ISO Rule 501.2
Security of Critical Facilities
Stakeholder Session

Alberta Electric System Operator
March 27, 2015

Introductory Remarks

- AESO team introductions
- Safety
- Objectives of this session:
  - Facilitate an understanding of Rule 501.2 and how the AESO plans to monitor compliance to it
  - Provide an opportunity for stakeholders to seek clarity

Agenda

- Rule 501.2
  - History
  - Rule requirements
  - Relationship to CIP Standards
- Compliance Monitoring
  - AESO Compliance mandate and processes
  - ISO Rule 501.2 monitoring process
  - Site-assessment template walkthrough
- Q&A

Rule 501.2

- History
  - Formerly, Security Management Regulation (AUC Act)
    - EUB → AUC → AESO
  - ISO Rule 501.2, Security of Critical Facilities
    - Effective January 1, 2013
    - Available on AESO website:

http://www.aeso.ca>rules&standards>current ISO rules

Rule 501.2

- Applicability
  - a legal owner of a critical facility, being an electric industry facility named in the critical infrastructure list established under the Alberta Counter-Terrorism Crisis Management Plan (ACTCMP); and
  - the ISO
- Dependent resources
  - ACTCMP
  - Directive 071, Emergency Preparedness and Response Requirements for the Petroleum Industry (Directive 071)

Rule 501.2

- Rule 501.2 requirements for legal owners - highlights
  - Establish security measures in accordance with ACTCMP
  - Establish corporate emergency response plans in accordance with Directive 071
  - Demonstrate capacity to implement such measures and plans
  - Inform the ISO of threats to critical facilities and implement security measures

Rule 501.2 vs. …

- CIP-001-AB1-1 Sabotage Reporting
  - Reporting and notification only
- CIP-006-AB-5 Physical Security of BES Cyber Systems (awaiting approval)
  - Controls for securing BES cyber assets
  - Restrict access; monitor/log/alert; visitors; PACS
- CIP-014 Physical Security (under review)
  - Only TO and TOP Tx facilities
  - Risk assessment and security plan

AESO Compliance

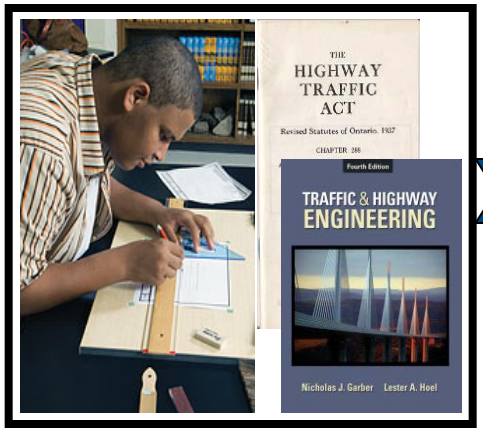
Mandate and Processes

Compliance
Underlying Legislation

- The *Electric Utilities Act* (EUA):
  - Requires market participants to comply with ISO rules (s. 20.8)
  - Establishes the AESO as the compliance monitoring entity for the ISO rules (s. 17)
  - Requires the AESO to refer compliance matters to the Market Surveillance Administrator (MSA) if the AESO suspects that a market participant has contravened an ISO rule or reliability standard (s. 21.1)

