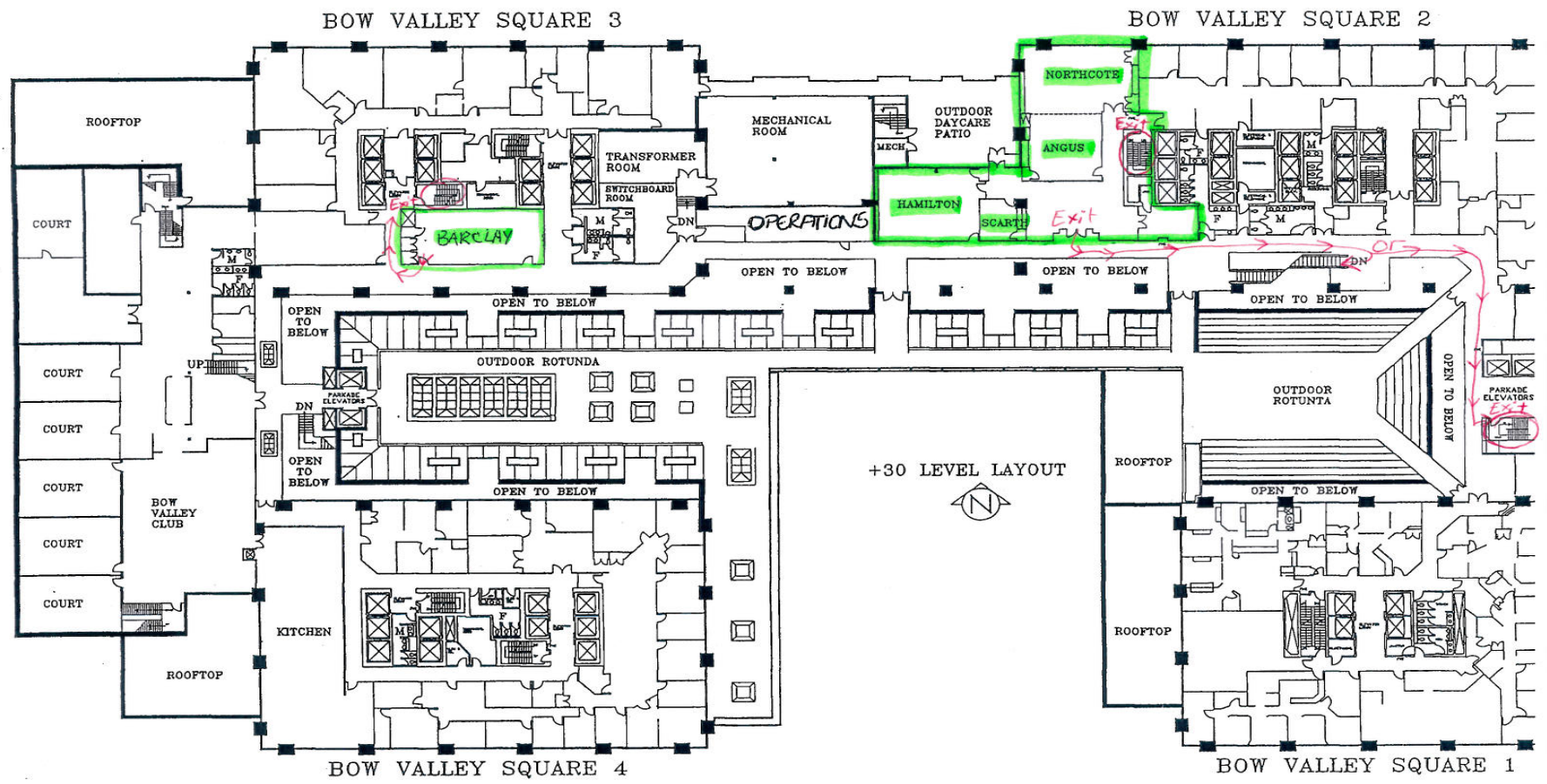


# CIP v5 Compliance Monitoring

October 25, 2017

- CIP Stakeholder Session
- AESO team
  - Daniela Cismaru, Jeff Norek, Chris Dittrick, Peter Wong
- Safety, Washrooms and Logistics

# Fire Procedure



- Session is booked from 9 am to noon
  - Will have one 15 minute break
  - Will cover the Agenda in a couple of slides
- Sign-in Sheet

