• **8:10 – 8:40 a.m.:** CIP v5  
  - Felek Abbas

• **8:40 – 9:00 a.m.:** CIP-014 Physical Security  
  - Felek Abbas

• **9:00 – 9:30 a.m.:** CIP Modifications Standards Development Update  
  - Sean Cavote  
  - Katherine Street  
  - Mat Bunch

• **9:30 – 9:45 a.m.:** Internal Controls (Recent Changes to the Guide, Current Expectations)  
  - Ryan Mauldin
Today’s Agenda

- **9:45 – 10:15 a.m.:** Break
- **10:15 – Noon:** Panel-Operationalizing Compliance: Internal Controls (ERO Enterprise update, Registered Entity lessons learned and experiences)
  - Ryan Mauldin
  - Joseph Suich
  - Kelly Montanaro
  - Terry Bilke
  - Nicole Mosher
  - Kim Moulton
- **Noon – 1:00 p.m.:** Lunch
Today’s Agenda

- **1:00 – 2:30 p.m.:** Compliance Exception Discussion and Making the Process Work for You
  - Ed Kichline
- **2:30 – 2:45 p.m.:** Break
- **2:45 – 4:15 p.m.:** NERC Standards Development Update, Periodic Reviews, IRO-002-5 and TOP-001-4 Implementation
  - Steven Noess
  - Sean Cavote
  - Soo Jin Kim
- **4:15 – 4:45 p.m.:** NERC Legal Update
  - Shamai Elstein
Today’s Agenda

• **4:45 – 5:00 p.m.**: General Q&A and Closing Announcements
  - Laura Anderson
  - Latrice Harkness
Questions and Answers
Interactive Remote Access

Felek Abbas, NERC, Senior CIP Compliance Advisor
2017 Standards and Compliance Workshop
July 12, 2017
Interactive Remote Access

- User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1. Cyber Assets used or owned by the Responsible Entity, 2. Cyber Assets used or owned by employees, and 3. Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
CIP-005-5, Requirement R1, Part 1.1

- All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
Intermediate System

- A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.
CIP-005-5, Requirement R2

- Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
- For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
- Require multi-factor authentication for all Interactive Remote Access sessions.
Standalone Machines
Serial Communications

Modem Bank

Serial Device

Serial Device

Serial Device

Serial Device

Serial Device

Analog Leased Line
Serial to IP Conversion

BES Cyber Asset #1

Port Server

BES Cyber Asset #2

Intermediate System or Similar

Routable Communications

Serial Communications
CIP-005-5 Noncompliance
7/1/2016 - 6/21/2017

- CIP-005-5, R1
  - Self-Report: 19 (57.6%)
  - Audit: 14 (42.4%)

- CIP-005-5, R2
  - Self-Report: 16 (64%)
  - Audit: 9 (36%)
NERC conducted a Remote Access Study to study the effectiveness of CIP Reliability Standards and implementation. The study found that the standards and the way registered entities have implemented them are largely effective in mitigating many of the risks associated with remote access. NERC identified areas that should be considered to further enhance the security posture of industry. NERC will use its various reliability tools, including training and outreach, the issuance of security guidelines, or modifications of the CIP Reliability Standards to address the issues identified in the report.
Questions and Answers
“To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection”
To Prevent Successful Physical Attacks
• No cut/No Climb or Expanded Metal Fencing with Top Guard
• Reinforced Perimeter Corner Posts with High Tension Aircraft Cables
• Removable Bollards and Jersey Barriers at entrances
• Creating Serpentine approaches to entrances
• Automated Reinforced Metal Entrance Gates with Single and/or Dual-factor Authentication
• LED Perimeter and Internal Lighting
• Pan/Tilt/Zoom (PTZ) Cameras with Low Light Capability for Perimeter Surveillance
• Passive Infra-Red (PIR) Sensors
• Innovative Thinking
  ▪ Sand-filled cable trays leading into Control Houses
  ▪ Employing resiliency measures to mitigate threats
  ▪ Use of screening material to minimize “nuisance alarms” with PIRs

• Security Culture
  ▪ Policies and Procedures
  ▪ Security Education and Training
  ▪ Security Awareness through use of Signs and Posters
• Maintenance Programs
  ▪ Inspection Schedule
  ▪ Scheduled Equipment Tests
• Regular Testing of Security Plans and Procedures
• High Impact Control Centers for CIP-014-2 Critical Substations
Ineffective
Questions and Answers
Modifications to CI P Standards
Project 2016-02

Sean Cavote, Manager of Standards Development
Katherine Street, NERC Senior Standards Developer
Mat Bunch, NERC Standards Developer
2017 Standards and Compliance Workshop
July 12, 2017
Project 2016-02 Background