AESO Compliance

Alberta Compliance and Enforcement Model



Rules
AUC / AESO

Policing
AESO
Compliance

Penalties/
Enforcement
MSA or AUC

Disputes/
Hearings
AUC

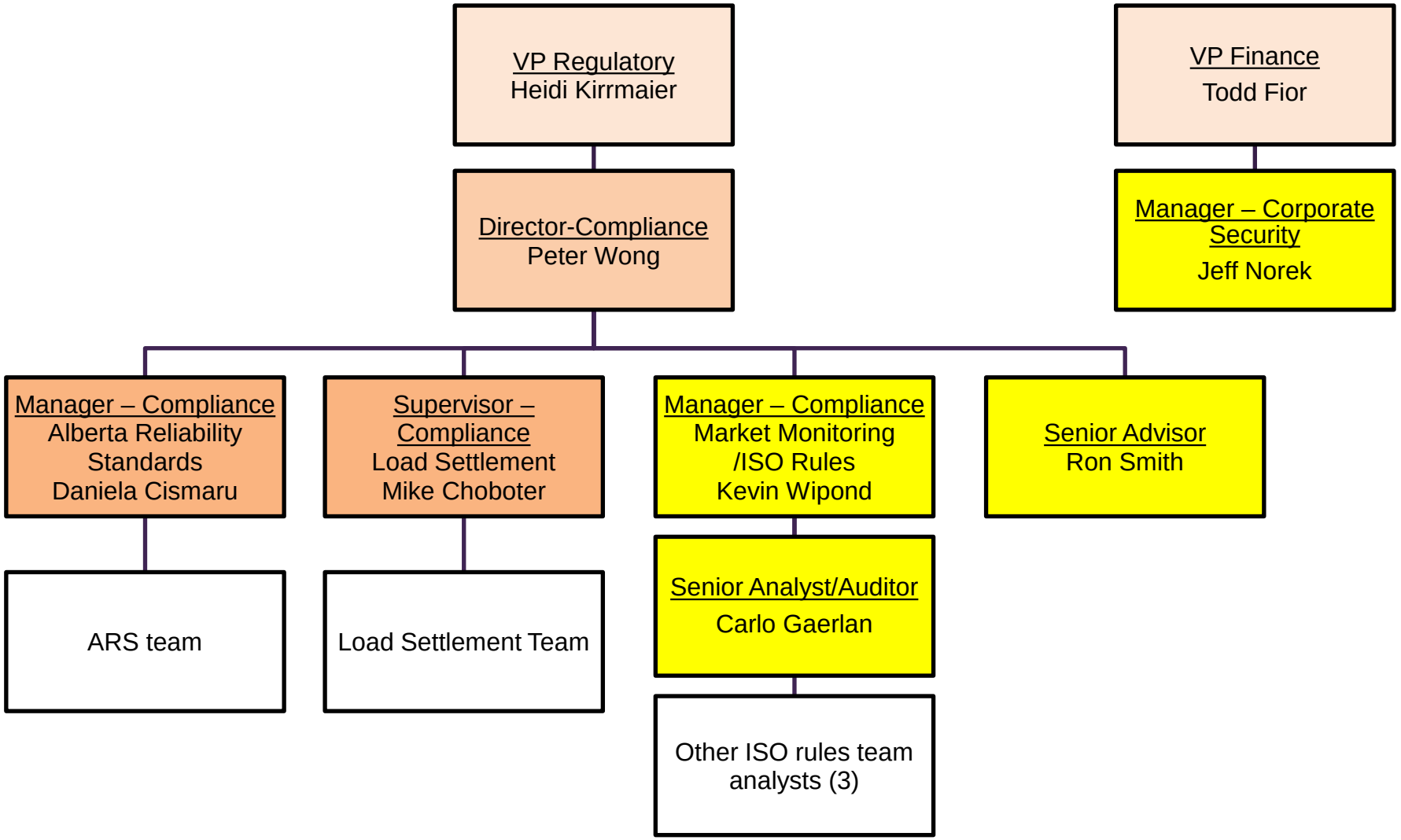
Agencies and Roles (specific to compliance)

- AESO
  - Monitors market participant behavior in regards ISO rules, technical requirements and standards, Ancillary Services contracts, Alberta Reliability Standards, and Settlement System Code Rule
  - Refers suspected contraventions to the MSA or the AUC, as appropriate
  - Serves as an expert witness in AUC hearings re these contraventions
- MSA (Market Surveillance Administrator)
  - Monitors the market for performance and anti-FEOC behaviors
  - Receives referrals from AESO regarding suspected ISO rule or ARS contraventions and decides on penalty/forbearance
  - Prosecution in AUC hearings re ISO rule or ARS contraventions
- AUC (Alberta Utilities Commission)
  - Approves the ISO rules and ARS
  - "Owns" the Settlement System Code Rules (AUC Rule 021)
  - Defines the 'specified penalties' for contravention of ISO rules and ARS (AUC 019, AUC 027)
  - Conducts hearings for contested ISO rule and ARS contraventions
  - Receives referrals from AESO regarding contraventions of Settlement System Code Rules

