PSPs in scope covered (where CIP standards apply)

Note: The above expectations on documentation extend to implementation

- Observed shortcomings

Evidence submission

- Revision history of documented process not specifically identifying changes made to the document during the audit period
- No references/ mapping of evidence to particular sub-requirements/ topics

- AESO expectations

Evidence submission

- Revision history of documented processes specifically identifying changes made to the document during the audit period. Alternatively, all process documents in effect during the audit period must be provided
- References/ mapping of evidence to particular sub-requirements/ topics provided under Evidence Description column in the RSAW (e.g. CIP-004 topics 2.1.1 through 2.1.9 mapped to training content that addresses each topic)

CIP-002-AB-5.1 BES Cyber System Categorization

- Good practices observed

Detailed documented process for BES cyber system (BCS) categorization

Well-defined cyber asset lists with detailed information including the assets, type, host name, IP address, functions, external routable connectivity, log/alert capability and more

The lists are presented in spreadsheets, easy to select samples for verification and sorting

Exempted cyber assets (ECA) are listed

R1.2. Identify each of the medium impact **BES cyber systems** according to Attachment 1, Section 2, if any, at each asset;

Attachment 1 - Section 2.12. (Medium Impact Rating)

*Each **control centre** or backup control centre used to perform the functional obligations of the operator of a transmission facility not included in High Impact Rating (H), above.*

AESO Authoritative Document Glossary

Control centre means one or more facilities hosting operating personnel that monitor and control the **bulk electric system** in real-time to perform the reliability tasks, including their associated data centres, of:

- 1) the **ISO**,
- 2) an **operator** of a **transmission facility** for **transmission facilities** at two (2) or more locations, or
- 3) an **operator** of a **generating unit** or an **operator** of an **aggregated generating facility** for either **generating units** or **aggregated generating facilities** at two (2) or more locations.

- Observed shortcomings

Incorrect assets categorization

- Examples: cyber assets pertaining to control centre, applicable virtual machines and tap changers relays not categorized as Medium Impact BES cyber assets (BCA)

Boundary of industrial system, operating area, city limit used as a factor of determining the boundary of “location”

- AESO expectations

Two named transmission substations are deemed as two locations

All applicable cyber assets are **correctly** categorized

R1.3. Identify each asset that contains a low impact BES cyber system according to Attachment 1, Section 3, if any.

- Observed shortcomings

- Some remedial action schemes (RAS) were not included

- Some substations were incorrectly viewed as radial circuits

- AESO expectations

- Correct use of Section 3.5 of Attachment 1, which includes:

- the RAS as specified in Section 4.2.1.2, and

- the RAS that supports the reliable operation of the bulk electric system (BES)

- Radial circuit assessments should take ID #2016-006RS into consideration

- Good practices observed

Clear references and mapping, in general

CIP Exceptional Circumstances (CEC) definition and/ or reasons for declaration identified in the policy consistent/ aligned with the definition per AESO Glossary

Description of CIP Senior Manager (CSM) roles and responsibilities consistent with the CSM definition per AESO Glossary

Delegation document includes specific actions delegated as allowed by CIP standards

R1. Each Responsible Entity, for its High Impact and Medium Impact **BES cyber systems**, shall review and obtain **CIP senior manager** approval at least once every **15 months** for one or more documented cyber security policies that collectively address the following topics:

1.1 Personnel & training (CIP-004-AB-5.1);...

- Observed shortcomings

- Missing policies covering some sub-topics in referenced standards per topics R1.1 through R1.9 (e.g. Access Management and Access Revocation to address topic 1.1 CIP-004 Personnel & Training missing)
- Typo errors in sub-section titles in the policy documents (e.g. titles not matching the content)
- Policy inconsistent with related requirement in referenced standard (e.g. testing and maintenance on a cycle no longer than 3 years per policy vs. at least once every 24 months per CIP-006, R3)

- AESO expectations

All sub-topics in referenced standards clearly mapped to/ addressed by the policies

Notes:

Errors in sub-section titles in the policy documents were deemed acceptable given that the actual content addressed the topics as required.

Inconsistency of policy with the related requirement was deemed acceptable given that the related requirement is addressed properly in some other document (e.g. documented procedures, plan or program).

However, both are not considered best practice.

- Observed shortcomings

Policy permits actions under CEC not directly allowed by CIP requirements (e.g. use of CIP-004 R4.1 to bypass normal requirements of PRA when CIP-004 R3 does not include a provision on allowing CEC)

- AESO expectations

Use of CEC per policy based on CIP requirements that allow CEC

R3. Each Responsible Entity shall identify a **CIP senior manager** by name and document any change within 30 **days** of the change.