- FERC issued Order No. 822, Revised Critical Infrastructure Protection (CIP) Reliability Standards, on January 21, 2016
- The Standards Committee accepted the Standard Authorization Request (SAR) on July 20, 2016
  - Project 2016-02 Scope:
    - FERC issues and directives identified in Order No. 822;
    - Issues identified by the CIP Version 5 Transition Advisory Group (V5 TAG); and
    - Request(s) for Interpretation (RFIs) and other issues identified in the SAR
• Low Impact External Routable Connectivity (LERC)
• Transient electronic devices used at Low Impact BES Cyber Systems
• Control Center communication networks
• Transmission Owner Control Centers (TOCC) performing the functional obligations of a Transmission Operator
• The Use of Virtualization in CIP Standards
• Cyber Asset and BES Cyber Asset
• Network and Externally Accessible Devices
• EnergySec RFI
  ▪ “Shared BES Cyber Systems” in CIP-002-5.1a
• SAR
  ▪ CIP Exceptional Circumstances (CEC)
<table>
<thead>
<tr>
<th>Issue Area</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>LERC definition</td>
<td>Order 822</td>
</tr>
<tr>
<td>Transient devices for low impact</td>
<td>Order 822</td>
</tr>
<tr>
<td>Communication between BES Control Centers</td>
<td>Order 822</td>
</tr>
<tr>
<td>Cyber Asset and BES Cyber Asset Definitions</td>
<td>V5TAG</td>
</tr>
<tr>
<td>Network and Externally Accessible Devices</td>
<td>V5TAG</td>
</tr>
<tr>
<td>Transmission Owner (TO) Control Centers (TOCC)</td>
<td>V5TAG</td>
</tr>
<tr>
<td>The Use of Virtualization in CIP Standards</td>
<td>V5TAG</td>
</tr>
<tr>
<td>CIP Exceptional Circumstances (CEC)</td>
<td>SAR</td>
</tr>
<tr>
<td>“Shared BES Cyber Systems” in CIP-002-5.1a</td>
<td>EnergySec RFI</td>
</tr>
</tbody>
</table>
Questions and Answers
<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-Chair</td>
<td>Christine Hasha</td>
<td>Electric Reliability Council of Texas</td>
</tr>
<tr>
<td>Co-Chair</td>
<td>David Revill</td>
<td>Georgia System Operations Corporation</td>
</tr>
<tr>
<td>Members</td>
<td>Steven Brain</td>
<td>Dominion Energy Services</td>
</tr>
<tr>
<td></td>
<td>Jay Cribb</td>
<td>Southern Company</td>
</tr>
<tr>
<td></td>
<td>Jennifer Flandermeyer</td>
<td>Kansas City Power and Light</td>
</tr>
<tr>
<td></td>
<td>Tom Foster</td>
<td>PJM Interconnection</td>
</tr>
<tr>
<td></td>
<td>Richard Kinas</td>
<td>Orlando Utilities Commission</td>
</tr>
<tr>
<td></td>
<td>Forrest Krigbaum</td>
<td>Bonneville Power Administration</td>
</tr>
<tr>
<td></td>
<td>Philippe Labrosse</td>
<td>Hydro-Quebec TransEnergie</td>
</tr>
<tr>
<td></td>
<td>Mark Riley</td>
<td>Associated Electric Cooperative, Inc.</td>
</tr>
</tbody>
</table>
Status Updates by Issue Area

- Control Center Communication Networks
- Transmission Owner Control Centers (TOCC) performing the functional obligations of a Transmission Operator
- CIP Exceptional Circumstances
- Virtualization
<table>
<thead>
<tr>
<th>Issue Area</th>
<th>Source</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LERC definition</td>
<td>Order 822</td>
<td>CIP-003-7 filed with FERC 3/3/2017.</td>
</tr>
<tr>
<td>Communication between BES Control Centers</td>
<td>Order 822</td>
<td>Informal Posting concluded 3/13/2017; development in progress.</td>
</tr>
<tr>
<td>Cyber Asset and BES Cyber Asset Definitions</td>
<td>V5TAG</td>
<td>Development in progress.</td>
</tr>
<tr>
<td>Network and Externally Accessible Devices</td>
<td>V5TAG</td>
<td>Development in progress.</td>
</tr>
<tr>
<td>Transmission Owner (TO) Control Centers (TOCC)</td>
<td>V5TAG</td>
<td>Informal Posting concluded 4/11/2017; development in progress.</td>
</tr>
<tr>
<td>The Use of Virtualization in CIP Standards</td>
<td>V5TAG</td>
<td>Informal Posting concluded 4/11/2017; development in progress.</td>
</tr>
<tr>
<td>CIP Exceptional Circumstances (CEC)</td>
<td>SAR</td>
<td>Informal Posting concluded 3/13/2017; development in progress.</td>
</tr>
</tbody>
</table>
• SDT conference calls will be scheduled as needed to allow the team to process input and develop proposals
• Updated call information available on the NERC Standards calendar of events
• Standards Development Contacts
  
  Katherine Street, NERC Staff
  
  katherine.street@nerc.net
  (404) 446-9752

  Mat Bunch, NERC Staff
  
  mat.bunch@nerc.net
  (404) 446-9785
Questions and Answers
• Updates to the Guide for Internal Controls
  ▪ Key principles supporting ERO Enterprise review of internal controls
  ▪ Clarification on review processes and documentation
Break

Webinar participants: We will return at 10:15 a.m. Central
Compliance at GE

Prepared for: NERC 2017 Standards & Compliance Workshop
Keith Carr, GE Power General Counsel
Joseph Suich, GE Power Chief Compliance Officer

Imagination at work.
GE & GE Power
Leading the digital transformation of all industries, including power
GE POWER

~$26.8B revenue ~55,000 employees >150 countries

GAS POWER SYSTEMS
POWER SERVICES
STEAM POWER SYSTEMS
WATER & PROCESS TECHNOLOGIES
GE HITACHI NUCLEAR ENERGY
POWER DIGITAL SOLUTIONS

Baden, Switzerland
Baden, Switzerland
Baden, Switzerland
Trevose, PA, USA
Wilmington, NC, USA
San Ramon, CA, USA

FUNCTIONAL EXPERTISE
OPERATIONAL EXCELLENCE
DIGITAL CAPABILITY

GE Compliance Team Structure
**Organization**

**Infrastructure**

- ~300 business compliance leaders
- Corporate investigations team… Includes former prosecutors … closely involved in integrity programs
- Corporate HQ compliance team… dedicated executives
- Policy owners / coordinators for every S&L policy
- Region / Country Corporate GGO (Global Growth Operations) leaders, 12 compliance leaders + country resources
- ~600 ombuds contacts globally
- CAS… compliance-related areas across businesses

**Business Teams**

- **Policy owners**
  - Policies & procedures
  - Domain expertise
  - Lead initiatives across GE

- **Region / Country Leaders**
  - Identify pole / country trends
  - EWS on country specific regs
  - Lead & relate with regulators

- **Corporate Ombuds**
  - Company wide ombuds system
  - Collect & review trends
  - Global tool

- **Compliance Leads**
- **Ombuds**
- **Risk Area Focals**
GE’s Code of Conduct/S&L
What is *The Spirit & The Letter*?

*The Spirit & The Letter* is our guide to doing the right thing and establishes the policies and standards that all GE employees must commit to follow.

How do I know if it is the right thing to do?

- How would this decision look to others within our company and externally?
- Am I willing to be held accountable for this decision?
- Is this consistent with *The Spirit & The Letter*?
Two Essential Parts

The Spirit (Ethics)

Helps us to do the right thing

GE code of conduct

01 Be honest, fair and trustworthy.

02 Obey applicable laws and regulations.

03 Be the Voice of Integrity and promptly report any concerns you have about compliance with law, GE policy or this Code.

04 Simple compliance is more effective compliance. Effective compliance is a competitive advantage. Work to run the company in as competitive a way as possible – with speed, accountability and compliance.