AESO Compliance
Main Functional Areas

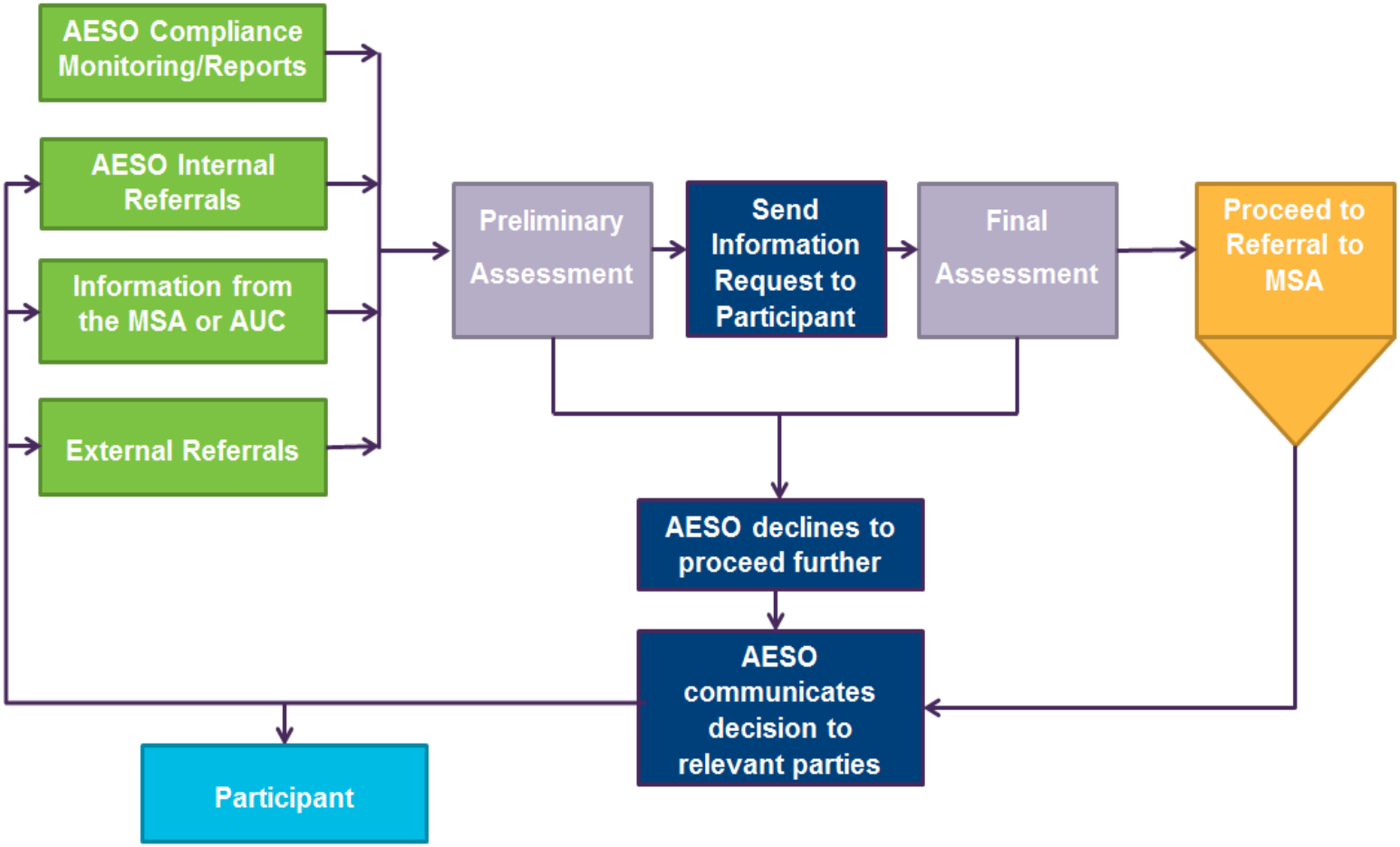
- **ISO rules Compliance - Monitoring the behavior of market participants (e.g. marketers, generators, load, transmission operators, etc.) with regard to ISO rules, including OPPs**
- ARS Compliance - Monitoring of the market participants compliance with Alberta Reliability Standards (ARS)
- LS Compliance - Monitoring of the market participants with Load Settlement (AUC Rule 021)
- (No role with ISO Tariff compliance)