- Observed shortcomings

No CSM identified during the audit period

CSM roles and responsibilities

- Not described
- Description not detailed

CSM approval of own designation (not considered best governance practice)

Evidence referencing “NERC CIP Senior Manager” and/or “NERC CIP standards” (ARS coverage unclear)

Approval of CSM designation by a “high-level official” not clearly addressed

- AESO expectations

A CSM identified by name throughout the audit period

The following NERC guidance is addressed:

“CSM is of sufficient position in the RE to ensure that cyber security receives the prominence that is necessary.”

Clear description of the roles and responsibilities of the CSM that are aligned with the CSM definition

CSM designation approved by a different individual (considered best practice but still depends on RE’s organizational structure)

Evidence clearly pertaining to ARS (e.g. reference to ARS CSM instead of NERC CSM)

Clear description of the role and/ or authority of the CSM approver (if being a “high-level official” is not evident given only the title)

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP **reliability standards**, the **CIP senior manager** may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the **CIP senior manager**; and updated within **30 days** of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

- Observed shortcomings

Delegation not approved by the CSM/ Evidence of approval not properly documented

Delegation not implemented in accordance with the RE's own documented process (e.g. documented process requiring notices of delegation sent by email/ acknowledgment obtained through email response/ prohibiting certain tasks to be delegated not followed)

- Observed shortcomings

Delegation document

- Includes delegated actions not specific enough to clearly indicate whether they are allowed by the CIP standards
- Includes actions not considered delegated actions in scope of R4 (e.g. tasks being assigned to CSM; actions not specifically mentioned in CIP standards as CSM responsibility)

- AESO expectations

Delegation approved by CSM with evidence of approval properly documented

Delegation implemented in accordance with RE's documented process

Documented delegated actions specific enough and in accordance with CIP standards

CIP-004-AB-5.1

Personnel & Training

- Good practices observed

 - Some MPs provided clear references and mapping

 - Use of NERC Guidance in understanding the requirement

 - Some MPs provided well organized IR responses and sampling evidence

- Observed shortcomings

Errors in the lists of personnel in scope of particular requirements during the audit period (e.g. included personnel who never had access; personnel included in both lists of terminated and reassigned personnel)

- AESO expectations

Accurate lists of personnel in scope of particular requirements (e.g. based on types of access) during the audit period as basis for samples

Notes:

Consider who (personnel), what (type of access) and when (date granted/ revoked; during the audit period vs. end of audit period)

As needed, provide clear, complete and accurate filtering instructions OR filter before sending to the auditor

- Observed shortcomings

No tracking of when access were granted, only when user was authorized/ approved for access (not considered best practice)

- AESO expectations

Evidence of authorized access grant

- Date access granted
- Date authorized – deemed acceptable under the premise that authorization always happens prior to access grant (Note: must be supported by the documented process)

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R1 – Security Awareness Program*.

Part 1.1 Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to **BES cyber systems**.

- Observed shortcomings

Reinforcement of cyber security practices not provided to contractors who had access per R1.1

- AESO expectations

Security awareness reinforcing cyber security practices provided to all personnel (i.e. contractors and employees) who had access per R1.1

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-AB-5.1 Table R2 – Cyber Security Training Program*.

Part 2.1 Training content on: 2.1.1. cyber security policies; 2.1.2. physical access controls; 2.1.3. electronic access controls; 2.1.4. the visitor control program; 2.1.5. handling of **BES cyber system information** and its storage; 2.1.6. identification of a **cyber security incident** and initial notifications in accordance with the entity's incident response plan; 2.1.7. recovery plans for **BES cyber systems**; 2.1.8. response to **cyber security incidents**; and 2.1.9. cyber security risks associated with a **BES cyber system's** electronic interconnectivity and interoperability with other **cyber assets**.

- Observed shortcomings

Content of training does not address all topics

- AESO expectations

Training content appropriately address all topics

NERC Guidance considered

Part 2.2 Require completion of the training specified in part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable **cyber assets**, except during **CIP exceptional circumstances**.