The Letter (Compliance)

Our guide to doing it right

GE integrity policies

IMPROPER PAYMENTS
Don’t bribe; don’t permit bribes; watch third parties.

INTELLECTUAL PROPERTY
Identify and protect GE innovations; don’t take or use IP without authorization.

INTERNATIONAL TRADE COMPLIANCE
Never let GE goods, technology or services go to prohibited persons or places; know the risks and follow the rules for cross-border transfers.

WORKING WITH GOVERNMENTS
Never take shortcuts when dealing with government; never deviate from the contract.

COMPETITION LAW
Never agree with competitors to fix prices, rig bids, or allocate customers, projects or territories.

FAIR EMPLOYMENT PRACTICES
Treat all employees fairly; respect the right to associate; base decisions on merit; don’t harass or discriminate.

CONTROLLERSHIP
Documents, communications and accounting must be 100% accurate and honest.

CYBER SECURITY & PRIVACY
Respect privacy rights and protect against cyber risks to GE information, networks and products.

ENVIRONMENT, HEALTH AND SAFETY (EHS)
Follow EHS procedures and be alert to EHS hazards in your workplace.
Creating a “Speak Up” Compliance Culture
Investors’ Valuation of Compliance

-20% +10% +10% +10% +28%
-30% +10% +10% +10% +40%
-35% -30% -30% -40% -50%

United States Canada United Kingdom Cont. Europe Asia-Pacific

= Median Valuation Premium from “superb” corporate governance
= Median Valuation Discount from “poor” corporate governance

In a number of studies, we've found that when employees can voice their concerns freely, organizations see increased retention and stronger performance.

Compliance ROI
Three Programs Compared

Values-Based Programs Produce Greatest Program Benefits

Source: Adapted from the LRN 2016 HOW Report
A culture of integrity...easy to propose

A few examples...

“We must always act with integrity, even when the right thing is hard to do.”

“Nothing is more important to [our company] than making sure we do what is right – and nothing puts us at risk more than failure to do so.”

“We stand for respectable, honest, and actions in everyday business that are in accordance with rules, and we commit ourselves to the following Code of Conduct.”
2016 - the biggest enforcement year in FCPA history
GE’s Compliance Program

- Inaugural Corporate Award 2010
- 11 years in a row (2017)
- Recognized by US DOJ for strength of program
- Benchmarked around the globe as best in class

Founding Member 1986

Top 10
This was not always the case...

GE in the 1980's...
Leaders are the primary influence on culture

- Employees look first to their leader for cues on how to behave
- It's not what a leader says, but what a leader does that really matters
GE Leaders Create a Culture of Compliance

Clear & Simple Mandates Leaders Must Follow

- **Ensure employees understand** that business results are never more important than ethical conduct and compliance with GE policies
- **Create an open environment** in which every employee feels comfortable raising concerns
- **Personally set the example for integrity**, not just through words, but more importantly, through actions
- **Know the policies** that apply to you and your team and regularly talk about compliance
- **Document and escalate** any employee’s expressed concern
- **Take prompt corrective action** to address identified compliance weakness
Center Your Leaders---Compliance Leadership Training

GE Power Compliance Leadership Training

Creating a culture of integrity

Handling integrity concerns

What happens if an employee comes to you:
- Concern is raised and logged into spirit.ge.com
- Impartial and objective investigation
- Implement corrective actions
- Feedback provided

What leaders must do:

**Engage**
- STOP, listen; be patient
  - Ensure privacy – close your door
  - Place importance on all enquiries...be serious (avoid jokes or humor)
  - Acknowledge how difficult it is to raise the concern and make them comfortable

**Evaluate**
- Gather facts from the employee
  - Assess the facts immediately after the discussion
  - Determine if there is a policy or integrity concern
  - Determine to whom to escalate
  - Assess whether a conflict of interest exists
  - Seek HR or Legal advice

**Escalate**
- Determine to whom to escalate
  - Escalate policy concerns as directed by your business through the SPIRIT workflow tool or to your manager, Compliance, Legal, HR or Ombuds
  - Maintain confidentiality is essential. Do not share any information regarding the matter except with those who have a need and right to know

**Ensure**
- Employees who raise complaints are protected
  - Be sensitive to employee’s apprehensions and perceptions of retaliation
  - Calm fears about retaliation; emphasize GE’s zero tolerance policy
  - Contact Legal before taking any employment actions

Prevent
- Prevent ethics, compliance and regulatory problems

Detect
- Detect problems that do occur at the earliest possible stage

Respond
- Respond quickly and thoroughly

Visit spirit.ge.com for more information
Sample Handouts for Leaders

**Compliance questions for managers**

_Suggested questions for managers to discuss with employees:_

1. What are your biggest compliance risks?
2. What do you do when there is an issue?
3. Do the people you work with follow the rules?
4. How can compliance help you do your job?
5. Do you know who to contact with questions?
Duty of Compliance Team to Leaders: Keep it Relevant, Keep it Simple

Code of Conduct
- 40%+ Shorter
  - Simplified
  - Hearts & Minds

Refreshed Training
- From 7 hrs ↓ 2 hrs
  - Video-based format
  - Global rollout

Acknowledgements
- 80% Shorter
  - 970 down to 120 words
  - Leader intro video

Simple compliance is more effective compliance
GE’s Compliance Executive Dashboard—Leader Snapshot of Their Program

Open reporting, COI, Schedule II, Training launched, Monitoring...

- Automated system for metrics analysis
- Data pulled from the source systems

One-stop

+ 1 click drill-down capability, filtering
+ Dramatic ↓ in time for data analysis

Analysis

+ Send training reminders directly from the tool
+ Follow-up on open conflicts of interest

Action

+ Full iPad compatibility
+ Summary dashboards & export capabilities

Reporting

Central Data Warehouse

Open Reporting

eCOI

CAS

Learnin

KYC

Approvals
Center Your Employees--Spotlight on Integrity Day

Singular day to come together to underscore the importance of integrity and compliance

**Approach**

*Utilize cross-functional committee ...*

- CEO-led broadcast with key business leaders
- Manager-led conversations
- S&L acknowledgment & COI rollout

**Real compliance video**

- GE experience proves value of candid acknowledgment of compliance misses

- Key messages:
  - Compliance is a journey
  - Rules are not enough, culture is paramount
  - Crisis presents a unique opportunity to renew commitment to ethics and integrity
  - Leadership expectations