AESO Compliance Team



ISO Rules Compliance Process

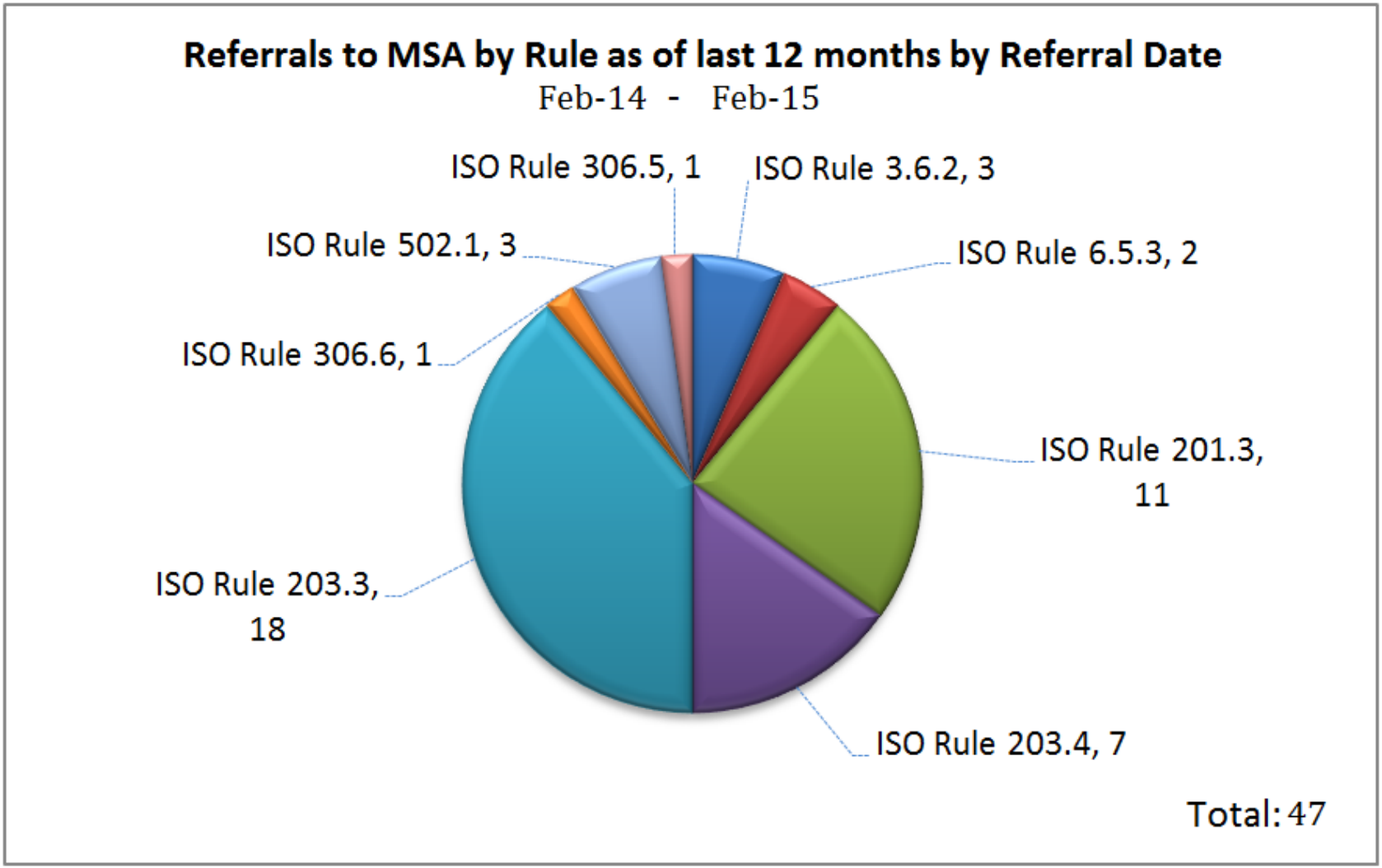
General Assessment Process



ISO Rules Compliance Process

- Referral to MSA
  - MSA handles – Generally independent of the AESO
  - Additional opportunity for market participant to argue their case
  - MSA has discretion to forbear vs specified penalty or administrative penalty
  - Possible MSA/AESO discussion re: impact, rule interpretation
  - AUC hearings – AESO as expert witness