- Observed shortcomings

Personnel granted authorized access per R2.2 prior to completion of the required training

Deficiencies in the training evidence

- No evidence of training for all departments/ groups in scope
- Training tracking sheets provided instead of training records/ evidence of training completion

- AESO expectations

Personnel not granted authorized access until the required training is completed

Evidence of training completion

- Dated
- Covers all departments/ groups in scope
- Training records
- Demonstrates completion, not just attendance
- System generated/ raw data is preferred

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to **BES Cyber Systems** that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R3 – Personnel Risk Assessment Program*.

- Observed shortcomings

Evidence showing inconsistent implementation of the PRA process (e.g. whether identity check was performed; how many years back the criminal background check went)

Deficiencies in sampling evidence

- Not providing evidence for the AESO's selected samples; providing evidence for own selected samples
- Reuse of evidence provided in a separate sampling stream (e.g. referencing samples on contractors for the testing on employees)

- AESO expectations

Evidence of PRA completion

- Dated; within the last seven years
- Covers all departments/ groups in scope
- PRA reports, not only tracking sheets
- Covers the whole PRA process (i.e. confirm identity; 7 year criminal history records check; evaluation of criminal history records check)
- Complete and consistent implementation of the PRA process

Sampling evidence

- Complete evidence as requested per the AESO selected samples
- Well organized
- With proper references
- With sufficient explanation, as needed

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R4 – Access Management Program*.

Part 4.1 Process to authorize based on need, as determined by the Responsible Entity, except for **CIP exceptional circumstances**: 4.1.1. electronic access; 4.1.2. unescorted physical access into a **physical security perimeter**; and 4.1.3. access to designated storage locations, whether physical or electronic, for **BES cyber system information**.

- Observed shortcomings

One time authorization for a group of personnel

Documented authorization process not addressing “based on need”

Deficiencies in implementation evidence of authorization process (e.g. not addressing “based on need”; no PRA/ training at the time of request; no evidence to show that prequalification approval is not granted until PRA/ training are completed; authorization forms not fully completed)

- AESO expectations

Individual authorization evidence is preferred

Note:

One authorization document for a group of personnel was deemed acceptable given the detailed list provided supported by the documented process/ mapping of roles to access types

Documented authorization process addresses “based on need” (includes criteria to follow; how the approver determines that the business justification is acceptable)

Evidence of implementation of the authorization process

- Demonstrates implementation of the documented process
- Addresses “based on need”
- Consistent and complete authorization forms

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R4 – Access Management Program*.

Part 4.2 Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

- **Observed shortcomings**

Insufficient evidence to show that all active access were validated and when the validation took place

- **AESO expectations**

Evidence demonstrates quarterly validation of all active access against authorization records

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-AB-5.1 Table R5 – Access Revocation*.

- Observed shortcomings

Access of terminated personnel not removed/ revoked within the required timelines

Deficiencies in implementation evidence

- No time specified for the effectivity of termination action
- Not clear which dates/ fields in the evidence represent the effective date and time of termination action/ access removal/ access revocation
- Missing evidence
- Inconsistent evidence

- AESO expectations

Access of terminated personnel removed/ revoked within the required timelines

Evidence of termination

- Specifies date and time of termination action
- Clear references provided (which dates/ fields)
- Complete and consistent with other evidence provided

Evidence of access removal/ revocation

- Specifies date and time of removal/ revocation of access
- Clear references provided (which dates/ fields)
- Complete and consistent with other evidence provided
- Complete information on what types of access are removed/ revoked by a specific action (e.g. LAN ID disabled removes IRA, access to DSL for BCSI, etc.)

- **Good Practices Observed**

Well-developed criteria of defining electronic security perimeter (ESP) and electronic access point (EAP)

Detailed ESP related process

Concept of defense-in-depth in network design being adopted

Use firewall technology to control inbound and outbound traffic

Use proven technology for interactive remote access management

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-AB-5 Table R1 – Electronic Security Perimeter*.

Part 1.1 All applicable **cyber assets** connected to a network via a routable protocol shall reside within a defined **electronic security perimeter**.

Part 1.2 All **external routable connectivity** must be through an identified **electronic access point**.

- Observed shortcomings

No steps included in the documented process on “how” Parts 1.1 and 1.2 is implemented

- AESO expectations

The documented process should include, at a minimum, the following:

- Analyze current/proposed system architecture
- Determine ESP boundaries
- Determine access and external connectivity needs
- Determine and configure an EAP
- Document the ESP diagrams

Part 1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

- Observed shortcomings

No steps included in the documented process on “how” Part 1.3 is implemented

The documented process repeats the language of the requirement, without sufficient content to implement Part 1.3

Reasons of granting access lack sufficient details

- E.g. SNMP- Trap

Note: SNMP stands for simple network management protocol

- AESO expectations

The process should include how business need is evaluated and, criteria and/or justification of inbound and outbound access permissions

The process should address managing the change of EAP due to system reconfiguration or technology upgrade, etc.