Employee engagement key to success
“Open Reporting”: Your Compliance Culture Indicator
GE Compliance Rhythm

Clear Policies & Expectations

Simple Compliance is Better Compliance

All Employees Own Compliance
Leaders Drive the Program

Leveraging Metrics & Data Analytics

Focus on JVs/Remote Sites

Keeping Training Fresh

Visible & Active

Opened Reporting and our Ombuds Network

- An integral part of GE’s overall compliance strategy
- Each Ombuds serves as a resource for individuals to ask questions or report integrity concerns without fear of retaliation
- Worldwide network of 600 ombudsmen, coverage is provided for every business and country in which GE operates
- 3,000+ integrity concerns reported through the Open Reporting & Ombuds process annually

The Roles and Responsibilities of an Ombudsperson

- Receive reports of integrity concerns
- Seek help on integrity questions
- Refer non-policy concerns to appropriate resources
- Ensure confidentiality to the extent possible
- Facilitate on-boarding, training & impactful investigations
- Ensure closure & feedback

Aligned to Business Risks

“Boots on the Ground”

Real Life Videos: Sharing Lessons

Best Culture Indicator

Facilitating Speak Up Culture.
Open Reporting, Risk Roll Up
ECI Survey

A 2016 global survey of employees from public, private and non-profit sectors:

- **Observed Misconduct**: 33%
- **Reported Misconduct**: 59%
- **Experienced Retaliation**: 36%

Open reporting: Best indicator of health of culture, positive or otherwise

---

1 Results of the Ethics & Compliance Initiative 2016 Global Business Ethics Survey – 13,000 employee responses across 13 countries
“Open Reporting” at GE

- GE’s reputation is one of our most valuable assets. We believe every employee is responsible for integrity and we work hard to create an open reporting environment where employees are empowered and expected to raise integrity concerns.
- An employee’s willingness to voice any concerns about potential policy violations is critical to being able to foster a culture of integrity. If employees are not comfortable doing so, without fear of retaliation, significant integrity concerns can go undetected.
- Concerns will be investigated objectively by a person or team of people with the right expertise.
- Appropriate remedial action will be taken when warranted, and feedback will be provided to the concern raiser (unless anonymous).

Why this matters

*Open and early reporting is more important now than ever because …*
- Global regulators demand it
- Find small problems and fix them early
- Whistleblowing statutes

Key information

Allegations or concerns about potential or existing violation of law, regulation or GE policy must be reported by contacting your manager, HR, compliance, legal, audit or Ombuds.

GE offers several channels for raising concerns:
- Managers
- Human Resources leaders
- Compliance leaders
- Auditors
- Company legal counsel
- Next level of management
- Business or region GE ombudsperson or integrity helpline
- GE Corporate ombudsperson
- The GE Board of Directors
GE’s Ombuds Program

The GE Ombuds Program is an integral part of GE’s overall Open Reporting strategy.

- GE’s extensive ombudsperson process serves as a mechanism for individuals to ask questions and report integrity concerns without fear of retaliation.

- With a global network of approximately 600 ombudspersons, coverage is provided for every business and country in which GE operates.

- GE ombudspersons speak the local language and understand the culture and business environment. The GE Ombuds Program is introduced at GE all-employee meetings at the business and regional-level, including GE integrity events and GE trainings.

- The GE ombudsperson network is assessed and measured by GE to ensure that it is operating with peak efficiency while providing the most comprehensive global coverage.
## Key Attributes of an Ombudsperson

<table>
<thead>
<tr>
<th>Guidance</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experienced employees with strong performance</td>
<td>2-5 years</td>
</tr>
<tr>
<td>Trustworthy and approachable by all employees</td>
<td>Middle Management</td>
</tr>
<tr>
<td>In a position that can afford to take on additional work, with manager support</td>
<td>Jobs with minimal travel</td>
</tr>
<tr>
<td>Process-oriented, organized, strong communications skills, ability to be objective, clear thinker</td>
<td>Operations, Supply Chain, Sourcing</td>
</tr>
<tr>
<td>Roles that are not in conflict with financial concerns</td>
<td>Controllers</td>
</tr>
<tr>
<td>Roles that do not represent an Open Reporting Channel</td>
<td>HR, Legal, Audit, Compliance</td>
</tr>
<tr>
<td>Employees who value leading Integrity for the business</td>
<td>Willing to be in role for at least 2 years</td>
</tr>
</tbody>
</table>
Ombuds | Roles & Responsibilities

**Respond to Contacts**

- **Receive reports** of integrity concerns
- **Seek help** on integrity questions
- **Refer** non-policy concerns to appropriate resources
- Ensure **confidentiality** – We cannot guarantee complete anonymity
- **Facilitate** an objective, thorough, & impartial investigation
- Ensure **closure** and **feedback** to reporting person if possible

**Build Relationships**

- **Promote** business compliance process improvement
- Build **trust**
- **Interface** with business, region, & corporate ombudspersons

**Promote** reporting process without fear of retribution

**Stay current** on process changes
Sample Open Reporting Metrics

**Open reporting count**

**Reporting channels 2016**
- Policy: Integrity, Non-Policy
- Non-Policy: Ombuds
- Compliance professional: 26%
- HR: 9%
- Leadership: 9%

**Anonymous rate**
- Policy concerns only
- 2014: 88%
- 2015: 53%
- Q1 2016: 39%

**Top Policy Concerns 2016**
- Controllership: 3; COI: 1; IPP: 1; FEP: 1

**Open reporting region 2016**
- Japan
- ASEA
- ANZ
- KR
- ID
- VN
- MY
- SG
- PH

**Reporting by P&L & Days to Close**
- Per 1000 employees

**Reporting by P&L & Days to Close**
- PS
- GP
- SPS
- SPS
- Water
- Others
Compliance Mobile App—Raising a Concern “On The Go”

Home Page
- Built on voice of customer
- Raise a concern
- Risk area highlights
- Business Courtesies
- Competition Law
- Immigration

Raise a Concern
- DIY answers to questions on business courtesies
- Easy access to contacts for answers
- Videos to enhance learning
- Compliance leaders
- Business Ombuds
- Anonymous
- Corporate

Business Courtesies
- Organization charts
- Quizzes & games
- Manager risk roll-up acknowledgement
- Spirit and Letter policies

Competitive Info. & Trade Associations
- Self reporting of competitor contacts, trade associations
- Quick hits … 5 things to know
- Decision tree on using competitor information