MSA Referrals



MSA Website


http://albertamsa.ca/index.php?page=2015-4
Alberta MSA - 2015
Convert
Select
Site Map | Contact Us | Complaint
MSA
Market Surveillance
Administrator
Home
About Us
Market Reporting
Compliance
Consultations
Guidelines
Retail Statistics
Privacy/Access
Archive
Compliance Process
ISO Rules
Reliability Standards
Compliance Reports
Compliance Presentations
MSA Investigation Procedures
Specified Penalties
Forms
2015
2014
2013
2012
2011
2010 and Older
2015
Notice of Specified Penalty - MSA
Notice of Specified Penalty - MSA
Notice of Specified Penalty - MSA
Notice of Specified Penalty - MSA 2014-421
The Market Surveillance Administrator is an independent enforcement agency that protects and promotes the fair, efficient and openly competitive operation of Alberta's wholesale electricity markets and its retail electricity and natural gas markets. The MSA also works to ensure that market participants comply with the Alberta Reliability Standards and the Independent System Operator's rules.
Copyright © 2010 Market Surveillance Administrator Home | Disclaimer | Site Map | Contact Us Designed by eKzact Solutions Inc

MSA Self-Reporting Process

- MSA ‘Compliance Process’ document (MSA website) defines a self-reporting process for ISO rules contraventions
- Incentive for market participants to track and identify their own non-compliance with ISO rules
- MSA determines handling – Forbearance based on satisfying MSA conditions
- 300-400 self-reports per year

Compliance Monitoring Confidentiality

- Information, recommendations and referrals to the AUC or MSA treated as confidential
- Source of any complaint regarding compliance treated as confidential
- Resources
  - AESO Commercially Sensitive Data Policy (internal)
  - ISO rule 103.1, Confidentiality
  - ISO rule 103.12, Compliance Monitoring

ISO Rule 501.2

Monitoring Process

Compliance Monitoring of Rule 501.2

- Why a new Compliance Monitoring Program for Rule 501.2?
  - Each ISO rule can require specific approaches to monitoring which are different than other ISO rules
  - AESO has two years experience with Rule 501.2 and has assessed that an active monitoring program will be the most effective
  - Leverages relationship with the Energy Security Unit (ESU) of the Justice and Solicitor General Branch
    - Extensive experience and expertise with ACTCMP obligations
    - Owner of the critical facility list
    - In a position to conduct site visits

Compliance Monitoring of Rule 501.2

- ISO may audit the security measures in respect of a critical facility and the capacity of the legal owner to implement those security measures
- ISO may audit the corporate emergency response plan and the legal owner’s capacity to implement the plan
- Combination of self-assessments and on-site reviews by the ESU

Compliance Monitoring of Rule 501.2 Self-Assessment

- Legal owner registration process
- Legal owner to perform self-assessment of its compliance with Rule 501.2
- Scheduled annual submissions by legal owner
- AESO worked with ESU in developing the template
  - Considered ACTCMP and Directive 071, as it applies to the electric industry
  - Contains a comprehensive summary of considerations from ACTCMP and Directive 071 (e.g. facilities, personnel, cyber)
  - Template will be published on AESO website

Compliance Monitoring of Rule 501.2 Self-Assessment - Process

1. ISO to notify legal owner of requirement to submit self-assessment
2. Legal owner to complete self-assessment template
   - Legal owners will be given 20 business days to prepare and submit the self-assessment
   - Approval by an Officer of the legal owner
3. AESO will review the self-assessments with two possible outcomes
   a. No further investigation required - END OF PROCESS
   b. Potential suspected contravention(s) identified

Compliance Monitoring of Rule 501.2 Self-Assessment - Process

4. AESO will send Information Request to legal owner
   - Typically 10 business days to respond to Information Request
5. AESO will review Information Request response and make its determination
   - Two possible outcomes:
     a. No suspected contravention(s) identified – Not pursuing letter
     b. Suspected contravention(s) identified – Referral to the MSA
   - Legal owner will be notified of the referral
   - MSA decides on penalty or forbearance
6. If no non-compliance has been identified, notification will be provided.