- To provide understanding of the CIP compliance monitoring program and approach
  - Provides assurances to the industry that those involved in reliability and security are meeting the standards set out
  - What do you need to know to be ready to demonstrate you are compliant
  - Not about how to be ‘technically compliant’, but how to show you are if you are

- September 2015 – AUC approves set of CIP standards
- November 2016 stakeholder session
  - Provided the approach for monitoring CIP standards
  - Identified areas of concern, plans to address them through 2017
- Submitting TFEs – what’s the process?
- Clarity around the use of NERC Guidance material
- Clarity around the IAC language
- Clarity around the CMP

# Agenda

- Purpose and Objective
- CIP v5 Compliance Monitoring Approach
- Next Steps
- Q&A

- During the CIP v5 standards consultation we have committed to establish and bring to the market participants the approach used for monitoring CIP v5 compliance
- Provide an overview of the tools and processes as they relate to CIP v5 compliance evaluation
- Get your input and identify any concerns
- The end goal
  - CIP v5 compliance approach is well understood, effective, and efficient for the AESO and the market participants



# Compliance Monitoring Approach

- Compliance Monitoring Program
  - Tools, timelines, expectations (including information management)
  - Technical Feasibility Exceptions (TFE)
  - Identify, Assess and Correct (IAC)
- Supporting Documentation and Processes
  - Training and guiding documentation
  - AA (Applicability Assessment)
  - RFI (Request for Information, Waivers or Variances)
- Technical and Implementation Matters
  - IDs
  - CIP-PLAN

## *Facts and considerations*

- CIP v5 standards are new to the industry and the AESO
- Different degrees of understanding of standards content and intent
- High volume of requirements
- Significant number of requirements are technical vs. procedural
- NERC's auditors qualifications and designations

## *Approach*

- Reviewed the current program for suitability
- Identified and evaluated options
  - Continue with the current approach
  - Increase reliance on spot audit, and self-certification
  - Change it all together
- Engaged market representatives to identify potential issues and impact
- Assessed NERC's CIP methodology
- Hired external expertise to support the technical and the compliance reviews (AESI)

## *Outcome*

- The current Compliance Monitoring Program will be used for assessing companies' compliance with CIP v5 standards

- Two types of audits – scheduled audit and spot check audit
- Selected option - **Scheduled audit**
  - Commence with Q1/2018 audits
  - Notifications – send 30 days in advance of the evidence submission date, except for the first group of audited companies/mid-November
  - Scope - all CIP v5 requirements applicable to your company & subset of the power system
  - Duration of the audit – 3 months, except when High and Medium Impact assets are identified/extended up to 5 months

- Processes, timelines and documentation
  - Submission of evidence – approx. 1 month after the audit end date
    - Q1 – early February
    - Q2 – early May
    - Q3 – early August
    - Q4 – early November
  - Information Requests - response required within 2 or 5 business days (clarification/missing information vs. sampling)
  - Audit reports
    - Draft report – 10 business days to reply
    - Final report - 10 business days after receiving your comments
  - Referrals – on the same day of issuing the Final audit report

- RSAWs
  - Developed in 2015 based on NERC RSAWs
  - Comprehensive review in 2017
    - Market's inquiries and the lessons learned during the AESO's implementation were considered
    - Outcome - no changes to the RSAWs
  - [Link to the external website - https://www.aeso.ca/rules-standards-and-tariff/compliance/alberta-reliability-standards-compliance/](https://www.aeso.ca/rules-standards-and-tariff/compliance/alberta-reliability-standards-compliance/)

# Compliance Monitoring Approach – Audit

- Submission of evidence - business as usual
  - Email, USB, mail delivery



.... Good old times....