Reasons of granting access should be specific and be tied to the functionality. Example:

- Allow Solarwinds to collect, react to and forward syslog message and SNMP traps for the function of network monitoring

R2. Each Responsible Entity allowing Interactive Remote Access to BES cyber systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-AB-5 Table R2 – Interactive Remote Access Management

Part 2.1 Utilize an **intermediate system** such that the **cyber asset** initiating interactive remote access does not directly access an applicable **cyber asset**

Part 2.2 For all interactive remote access sessions, utilize encryption that terminates at an **intermediate system**.

- Observed shortcomings

Unrelated documents submitted as evidence to demonstrate compliance

- AESO expectations

Process of determining, building and configuring the intermediate system

Process of configuring authentication servers

Process of configuring encryption

Part 2.3 Require multi-factor authentication for all **interactive remote access** sessions.

- Observed shortcomings

One-time password communicated with a dedicated cell phone or landline was incorrectly deemed as multi-factor authentication

- AESO expectations

In addition to one-time password, another factor of authorization is required, such as:

- something the individual knows such as passwords or PINs (this does not include User ID);
- something the individual has such as tokens, digital certificates, or smart cards; or
- something the individual is such as fingerprints, iris scans, or other biometric characteristics.

- Good practices observed

- Some MPs provided clear references and mapping

- Some MPs provided well organized IR responses and sampling evidence

- Entry logs containing all required information (i.e. identifies the individual, date and time of entry)

- Entry/ Visitor logs from more than 90 days prior to audit evidence submission date

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan*.

Part 1.1 Define operational or procedural controls to restrict physical access.

Part 1.2 Utilize at least one physical access control to allow unescorted physical access into each applicable **physical security perimeter** to only those individuals who have authorized unescorted physical access.

Part 1.3 Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into **physical security perimeters** to only those individuals who have authorized unescorted physical access.

- Observed shortcomings

List of applicable systems per R1.2 and R1.3 not provided

Operational and procedural controls to restrict physical access not clearly defined in documented physical security plan

Access methods using only a single access control (for High Impact BCS)

Unauthorized individual allowed physical access into an applicable PSP

- AESO expectations

List of all applicable systems

- Mapped to which PSP each is located
- Identified whether High or Medium Impact BCS, associated EACMS and PCAs, or PACS.

Operational and procedural controls to restrict physical access clearly defined in the documented physical security plan

Evidence of implementation of the controls as described in the plan (may be subject to sampling depending on the type of control)

Access methods utilizing two or more different physical access controls (for High Impact BCS)

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan*.

Part 1.4 Monitor for unauthorized access through a physical access point into a **physical security perimeter**.

Part 1.6 Monitor each **physical access control system** for unauthorized physical access to a **physical access control system**.

- Observed shortcomings

No evidence of monitoring for unauthorized access through physical access points into the PSPs/ Unmonitored physical access points (e.g. records of alarms map only to PSPs and not to the physical access points)

- AESO expectations

Evidence showing physical access points/ PACS being monitored throughout the audit period

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan*.

Part 1.5 Issue an alarm or alert in response to detected unauthorized access through a physical access point into a **physical security perimeter** to the personnel identified in the bulk electric system cyber security incident response plan within 15 minutes of detection.

Part 1.7 Issue an alarm or alert in response to detected unauthorized physical access to a **physical access control system** to the personnel identified in the **bulk electric system cyber security incident** response plan within 15 minutes of the detection.

- Observed shortcomings

Alarms not timely investigated to allow activation of the incident response plan in the event of detected unauthorized access

- AESO expectations

Timely investigation of alarms to allow activation of the incident response plan in the event of detected unauthorized access

Notes:

Alarm systems are intended to detect unauthorized access; and provide notification to individuals responsible for response. For this reason, all alarms should be timely investigated.

This applies even if the alarm is ultimately determined as caused by authorized access – not known at the time of the alarm and cannot be used as a mitigating factor.

Alarms going off with authorized access are not normal and may be an indication that the processes/ controls in place are not addressing the intent of the requirements.