Developed Based on Internal Customer VOC
Driving the Culture at the Middle: Risk Roll Up (RRU)
Risk Roll Up

✓ The RRU is a **bottom-up risk assessment**

✓ **Not a spectator sport**—requires manager & employee engagement

✓ **Strong ROI**: 1-2 hours/year to help identify “unknown unknowns”

✓ Managers drive the RRU

✓ Managers trained (1 hr)

✓ Managers tailors content to each team

✓ All materials, translations, etc…are **prepared for the managers**

✓ Only works if your leadership makes it a priority
RRU: Program Mechanics

- Managers pick only 3/16 S&L topics that relate to their ops
- Each topic has 1 video, 1 real life Power miss & a one pager on topic basics
- Managers can certify completion via mobile app
- Any Q not answered by manager will be answered by subject matter expert
Leader Communications Drive the Commitment

GE POWER MANAGERS: THE RISK ROLL-UP IS COMING!!! August 29 – October 14, 2016

WHAT IS RISK ROLL-UP?
Risk Roll-Up is GE Power’s compliance risk assessment process which showcases you, a GE Power manager, as the face of compliance to your employees by requiring that managers engage with their PB+ direct reports* to review relevant business policies and capture questions or concerns that the manager is unable to answer and reinforce GE’s open reporting culture and zero retaliation policy. Learn more about the process from Joseph Suich, GE Power Chief Compliance Officer, in the video (2:20) below:

News You Need

Risk Roll-Up Starts Monday
As the eyes and ears of the organization, your participation is key to the success of this valuable risk assessment process
Clear & Simple Process, All at One Website
GE Power 2016 RRU Metrics

Target Population: 37,000

Manager Population: 6076

Target Completion: 99%

Employee input also results in:
✓ Removal of unnecessary process
✓ Identification of gaps
✓ Cash out reductions
✓ Better product and worker safety
✓ Reinforcement of a “speak up” culture

RRU Metrics, Results and Follow-Up
Actions are Then Relayed to Employees

Keith Carr
General Counsel, GE Power

Joseph Suich
Chief Compliance Officer, GE Power
Risk Roll Up: Results

- The RRU drives tone @ the top and the middle
- The RRU make managers the face of compliance to employees
- The RRU drives the “unknown unknowns” issues to the top
- The RRU requires managers to learn compliance to teach it
- The RRU results provides top management a company risk assessment
Applying the RRU Results

Sample Heat Map

3 Top Risks

1. ADD COMPLIANCE ISSUE
2. ADD COMPLIANCE ISSUE
3. ADD COMPLIANCE ISSUE

Type & Strength of Defense

Eng. Admin Oversight Cultural

NOTE KEY ACTION ITEMS HERE, WITH OWNER & TIMELINE TO COMPLETE
Take Aways & The Access GE Compliance Program
Take Aways

✓ Culture, more than any rulebook, is the key

✓ Leaders are the primary influencer of culture

✓ Set expectations: make it simple/relevant

✓ Keep a compliance rhythm, and drive it at the middle
Access GE: Customer Compliance Visits

Leveraging GE’s global world-class compliance team for GE-to-customer benchmarking and best practice sharing sessions*

✓ strong compliance program helps to avoid fines and business interruptions
✓ there is increasing enforcement of multinational companies: US (FCPA), UK (SFO UKBA), China, Russia..
✓ focuses on looking around corners to spot issues before they happen

➢ We come to you

➢ You pick the agenda

➢ You get more with GE

Promotes a true business partnership, focused on your business model & go-to-market strategy

GE Contact to Arrange a Benchmarking Session
Joseph Suich, GE Power CCO
Joseph.suich@ge.com

*Access GE is at no cost to our customers.
Agenda

- Quick survey
- NERC CCC observations on internal controls
- Tips if you haven’t started your program
- MISO’s experience (if time allows)
Quick Survey

A. Who has undergone a pre-audit Internal Control Evaluation (ICE) from your Region?

B. Who is planning to participate in an ICE in the near future?

C. Who hasn’t pursued an ICE because you haven’t seen the value for the effort involved?

D. Who hasn’t pursued an ICE because you are struggling a little on what’s needed and how to get started?

E. Don’t know or not applicable
NERC CCC Observations

- There is not a “one size fits all” approach for implementing internal controls.
- All entities have many internal controls, they just might not have documented them.
- While ICE has been discussed as primarily a pre-audit engagement, this is not the sole nor primary Compliance Monitoring and Enforcement Program (CMEP) touchpoint related to internal controls.
- To meet its obligation to ensure an adequate level of reliability, the ERO needs to understand how Entities address their reliability and security risks.
NERC CCC Observations (continued)

- You cannot be found non-compliant for your controls or controls approach (unless the Requirement is a control*)
- While not required, it is in the Registered Entities’ best-interest to present their controls as opportunities arise
- Priority on controls should be on reliability and security risk, not audit evidence collection
- Requirements cannot be made foolproof via preventative controls
  - Multiple layers needed for higher risk issues
  - Can never get to zero risk

* lack of effective controls could lead to an event that results in non-compliance
Controls Evaluation Touchpoints

- Compliance program controls evaluation (to obtain self-logging authority)
- Intra-audit (periodic evaluation as part of oversight plan)
  - Guided self certifications
  - CMEP focus areas
  - Assistance visits
- Pre-audit ICE (to refine audit scope)
- During audits (to gain assurance)
- Enforcement
- Mitigation
Value Proposition

• Fewer and less severe reliability and security issues
• Focuses on reliability and security as opposed to stacking multiple layers of evidence
• Quicker path to gain assurance
• Potential support for Self-Logging authority (potential game-changer for efficiency and reliability and security)
• Possibly refine the scope of on-site audits
• Can demonstrate that the risk associated with a violation was reduced, which should lead to favorable consideration in enforcement
• Builds knowledge base and trust both within your organization and with your regulators
• Long term could result in an ongoing oversight approach that eliminates the need for major audit engagements
An Operator’s Perspective on Internal Controls
One Operator’s Definition

Internal Control:

A tool, training, procedure, or other aid intended to prevent or reduce the likelihood and/or impact of something evil happening on the grid

*While not a primary objective, an internal control can also be used to collect necessary compliance evidence.
Name That Control