Compliance Monitoring of Rule 501.2
On-Site Review

- ESU will perform on-site reviews of selected critical facilities on behalf of the AESO
- Objective: Provide the AESO with information to assess whether or not Rule 501.2 may have been contravened
- Scheduled annual on-site reviews of selected critical facilities.

Compliance Monitoring of Rule 501.2
On-Site Review - Process

1. Annually, AESO will select a subset of critical facilities that will be subject to on-site visits.
   - Each facility will be tentatively subject to an on-site review every 2-3 years or more frequently as required.
   - The legal owner will will receive advance notification of requirement for ESU to make a site visit
   - Legal owner must coordinate specific date(s) of site visit with ESU

Compliance Monitoring of Rule 501.2
On-Site Review - Process

2. ESU will perform detailed on-site visit
   - Evaluate the site's physical security measures, threat mitigation strategies and emergency response plans.
   - Detailed review of both security plan and emergency response plan
   - Assessment of capability of implementing both plans
   - Complete an assessment report and submit to the AESO
3. AESO and ESU discuss results of on-site review – 2 possible outcomes
   - No concerns – no further assessment – END OF PROCESS
   - Concerns identified – proceed to compliance assessment
4. AESO will send Information Request to legal owner

Compliance Monitoring of Rule 501.2
On-Site Review - Process

5. AESO will review Information Request response and make its determination
   - Two possible outcomes:
     a. No suspected contravention(s) identified – Not pursuing letter
     b. Suspected contravention(s) identified – Referral to the MSA
   - Legal owner will be notified of the referral
   - MSA decides on penalty or forbearance
6. If no non-compliance has been identified, notification will be provided.

Other Compliance Actions

- In addition to scheduled self-assessments and scheduled ESU site visits…
  - AESO has the authority to either request information (IR) or schedule an ESU site visit at any time (with reasonable notice)
  - Typically only in a situation where the AESO has become aware of potential non-compliance through other information – complaint, internal referral, etc.

What is a ‘suspected contravention’?

- AESO must refer all ‘suspected contraventions’ to the MSA
- AESO first carries out a ‘due diligence’ process to gather all evidence available (incl. from the market participant)
- Advisory nature of ACTCMP
- Directive 071 written to apply to energy industry
- Compliance will assess the potential state of non-compliance based on the nature of the ACTCMP, Directive 071 and augmented by a reliance on discussions with internal and ESU experts
- MSA has the final say after any referrals

Legal Owner Registration Process

- New process will require certain types of legal owners to register with the AESO, including legal owners of a critical facilities
- No current visibility of the identity of legal owners
- For assets with multiple legal owners, they can elect to have designated representative for compliance purposes
- Registration will be on a critical facility specific basis

Legal Owner Registration Process

- Will facilitate a more efficient monitoring process
- Initial registration process will be completed before the new Compliance Monitoring Program for Rule 501.2 becomes effective
- Implementation details will soon be published to the AESO website along with reminders in the AESO Stakeholder Newsletter

Self-Assessment Template Walkthrough

Template Walkthrough

- Template is 30 pages in total and consists of 3 parts:
  - Part 1: Security Measures for a Critical Facility
  - Part 2: Corporate Emergency Response Plans
  - Part 3: Declaration
- To be completed only when a notification from the AESO has been received
- Checklist format (in Word) with spaces provided for explanations

Template Walkthrough

- Always check for the latest version of the template
  - AESO's website under Compliance > ISO Rules > ISO Rule 501.2 Compliance Monitoring
- The self-assessment must be submitted to the AESO in both, Portable Document Format (PDF) and original electronic MS Word format.
- The self-assessment form must be signed by the appropriate officer of the organization.