Evidence of alarm/alert issuance within 15 minutes of detection of unauthorized access

- Specifies date and time of detection
- Specifies date and time of alarm/ alert issuance
- Alarm/ alert issued to personnel identified in the BES CSIRP (Note: Consistent with the evidence provided per CIP-008)

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-AB-5 Table R1 – Physical Security Plan*.

Part 1.9 Retain physical access logs of entry of individuals with authorized unescorted physical access into each **physical security perimeter** for at least ninety **days**.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-AB-5 Table R2 – Visitor Control Program*.

Part 2.3 Retain visitor logs for at least ninety **days**.

- **Observed shortcomings**

Documented physical security plan and visitor control program not specifically mentioning 90 days retention of logs (e.g. states that logs are set to specific volume size which once reached will be saved and backed up with a new active journal started)

- AESO expectations

Specific mention of the 90 days retention requirement in the plan/program is preferred

Note:

Setting specific volume size triggering back-up of logs was considered acceptable since the said practice was deemed sufficient to meet the 90 days retention requirement (as further supported by the existence of 90 days worth of logs).

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-AB-5 Table R2 – Visitor Control Program*.

- **Observed shortcomings**

No evidence demonstrating continuous escort of visitors (e.g. escort names not logged; no other evidence provided)

Required information not included in visitor logs (e.g. time of initial entry/ time of last exit/ name of individual point of contact not logged)

Missing visitor logs for a number of PSPs

- AESO expectations

Evidence demonstrating continuous escort of visitors (e.g. documented program; training; logs)

Visitor logs include all required information (i.e. date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor)

Visitor logs covering all PSPs (will be subject to sampling)

CIP-007-AB-5

System Security Management

- Good Practices Observed

Process for ports and services are well defined

- Criteria of evaluating enabling or disabling ports and services
- Tools to manually collect ports and services information
- Procedures for dynamic port assignment

Methods are in place to deter, detect or prevent malicious code

- Network firewalls
- Network IDS
- Whitelisting & Blacklisting
- System hardening

Robust process for security patch management

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R1 – Ports and Services*.

Part 1.1 Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports....

- Observed shortcomings

The reasons for enabling are generic and not specific. E.g.

- 11111 ~ 99999 TCP ports for window applications

- AESO expectations

Business needs to support the specific BES cyber assets' functions

- 11111 TCP Allow XYZ.exe which is needed for patch management agent to detect and deploy patches.

Part 1.2 Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.

- Observed shortcomings

 - Few serial ports not being physically protected

- AESO expectations

 - All ports should be physically protected irrespective whether there are other security controls in place to address vulnerability

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R2 – Security Patch Management*.

Part 2.1 A patch management process for tracking, evaluating, and installing cyber security patches for applicable **cyber assets**. The tracking portion shall include the identification of a source ...

- Observed shortcomings

Some type of patches were not included in the patch management process

BIOS was not included in patch management process

- AESO expectations

Ensure all patches are included in the patch management process

BIOS update should be included in the patch management process developed for R2.1.

Part 2.3 For applicable patches identified in part 2.2, within **35 days** of the evaluation completion, take one of the following actions:

- apply the applicable patches; or
- create a dated mitigation plan; or
- revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete.

- Observed shortcomings

- Missed the due day to create a mitigation plan

- No mitigation plans were seen for some patches

- AESO expectations

- Ensure that the mitigation plan is timely created

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R3 – Malicious Code Prevention*.

Part 3.3 For those methods identified in part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

- Observed shortcomings

 - No process for the testing the signatures or patterns

 - Reliance on vendor to update or retract the DAT File in the event that an error is found or impact is determined

- AESO expectations

 - Reliance on vendor is not deemed as an appropriate process for addressing testing

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R4 – Security Event Monitoring*.

Part 4.2 Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per **cyber asset** or **BES cyber system** capability):

- 4.2.1. detected malicious code from part 4.1; and
- 4.2.2. detected failure of part 4.1 event logging.

- **Observed shortcomings**

No steps included in the documented process on “how” Part 4.2 is implemented

Some assets were not included in the monitoring tools

- AESO expectations

The documented process should include, at a minimum, the following:

- Determine the logged events in Part 4.1 that necessitate alerts per Part 4.2
- Document the list of alerts for tracking and maintenance
- Configure the tools to generate or edit the required alerts for the logged events
- Add/remove alerts when the list of log events are changed due to new/removal of an applicable system.

Part 4.3 Where technically feasible, retain applicable event logs identified in part 4.1 for at least the last 90 consecutive **days** except under **CIP exceptional circumstances**.