- Example controls
  - Training and drills
  - Procedure, checklist, form or other job aid
  - Performance review (e.g. reviewing tapes of operator instructions and providing feedback)
  - Security constrained dispatch
  - Mantrap or intrusion alarm to control access
  - EMS alarm with instructional note on actions to take
  - Computer script to save daily operating plans
  - Tailgate session prior to a unique operating evolution
  - Corrective actions from a post-event or near-miss review
  - Periodic reminder to perform a task
  - Backup tool to continue operations should the primary tool fail

- Preventive, detective, corrective?
- Automatic, manual?
- Reliability/security, compliance/evidence?
Starting a Simple Program

- Select a risk approach
  - Risk assessment is an art not a science
  - Likely 50-80% of your risk lies in 10-20% of the NERC Requirements
  - Next slide suggests a way to categorize the risk of a Requirement
- Start with highest risk Requirements and work your way down over time
  - Look at the purpose of the standard to get an idea of your control objective
  - Document current controls (pick your people’s brains, review existing procedures, plans, etc.)
  - Add controls where gaps exist (focusing on reliability/security)
  - Create a simple narrative that describes the controls for each requirement
  - Consolidate redundant and out of date controls to gain efficiencies
- Create an “elevator speech” and get buy-in
- Don’t be shy about presenting controls
Risk Inputs You Might Consider

- Your inherent risk assessment (IRA)
- Requirements where you had near misses or violations
- NERC and your Region(s) CMEP “Areas of Focus” Requirements
- **NERC compliance statistics**
  - Most violated standards
  - Serious risk standards
  - Standards with reliability or security impact when violated
- High Violation Risk Factors (see **VRF matrix**) *
- If the standard is new (no similar prior version) and it has not been through an audit cycle
- No documented/tested controls in place

*Using the VRF matrix, you have a ready-made tool to add the risks you choose to include.
Compliance Program Self-Evaluation

- Up to date owner status for each Requirement?
- Know your top 10-20% highest risk requirements and are you reviewing their compliance and controls at least annually?
- Have corporate or department goals for compliance and do the goals incent rather than discourage self-reporting?
- Corrective action:
  - Do you have visibility on the number of near-misses?
  - Does Compliance sit in on event and near miss reviews?
  - Are near miss causes being mitigated?
- Controls focused more on reliability & security rather than evidence collection?
Appendix

MISO’s Experience

Useful Resources

Acronyms
MISO Overview

- **Generation Capacity**
  - 174,724 MW (market)
  - 191,062 MW (reliability)
- **52 Members**
- **437 Market Participants**
- **291,538 SCADA measurements**
- **Registered as RC, BA, PC, TSP**
- **4 Control Centers**
  - 3 primary (that can hand off to each other)
  - 1 backup
- **Distributed Compliance Process based on 3 lines of defense**
  - First line, divisional managers, compliance liaisons and requirement owners
  - Second line, supporting central compliance group
  - Third line, internal audit
MISO’s Internal Controls Journey

- Compliance responsibilities reside in line divisions
- In 2010, MISO’s board approved an incentive goal to create controls for all regulatory obligations
- At least two controls (some used multiple times) were created for over 3500 NERC and tariff requirements
- Limited success in sustaining these
- Some divisions actively maintaining and testing controls
- Migrating to software that will capture/manage
  - Obligations (requirements)
  - Control objectives
  - Controls
  - Testing
- In discussions with our lead Region on conducting an ICE
Useful Resources

- ERO Enterprise Internal Control Evaluation Guide
- ERO Enterprise Self-Logging Program
- NERC Enforcement and Mitigation website
- MRO Governance Risk Program
- MRO Highly Effective Reliable Organizations (HERO) website and associated quiz
Acronyms

- ERO: Electric Reliability Organization
- ICE: Internal Control Evaluation
- CCC: Compliance and Certification Committee
- CMEP: Compliance Monitoring and Enforcement Program
- EMS: Energy Management System
- IRA: Inherent Risk Assessment
Questions and Answers
Wednesday July 12, 2017

Internal Controls
Operationalizing Compliance
NSPI Overview

- Approximately 500,000 customer covering the Province of Nova Scotia
- Approximately 1700 employees
- 4 Territories (Eastern, Cape Breton, Western, Central)
- Generation – 2300 MW Capacity
  - 56% Thermal
  - 14% Wind
  - 14% Natural Gas/Light Fuel Oil
  - 10% Hydro/Tidal
  - 3% Heavy Fuel Oil
  - 3% Imports
- Transmission Lines – 5,133 Km (3,189 Miles)
  - 69 kV, 138 kV, 230 kV, 345 kV)
- Distribution Lines 26,414 Km (16,412 Miles)
  - 12.5kV, 25kV (some 4kV)
- NB Power provides Reliability Coordination Function for NS
- Energy Control Centre provides integrated planning, dispatch and control of generation, transmission, and distribution
NSPI Regulatory Framework

NERC - North American Electricity Reliability Corporation

NPCC - Northeast Power Coordinating Council

UARB - Nova Scotia Utility and Review Board

NSPI Registered Functions: BA, DP, GO, GOP, PA, RP, RSG, TO, TOP, TP and TSP
NSPI working with NPCC

NSPI participation in a number of NPCC Task Forces and working groups

✓ NSPI presently have 18 NPCC representatives.
✓ Working together to maintain compliance

Compliance Committee
Task Force on Coordination of Operation (TFCO)
Task Force on System Protection (TFSP)
Task Force on Coordination of Planning (TFCP)
Task Force on System Studies (TFSS)
Task Force on Infrastructure Security & Technology (TFIST)
CO-11 Restoration Working Group
CO-2 System Operator Training
CO-12 Operations Planning
CO-7 Operational Review Team
SP-7 Protection System Mis-Operations Review
CO-1 Control Performance
SS-37 Base Case Development
HOW DID NSPI LEARN ABOUT INTERNAL CONTROLS?

NPCC hosted a Compliance and Standard Workshop in the fall of 2015. This was the first NPCC Workshop I’ve attended. During this workshop Ben Eng, NPCC Manager delivered a presentation describing all of the benefits entities could gain from going through a voluntary ICE (Internal Controls Evaluation) process. While attending this workshop I was able to meet other professionals and discuss with them their experiences with ICE.