# Compliance Monitoring Approach – Audit Information Management

- Information Management
  - Currently managed in accordance to ISO Rules 103.12 and 103.1, meaning that all information obtained, created or exchanged during an audit must be handled with confidentiality
  - CIP011 “Cyber Security Information - Information Protection” triggered a comprehensive review of existing processes and practices

# Compliance Monitoring Approach – Audit Information Management

- Scenario 1: CIP-011 applies to your company
  - A new information exchange mechanism in place
- Scenario 2: CIP-011 does not apply to your company
  - The new information exchange mechanism is optional

## Information Exchange



## Internal Management



# Compliance Monitoring Approach – Audit Information Management

- Information Exchange
  - Pertains to
    - Evidence received by the AESO
    - IRs (issued and responses)
    - Audit reports
    - Referrals
    - Any information required by the MSA after the submission of the referral (Note: it may be used as the cc mechanism of the self-reports)
  - Solution developed by the AESO with input from market's representatives
  - Training will be provided in advance of the audit

# Compliance Monitoring Approach – Audit Information Management

- Internal management of information
  - Pertains to all information obtained, created or exchanged during the audit
    - Self-Reports
    - Evidence received by the AESO
    - IRs (issued and responses)
    - Completed RSAWs
    - Auditors' notes
    - Internal decisions summaries
    - Audit reports
    - Meeting notes
    - Referrals

# Compliance Monitoring Approach – Audit Information Exchange

## *Solution: SharePoint Online File Sharing*

- AESO Security Assessment
  - Thorough assessment of vulnerabilities, threats, impacts and risks to SharePoint Online services
  - Review and assessment of Microsoft SOC 2 report
  - NDA with Microsoft covers all data in AESO tenant
- Data & Storage
  - All data stored in Canadian data centres (primary and backup)
  - Encryption At Rest: BitLocker with AES 256-bit encryption on servers
  - Encryption In Transit: TLS/SSL with client machines

# Compliance Monitoring Approach – Audit Information Exchange

- Security Controls
  - 2-Factor authentication activated on all AESO accounts
  - Complex password requirements
  - Access to information further controlled with SharePoint site level permissions groups, company data and access always segregated at site level
  - Ability to access user data disabled
  - Each market participant is responsible for managing their users' login security

# Compliance Monitoring Approach – Audit Information Exchange

- Secure Processes
  - All permissions changes follow strict procedural control
  - Permissions changes performed by Application Administrators
  - Limited exposure: information uploaded to SharePoint is downloaded and deleted, never left online for extended periods of time
- Access to Information
  - ARS Compliance Team
  - SOs/SMEs/MSA based on need; assessment done by Manager
  - Application Administrators
- Audit & Logging
  - All activities in O365 are logged and are auditable

# Compliance Monitoring Approach – Audit Internal Management of Information

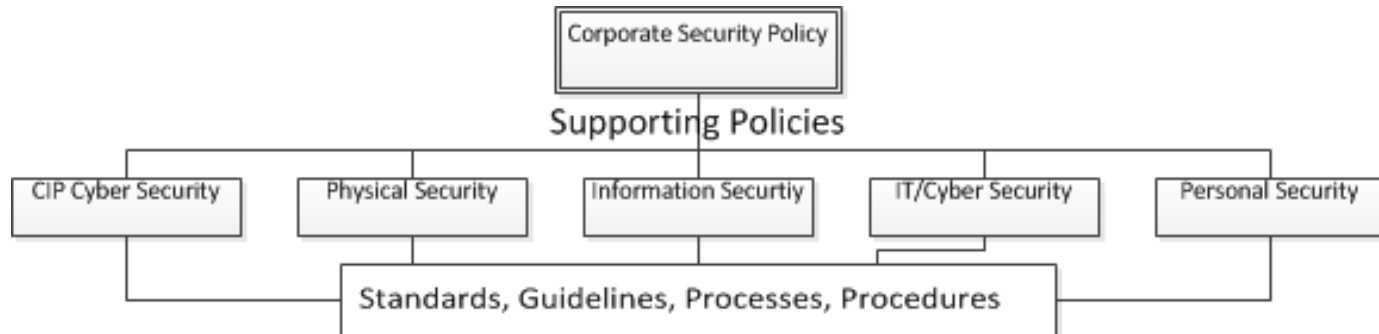
## *Overview*

- AESO Information Security Program
  - Information Security Program
  - Information Classification Scheme
- AESO's CIP Program (specific to information protection)
  - AESO CIP-011 Practice
  - AESO CIP-004 Practice
- Handling Market Participant (MP) Information



# Compliance Monitoring Approach – Audit Internal Management of Information

- AESO Information Security Program



- AESO Information Classification Scheme

- Public
- AESO Internal
- AESO Protected
- AESO Protected CIP

- Information Classification establishes the basis on which security controls are applied to given information