- Observed shortcomings

The documented process does not include steps for implementation

No evidence of implementation

- AESO expectations

Process of how to configure the monitoring tools to retain applicable event logs identified in part 4.1 for at least the last 90 consecutive days for each applicable system.

Dated screenshots could be used to demonstrate implementation.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-AB-5 Table R5 – System Access Controls*.

Part 5.4 Change known default passwords, per **cyber asset** capability.

- Observed shortcomings

The steps included in the documented process for implementing Part 5.4 is too high level and generic

- AESO expectations

Process of ensuring that all know default passwords are changed before putting the cyber assets in service, such as commissioning checklists, quality check, change records management, etc.

Part 5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 **months**.

- **Observed shortcomings**

- No steps included in the documented process on “how” Part 5.6 is implemented

- Lack of evidence for demonstrating implementation

- **AESO expectations**

- Process of configuring the related authentication servers to enforce password changes or an obligation to change the password at least once every 15 months

- Dated screenshots of configuration could be used to demonstrate implementation

Part 5.7 Where technically feasible, either:

- limit the number of unsuccessful authentication attempts; or
- generate alerts after a threshold of unsuccessful authentication attempts.

- **Observed shortcomings**

The process of how to implement Part 5.7 is too high level

- **AESO expectations**

Process of configuring the related authentication servers to implement Part 5.7 including the documentation of account-lockout parameters

- **Good practices observed**

- Clear references in general

- Well organized IR responses with sufficient explanation

- Documented cyber security incident response plan addressing the sub-requirements

R1. Each Responsible Entity shall document one or more **cyber security incident** response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

Part 1.1 One or more processes to identify, classify, and respond to **cyber security incidents**.

- Observed shortcomings

Documented process has less emphasis on identification (e.g. focused on classification and response, not much on identification)

- AESO expectations

More emphasis on processes to identify cyber security incidents

Notes:

Processes to identify cyber security incidents could be in the form of observations, monitoring, alerting or other ways to detect possible cyber security incidents.

R2. Each Responsible Entity shall implement each of its documented **cyber security incident** response plans to collectively include each of the applicable requirement parts in *CIP-008-AB-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

Part 2.2 Use the **cyber security incident** response plan(s) under Requirement R1 when responding to a **reportable cyber security incident** or performing an exercise of a **reportable cyber security incident**. Document deviations from the plan(s) taken during the response to the incident or exercise

R3. Each Responsible Entity shall maintain each of its **cyber security incident** response plans according to each of the applicable requirement parts in *CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

Part 3.1 No later than 90 **days** after completion of a **cyber security incident** response plan(s) test or actual **reportable cyber security incident** response: 3.1.1. document any lessons learned or document the absence of any lessons learned; 3.1.2. update the **cyber security incident** response plan based on any documented lessons learned associated with the plan; and 3.1.3. notify each person or group with a defined role in the **cyber security incident** response plan of the updates to the **cyber security incident** response plan based on any documented lessons learned.

- Observed shortcomings

Not clear as to whether an exercise/ test of a reportable cyber security incident was performed during the audit period (e.g. evidence provided described as sample lessons learned exercise; attestation letter covered only actual incident)

- AESO expectations

Evidence clearly indicates:

- Exercises/ tests of reportable cyber security incidents during the audit period
- Actual reportable cyber security incidents during the audit period

Notes:

Requirements per Parts 2.2 and 3.1 are triggered by an actual reportable cyber security incident or an exercise of a reportable cyber security incident.

Sample evidence of implementation outside the audit period may be useful but not relevant in the assessment.

R3. Each Responsible Entity shall maintain each of its **cyber security incident** response plans according to each of the applicable requirement parts in *CIP-008-AB-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

Part 3.2 No later than **60 days** after a change to the roles or responsibilities, **cyber security incident** response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. update the **cyber security incident** response plan(s); and 3.2.2. notify each person or group with a defined role in the **cyber security incident** response plan of the updates.

- **Observed shortcomings**

Not clear as to whether a change to roles and responsibilities, cyber security incident response groups or individuals, or technology that the RE determines would impact the ability to execute the cyber security response plan occurred during the audit period

- AESO expectations

Evidence clearly indicating whether changes per R3.2 occurred during the audit period (e.g. use of non-event attestation letter)

Note:

Requirements per Part 3.2 are triggered by these changes.

- Good Practices observed

The recovery plan includes a list of backup procedures and a brief summary of the content, with references to the storage location

Conditions for activation are well-defined to meet the intent of CIP-009

Roles and responsibilities of responders are documented

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-AB-5 Table R1 – Recovery Plan Specifications*.