Some NSPI Benefits:

- Excelling standards and requirements
- Alignment of staff performance to Key Performance Indicators
- Targeted BES reliability risk-focused scoping
- Reduction in audit scope and duration
- Enhanced entity communication and interaction across organizational business functions
- Improving risk and control awareness
- Gained relationships with NPCC staff and other business professionals
The scope of the internal controls assessment was actually determined by NSPI. NSPI was able to pick and choose to offer the Internal Controls design for one, few, many or all of the standards in the proposed scope of our upcoming audit, for assessment. Regardless of volunteering for the NPCC controls assessment, NSPI had existing internal controls to mitigate risks (e.g. Operations/Operational Continuity, Legal and Compliance, Theft/Loss/Fraud, Market Rules).

What were some of the things that we considered making the decision:

- How much extra work will this add?
- Is there is a cost?
- List our pro’s and Con’s
- What do WE gain as a utility by participating?
- How much time do we have to prepare, and complete?

It was a team decision at Nova Scotia Power between Management, Compliance, and Subject Matter Experts. Once we determined we will take advantage, within a couple of weeks NPCC sent us all information and materials to move forward to complete ICE.
NSPI "operationalize compliance" by integrating it into our business processes, so it becomes part of how our employees (Subject Matter Experts) do their job duties.

NSPI Document Review Committee – Documents which are reviewed and approved, have managed distribution, and which cannot be revised except through the Document Change Request Procedure. This would include, annually evaluating our NSPI Compliance Program.

Enhanced Internal Quality Assurance Audits. NSPI Compliance Team has based this on our Internal Controls Evaluation. Focusing on our recommendations, and learnings ICE had provided to us through their review.

Compliance Awareness – We provide Subject Matter Experts with regular NERC/Compliance updates. NSPI Follows up on compliance, and being approachable is key.

We Continue to grow our Compliance Culture by making sure it’s as important as safety here at Nova Scotia Power.
New controls as a result of controls assessment

NSPI has developed newly updated documentation for EO hours to ensure information is easy to find, and reads clear.

Compliance and Training Coordinator meets regularly to review all new or revised NERC standards to determine where and if training is required.

Incorporate NSPI planning methodology documents within the document review process.

Using software i.e. Maximo to schedule and track PMs or relay maintenance, with relays individually identified.
Internal Controls

Control Identification, Control Design Assessment, Effectiveness Training, Results
COM-002-4 Operating Personnel Communication Protocol
System Operators two-party or person to person shall use 3 part communication - Using RAT-STAT processes not just to be compliant but to communicate performance to System Operators during their quarterly reviews.

EOP-005-2 System Restoration from Blackstart Resources
Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator’s restoration plan that are outside of their normal tasks.
During our review we identified that we needed to change our approach to compliance with this requirement.
EOP-008-1 Loss of Control Centre Functionality

Requirement 1.5 states A transition period between the loss of primary control center functionality and the time to fully implement the backup functionality that is less than or equal to two hours.

*Completed in less than hour and half by revising timeline with key stakeholders, and transmission operator lead identified.*
Experiences & Conversations about controls

- Entities should identify their internal controls and any gaps
- Entities should see a bigger picture within Compliance
- Corroborate with others, and realize within the company there are more controls than expected. Every department has controls to being compliant.
- Find an opportunity for subject matter experts to come together within your organization
- Provide and allow opportunities for entities to build on their Compliance culture
- Have your SMEs use the 5 W’s + 1 H rule to describe the Process Function/Workflow and underlying internal controls. The attributes of Who, What, When, Where, Why & How are used to assess the design which is very helpful, and easy to follow and understand
- Flowcharts provided us the understanding in a different manner on how different areas of the business had certain areas to manage controls. Great tool.
Lessons Learned

✓ Determines if your entity has implemented an internal control program containing sufficient controls that provide reasonable assurance of compliance. Understanding the difference between internal controls documentation, and audit evidence.

✓ Flow charts are very useful in providing a visual depiction of the controls for compliance and other areas of the business.

✓ Plan weekly meetings for everyone to get into a room and review each others work, make suggestions, and double check work. These meetings make business units more aware of the roles they play in BES reliability. They acknowledge undocumented inputs, handoffs, verifications, tools, work tasks/management which are all internal controls. Team Effort.

✓ NPCC’s Internal Control Evaluation was an opportunity to have an independent 3rd party assess the design, implementation, and effectiveness of NSPI’s internal controls/internal control designs for a subset of selected standards (IRA) applicable to its registered functions.

✓ NSPI found that the NPCC ICE was more of a collaborative effort to promote open communication between NSPI’s Subject Matter Experts and Compliance team to tease out and document NSPI’s internal controls for evaluation.

✓ The entity does not need to volunteer for ICE to take an introspective look at their internal controls. It is good business practice to be aware of and document your internal controls. Going forward, ERO auditors are expected to review controls during a compliance engagement. Having internal controls information ready (as a result of ICE or not) will make the audit more efficient.
Closing

QUESTIONS
ARE YOU UP FOR THE CHALLENGE?
Who is VELCO?

- Established in 1956 as a Transmission only company
- Transmission provided for the State of Vermont
  - 738 miles of transmission lines
  - 115 kV to 450 kV
  - 14,000 acres of rights-of-way
  - 55 substations, switching stations and terminal facilities
    - 2 = High Control Centers
    - 7 = Medium facilities
    - Low = remaining
  - Interconnected with Hydro-Québec
  - 1500 miles fiber optic communication networks
- Member of ISO-NE
- NERC Registration: Vermont Transco LLC
  - Member of NPCC
  - TO, TOP, TP & TSP
- Approximately 150 employees
What is our industry’s purpose?

Compliance?

or

- To enrich lives by providing:
  - Peace of mind while keeping people safer, more connected, educated, healthier, etc.
  - A higher quality of life - happier/better/bring families together
  - Empower people – create new jobs – provide opportunities / resources / education – to live their dreams

- As a Country:
  - Leave a minimal footprint
  - Protect endangered species / resources
  - Aesthetically conscious
  - Make the world a better place for future generations to come.

- As a company:
  - provide quality services at least cost
How do we accomplish this?

Provide a safe, reliable, secure, forward looking electric grid

What are we facing?

- Exponential growth in new technologies, data, severe weather incidents, threats, etc.
- Increased difficulty in maintaining, operating, and securing the grid

What is the future?