## AESO's CIP Program Structure (AESO Protected CIP)

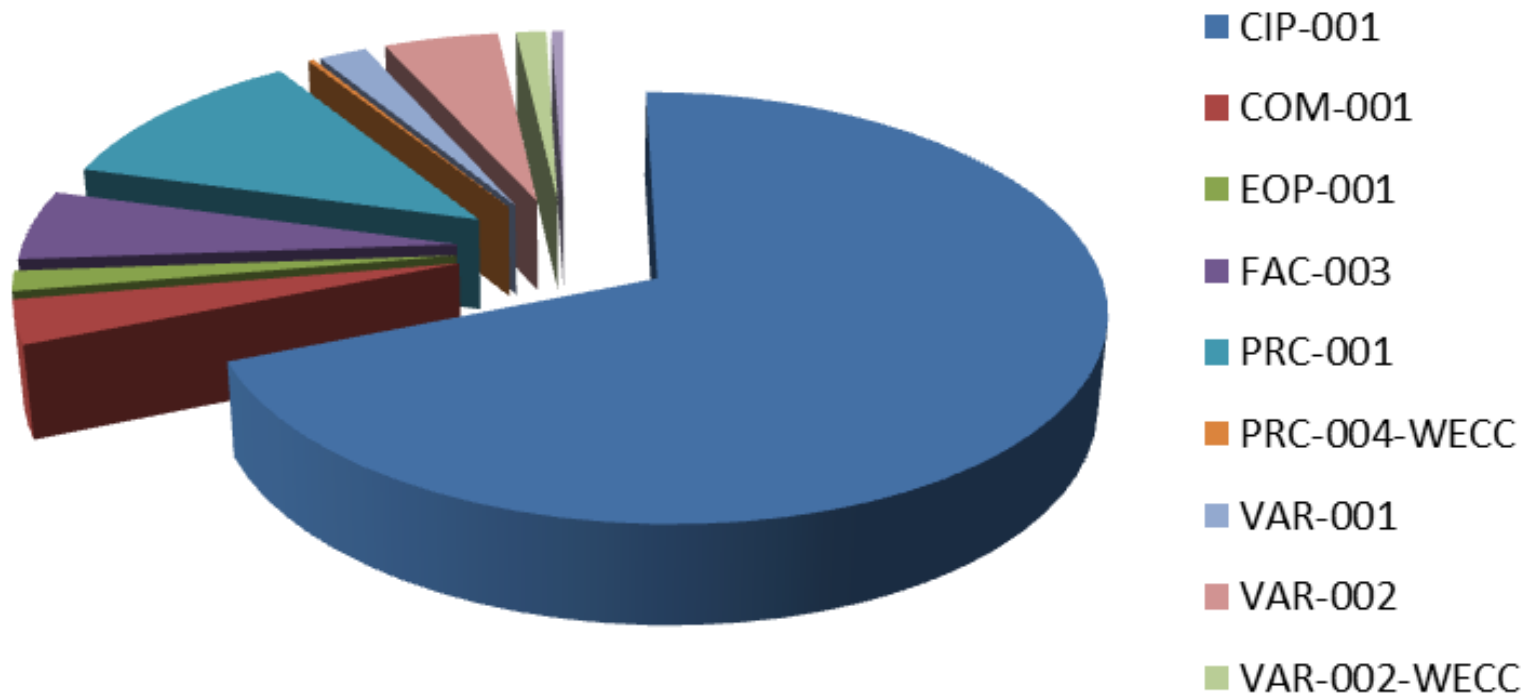
- CIP Cyber Security Policy
- 10 Standards each with accountable Standard Owner
- Each Standard has defined and formally accepted Internal Business Practices (IBPs)
- CIP-011 Practice
  - R1: Identify → Mark → Store (Designated Storage Location - DSL)
  - DSL list is maintained by the Corporate Security Team
  - R2: Information Handling: Information Security Standard defines how AESO Protected CIP information will be handled and protected through it's lifecycle
- CIP-004 Practice
  - DSL links both CIP-011 and-CIP 004 standards
  - CIP-004 uses DSL to monitor and report on access management to locations identified in the DSL list

# Compliance Monitoring Approach – Audit Internal Management of Information

- Handling Market Participant (MP) Information
  - MP information is marked as **AESO Protected CIP**
  - All security controls associated with **AESO Protected CIP** are afforded to MP's information
  - Subject to WECC audit
  - Independent attestation on AESO's Security Controls