Part 1.2 Roles and responsibilities of responders.

- **Observed shortcomings**

Roles and responsibilities of responders are too generic and high level

The roles and responsibilities as documented in the Corporate disaster recovery plan are too high level

Unrelated document was submitted as evidence to demonstrate compliance

- **AESO expectations**

Roles and responsibilities of responders should be specific and clearly tied with the conditions of activation

Part 1.3 One or more processes for the backup and storage of information required to recover **BES cyber system** functionality.

- Observed shortcomings

Documented process for backup and storage of information does not cover all applicable systems. Common missing applicable system is physical access control system (PACS)

Documented processes for backup and storage of information lack formality such as title, scope, document reference number, version control, effective date, etc.

- AESO expectations

Documented process for backup and storage of information should cover all application systems as specified in CIP-009-AB-5

Process for backup and storage of information should include title, scope, document reference number, version control, effective date, etc.

Part 1.4 One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.

- Observed shortcomings

No or inadequate process to address backup failures

- AESO expectations

The process to address backup failures should include, at a minimum, the following:

- Identification of backup failures
- Notification process
- Mitigation measures

Part 1.5 One or more processes to preserve data, per **cyber asset** capability, for determining the cause of a **cyber security incident** that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.

- Observed shortcomings

The documented process is too high level and generic

- AESO expectations

One-size-fit-all approach is not appropriate, a process for each applicable system is suggested; define what data is preserved

Capability to document and preserve copies of network layout and configuration at the time of the attack, including network topology and the configuration of any routers and firewalls

Capability to preserve originals of any modified files, to ensure that your preservation process retains metadata (such as creation and last-modified dates)

Capability to preserve logs expeditiously as they may be deleted or overwritten as time passes

- **Good practices Observed**

Well-documented configuration change management process

Evidence is sufficient and appropriate to demonstrate compliance

The spreadsheets for identifying baseline configuration are well structured.

Automatic tools for monitoring configuration change

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R1 – Configuration Change Management*.

Part 1.1 Develop a baseline configuration, individually or by group, which shall include the following items:

–1.1.1. operating system(s) (including version) or firmware where no independent operating system exists;

- **Observed shortcomings**

Operating systems missed in baseline configuration

Several cyber assets missed in baseline configuration

- **AESO expectations**

The baseline configuration includes all applicable cyber assets and operating systems

Part 1.4 For a change that deviates from the existing baseline configuration:

- 1.4.1. prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
- 1.4.2. following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and
- 1.4.3. document the results of the verification.

- Observed shortcomings

Post change verification missed in the documented process

- AESO expectations

The Process includes post change verification

The results of the verification are documented

Part 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration:

- 1.5.1. prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and
- 1.5.2. document the results of the testing ...

- Observed shortcomings

No testing records being provided

- AESO expectations

All changes are tested

The results of the testing are documented

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R2 – Configuration Monitoring*.

Part 2.1 Monitor at least once every **35 days** for changes to the baseline configuration (as described in requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

- Observed shortcomings

 - Missed the due day

- AESO expectations

 - The changes to the baseline configuration are monitored at least once every 35 days

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-AB-1 Table R3– Vulnerability Assessments*.

Part 3.3 Prior to adding a new applicable **cyber asset** to a production environment, perform an active vulnerability assessment of the new cyber asset...

Part 3.4 Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments ...

- Observed shortcomings

One of applicable systems was not included in the documented process

- AESO expectations

The documented process should include all applicable systems

CIP-011-AB-1

Information Protection

- Good practices observed

Clear references in general

Documented information protection program and process on BES cyber asset reuse and disposal addressing the sub-requirements

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-AB-1 Table R1 – Information Protection*.

Part 1.1 Method(s) to identify information that meets the definition of **BES cyber system information**.

- Observed shortcomings

Insufficient information included in the documentation to allow RE's personnel to properly identify/ recognize BCSI

- AESO expectations

Methods used provide sufficient information to allow RE's personnel to properly identify/ recognize BCSI (e.g. use of a set of criteria or process)

Notes:

Effectiveness of implementation tools (e.g. training, communication) is dependent on the quality and content of these tools.