Template Walkthrough

- Enter the site number of the facility – 1 Self-Assessment for each critical facility (stand-alone)

Critical Facility Site No.:

- Parts 1 and 2 start with…

Background				
	Yes	No		Comments
Does the facility have an approved threat response plan in place?	☐	☐		[Replace this text with information such as who approved the plan, when was it approved, when was it last updated and was was the current/updated plan communicated to involved parties.]

Background				
	Yes	No		Comments
Does the facility have an approved corporate emergency response plan in place?	☐	☐		[Replace this text with information such as who approved the plan, when was it approved, when was it last updated and was was the current/updated plan communicated to involved parties.]

Template Walkthrough

FACILITY SECURITY PROGRAM	Description	Documented in the plan?			If Yes, please provide description of the security measure(s) applicable. If No or NA, please explain why and note the compensating security measure(s).	Able to implement?		Additional explanation on capability to implement the security measures
		Yes	No	N/A		Yes	No	

- Facility Security Program – lists actions and areas of concern where security measures are expected
- Description of each action and area of concern is included to provide common understanding
- Checkboxes to confirm documentation in the plan (Y, N, N/A)
- Checkboxes to confirm ability to implement what is in the plan
- Provide adequate explanations

Template Walkthrough

- Declaration is a confirmation of completeness and accuracy of the self-assessment

Part 3: Declaration

I confirm that the information given on this self-assessment form and in any documents attached are correct and complete.

Name of officer and position:	Signature:
Telephone:	Date:

Template Walkthrough

Part 1: Security Measures of a Critical Facility

Sample documentation 1:

FACILITY SECURITY PROGRAM	Description	Documented in the plan? Yes	No	N/A	If Yes, please provide description of the security measure(s) applicable. If No or NA, please explain why and note the compensating security measure(s).	Able to implement? Yes	No	Additional explanation on capability to implement the security measures
i. *Security Plan*						☐	☐	
	a. Separate security plan in place; circulation centrally controlled	☒	☐	☐	Marked with internal security marking "ABC Confidential"	☒	☐	Currently controlled by corporate security, only circulated to personnel with a need to know.
	b. Record of past and current problems	☒	☐	☐	Corporate security review security incidents and logs.	☒	☐	Done as needed in response to security incidents.
	c. Security threat response plan is layered	☒	☐	☐	Site is considered a high critical infrastructure, will always maintain a MEDIUM threat response.	☒	☐	Security threat response plan is designed to respond to MEDIUM threat level.
	d. Security threat response plan allows for increased threat level	☒	☐	☐	Details roles/responsibilities of positions at higher threat levels.	☒	☐	All affected positions have received training and education of the security threat response plan. Most recent training was done on January 1, 2015.
	e. Periodic review of security threat response plan	☒	☐	☐	Corporate security to review bi-annually.	☒	☐	The 2 most recent reviews were done on June 1, 2014 and December 1, 2014.

Template Walkthrough

Part 1: Security Measures of a Critical Facility

Sample documentation 2:

FACILITY SECURITY PROGRAM	Description	Documented in the plan?			If Yes, please provide description of the security measure(s) applicable. If No or NA, please explain why and note the compensating security measure(s).	Able to implement?		Additional explanation on capability to implement the security measures
		Yes	No	N/A		Yes	No	
j. Protocols	• Make contact with liaison personnel in local fire, police, emergency management, media, suppliers, customers, etc. • Establish regular communication with liaison contacts. • Implement emergency communication procedure with all site personnel.	☐	☒	☐	Corporate security is responsible for providing "security liaison with external parties", but points of contact are not identified in the security plan. Emergency contacts are identified in CIP-001 AND Business Continuity Plan; nature of threat would determine whether BCP would be implemented. Corporate communications manages employee call-out system; system is tested as part of crisis communication exercises.	☒	☐	The entity tested the BCP within the past 12 months.