- Mid-2018 the AESO will perform a comprehensive review of the Q1 and Q2/2018 audits performance and make changes if necessary
  - Pilot approach
  - Evaluate internal and external preparedness (focus of evidence)
  - Alignment on understanding the standards (wording, intent)
  - # of IRs and quality of the replies

## Suspected Contraventions



# Compliance Monitoring Approach – Self-Certification

- Status quo
- Annual self-certification required on all applicable requirements
- Letters submitted via emails or USBs
- Sharepoint Online access provided if the technical assessment of the self-certification letter pertains to or requires BCSI

- “where technically feasible” term referenced in some CIP v5 requirements
- CIP-SUPP-002 – allows for submission and approval or disapproval of Technical Feasibility Exceptions (TFE)
- ID #2016-005RS includes
  - Criteria for approval
  - Request form
  - Submission, Review, Approval and Amendment processes
- TFE process is not a compliance process
- All information pertaining to a TFE is treated as “AESO CIP Protected”

- Compliance assessment of approved TFEs
  - Up to the date of the TFE approval, in accordance to the requirement
  - After the TFE approval, in accordance to the TFE's conditions
  - If found in contravention, the approved TFE will be provided to the MSA for reference



- “identifies, assesses and corrects” term used in a subset of CIP v5 requirements
- Section 5 of ID #2015-003RS clarifies:
  - The language is going to be removed from future versions of the CIP standards
  - In the meantime, reliance on the self-report, with focus on the mitigation plan

- Compliance expectations
  - Evidence that the market participant is able to identify deficiencies in meeting the technical part of the requirement
  - Records of each identified deficiency in meeting the technical part of the requirement
  - Records of the result of an assessment made of each identified deficiency in meeting the technical part of the requirement
  - Records of the mitigating actions made to correct each identified deficiency in meeting the technical part of the requirements
  - Evidence that each identified deficiency in meeting the technical part of the requirement was corrected

- Compliance processes training
  - Available to market's representatives
  - Targeted audience are the Compliance representatives, but it could be beneficial to SOs/SMEs
  - Provided a few days after the Audit or Self-Certification notifications are issued
  - On-line training provided on the external website - <https://www.aeso.ca/rules-standards-and-tariff/compliance/alberta-reliability-standards-compliance/>

- Documentation and guides
  - Posted externally - <https://www.aeso.ca/rules-standards-and-tariff/compliance/alberta-reliability-standards-compliance/>
  - No updates were viewed as necessary

- Applicability Assessment (AA)
  - Requests could be made for assessing applicability of:
    - Functional Entity
    - Reliability Standard
    - Requirement
    - Facility, generating unit
  - While AA is not a Compliance process, [rscompliance@aeso.ca](mailto:rscompliance@aeso.ca) used to receive request and communicate assessments
  - Observations:
    - AA is not meant to support confirmation of non-applicability
    - CIP-002/R2.12 - each control centre or backup control centre used to perform the functional obligations of the operator of a transmission facility (*transmission facilities at 2 or more locations*)

- Request for Information, Waivers or Variance (RFI)
  - Requests to be sent at [RFI@aeso.ca](mailto:RFI@aeso.ca)
  - This is not a Compliance process
  - Assessment could result in an ID being issued or updated (compliance evaluation takes the IDs into considerations)

- New CIP ARS Terms and Definitions
  - Referenced on the landing page off all CIP v5 standards
- ID #2015-003RS
  - Section 2 – Use of NERC Guidance Information for the CIP Standards
- #2016-006RS
  - Radial Circuit
- CIP-PLAN
  - Most of the requirements in effect as of October 1, 2017
  - Exceptions referenced in the CIP-Plan

# Next Steps

- Audit Notifications
  - For Q1/2018 - mid-November 2017
- Audit training
  - Provided by the AESO - late November/early December 2017
  - On-line training
- Self-Certification notifications
  - Cycle 4, 2017 – October 31, 2017
- Self-Certification training
  - November 29, 2017
- SharePoint Online training
  - January 2018; future communication to work on the details



# Next Steps

- Questions, concerns, issues pertaining to CMP, training, documentation: [rscompliance@aeso.ca](mailto:rscompliance@aeso.ca)
  - We are committed to a timely response
  - Provide details, reasons, impact, constraints
- Feedback opportunity



**Thank You!**