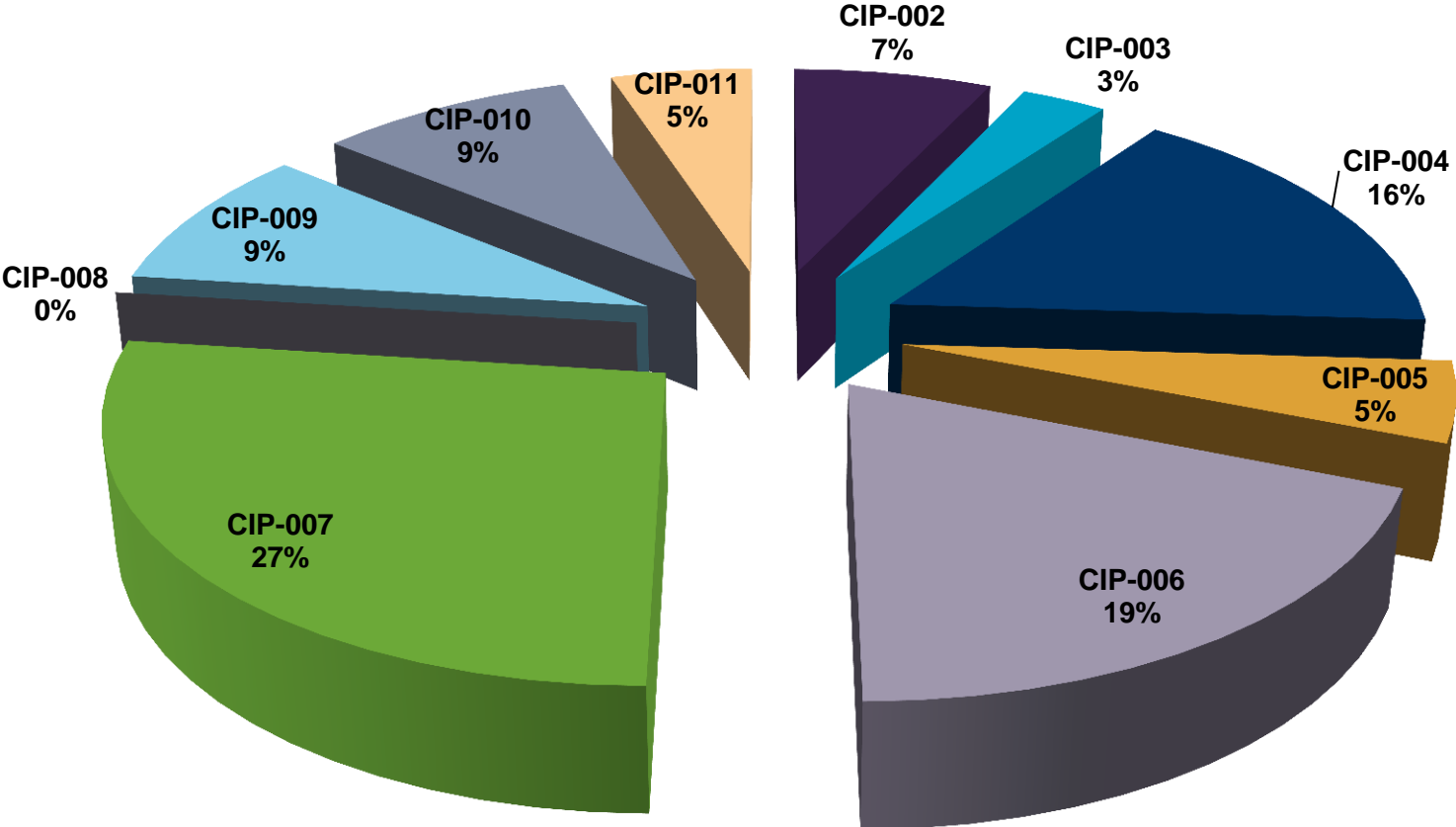
Training materials that provide personnel with sufficient knowledge to recognize BCSI is an example of acceptable evidence.

- The existing process went well; minimum extension of the timelines (2 weeks)
- The only change was in allowing submission of MPs comments in batches
- The timelines could/will be extended if there is an increased volume of suspected contraventions or positions

- Referrals

As per the normal process, sent to the MSA on the same day of issuing the Final audit report

CIP Pilot Audits Suspected Contraventions



Next Steps

- Planning two more CIP audits of companies with High/Medium Impact assets in 2019
- Same process is going to be used
- RSAWs to be updated and posted by mid-March 2019
- Separating the CIP audits for High/Medium Impact assets from the normal scheduled audits

rscompliance@aeso.ca

Thank you!