Template Walkthrough

Part 2: Corporate Emergency Response Plan

Sample documentation:

Directive 071 Requirements	Description	Documented in the plan?			If Yes, please provide some description as documented in your plan. If No or NA, please explain why and note the compensating measure(s).	Able to implement?		Additional explanation on capability to implement
		Yes	No	N/A		Yes	No	
2.1.4 Incident Management Systems								
	• ERP describes how it will manage and coordinate a response to an emergency	☒	☐	☐	The entity has defined an Incident Command System (ICS).	☒	☐	The entity tested the ERP within the past 12 months.
	• ERP address the roles and responsibilities of personnel at on-site command post, regional emergency operations centre (REOC), and the corporate EOC	☒	☐	☐	The ERP defines the roles and responsibilities of all entity personnel outlined in the ICS.	☒	☐	The entity tested the ERP within the past 12 months.
	• ERP clearly outlines the communication protocols and procedures	☒	☐	☐	The ERP outlines procedures for communications between entity personnel and emergency response personnel.	☒	☐	The entity tested the ERP within the past 12 months.

Template Walkthrough

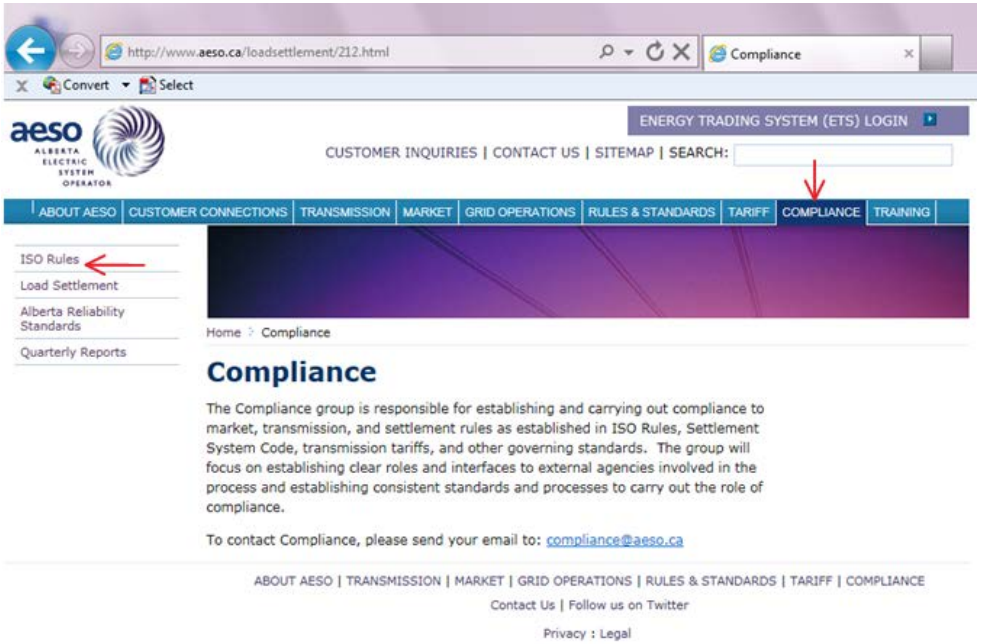
- Subsequent years…
  - If there is a new version of the template, complete a new form
  - If the template version is the same, you may use the old submitted form and update as necessary

Compliance Monitoring of Rule 501.2 Tentative Schedule

- Advance notification will be sent in April or early May 2015
- Self-Assessment process will commence in mid-May 2015
- On-site reviews will commence in July 2015
- A notification will be sent for each critical facility notifying the legal owner that either an on-site review will be performed or a completion of the AESO security assessment is required
- The AESO plans to select a number of critical facilities each year to be subject to the on-site reviews

Compliance Monitoring of Rule 501.2 Resource Documents

- New page in ISO Rules
  - "ISO Rule 501.2 Compliance Monitoring"



- Resources:
  - Compliance Monitoring Program Guide
  - Self-Assessment template
  - Stakeholder Session slides

Questions

- Contact us:

AESO Compliance

securityrulecompliance@aeso.ca

Jeff Norek

Manager, Corporate Security

jeffrey.norek@aeso.ca

Kevin Wipond

Manager, Compliance – ISO Rules

kevin.wipond@aeso.ca

Discussion

Thank you