- Industry role/need is changing
- Agility
- Empower our resources
- Be innovative/creative/out of the box
Moving forward we need to…

1. Focus on what’s most important
2. Align resources - empower those responsible
3. Develop & implement strong internal controls
4. Transform our cultures around compliance
5. Be willing to experiment
6. Create the future we want
When it comes to organization, it often seems like there’s really only one way...
Actual way things get done at any given company...
Moving forward – focus on functional team approach
Example experiments …

- Corporate Compliance Key Performance Indicators
  - Refocus corporate compliance with values, goals, and metrics
  - Resources focused on what’s important – reliability and security
  - Success = zero tolerance = mitigations/controls/lessons learned

- Internal Controls development
- Oversight Team (Compliance Leads)
- Incident reviews
- Think tank and visioning sessions
- Empower, challenge, excite employees
- Questioning: Why? What if?
- How to make compliance align with operations
- Align resources and innovation – add value, feel valued, and live our values
Compliances oversight evolution…
Compliances oversight evolution…

...to be continued
Compliance Focus

Compliance Oversight
(day-to-day)

- NERC / FERC
- Non-NERC
- Day to day support
- Audit/assessments
- Educate/monitor/understand
- Advise
- Network w/peers
- Regulator relationships
- Coordinate with all depts
- New standards

Internal Controls
(continuous improvement – integrate governance and automate procedures)

- Program assessment (review existing & emerging / future looking)
- Design & development
- Effectiveness testing of automation
- Document
- Tool development
- Maximize use of technology assets

Culture & Risk
(forward looking assessments)

- Corporate risk tracking
- Identify risks & mitigations
- Culture initiatives
- Training
- Communications
- Promote accountability & responsibility
- Resiliency / human performance
- Less traditional approach to sustaining compliance

Event Analysis
(reactionary)

- Incident Reviews
  - Standardized approach
- Independent view
  - Compliance determinations
    - GRIDEX
  - Emergencies
  - CIP Exceptional Circumstances
To move the needle we need...

1. Aligned resources

2. Strong internal controls to:
   - Understand roles/responsibilities
   - Hand-offs
   - Deadlines
   - Verify compliance
   - Reduce risks, cost, & work load

3. Strong culture of compliance
Functional Internal Assessments

System Operations

Transmission Owner / Transmission Operator Overview

Control Center

System Operator Functions

- Manage the VT electric grid
  - Real-Time Assessments
  - Operational Planning Analysis
  - Mitigate SCL Exceedances
  - Dispatch Generation
  - Outage Coordination

- Manage System Disturbances or Outages
- Operate/monitor Energy Management System (EMS)
- Communicate Facility Information
- Actions to Mitigate Capacity Deficiencies
- Implement Load Shedding

- Platform System Restoration
- MCC Evacuation
- NERC Certification / Training
- Emergency Events
- Communication

- Follow ISO-NE/VELCO procedures, guides, instructions
- Physical Security
- Weather Monitoring/response

Internal Controls

- VELCO Heads
- NERC Certification
- Emergency Preparation
- Emer. Resp. Plan
- Incidents - Corporate Events - Operations
- Capital Projects
- Design Standards Group
- Reliability Operating Committee
- Procedure Approval/development

Applicable Standards

- VELCO Operating Manuals
- VELCO Policies
- NERC Standards
- ISO-NE Standards
- Other Relevant Standards
Process Maps

Standard/requirement process map

Functional process map

Legend
Benefits…

• Compliance becomes part of what you do
• Encourages a strong culture
• Provides leadership opportunities
• Reduces hours / costs
• Efficiency & higher performance
• Job satisfaction
• More informed employees
• Cross functional communication / collaboration and removal of barriers
• Work smarter, more efficient, sustainable, and allow employees to do the “sexy” work
• Provides employees the freedom to be innovative and creative in how we meet, maintain, and verify compliance
• Employees will have an opportunity to have a greater impact, be innovative, share their passions, be courageous, and to help each other be great!
Questions? Ideas? Comments?

“There must be an inherent involvement of people at all levels of an organization, the idea of emergence, landscape and culture intelligence.” and

“You can intentionally design your organizational culture to increase the value of your business.”
– Claudette Rowley

Contact Information:
Kim Moulton
Vermont Electric Power Company
Chief Compliance Officer
kmoulton@velco.com
Work: (802)770-6233
Cell: (802) 747-8461

http://culturalbrilliance.com

http://www.coachingcenterofvt.com
Lunch

Webinar participants: We will return at 1:00 p.m. Central
Making the Enforcement Process Work for You

Ed Kichline, Senior Counsel and Director of Enforcement Oversight, NERC
Leigh Faugust, Counsel, NERC
Patrick O’Connor, Counsel, ReliabilityFirst
2017 Standards and Compliance Workshop
July 12, 2017
Overview

- Risk
- Cause
- Controls
Focus Questions

- How does information entities provide in Self-Reports and mitigation activities inform the enforcement process?
- How does the ERO Enterprise approach risk?
- What is a “root cause” and why is it important to identify?
- Why do internal controls matter in the enforcement context?
- What other factors can affect the disposition of noncompliance?
- What resources are available to help navigate the enforcement process?
Provide a Complete Record

What
- What happened?
- What type and how many assets are involved?

When
- When did it start and end?
- When was it discovered?

Why
- Why did the noncompliance happen?
- Did internal controls fail to prevent the noncompliance?

How
- How was it discovered?
- How will mitigation activities address the cause and prevent recurrence?
How does Enforcement mitigate risk?

- Risk Assessment
- Risk Prioritization
- Informed Decision Making
Defining Risk

Probability $\times$ Impact = Risk
• Likelihood of Occurrence
  - How likely is it that the potential harm level would have actually been realized during the noncompliance?

• Effectiveness of Controls
  - How effective were the entity’s systems (e.g., policies, procedures, etc.) at preventing, detecting, and correcting the noncompliance before manifestation of harm?

Rare/Unlikely/Moderate/Likely/Very Likely
• Potential Harm Magnitude
  ▪ What was the potential harm, specific to this registered entity, to the reliability of the Bulk Electric System posed by the noncompliance?

Inconsequential/Minor/Moderate/Major/Catastrophic
## Risk Matrix

<table>
<thead>
<tr>
<th>Probability</th>
<th>Inconsequential</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td>Minimal</td>
<td>Minimal</td>
<td>Minimal</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Minimal</td>
<td>Minimal</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Moderate</td>
<td>Minimal</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Serious</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Serious</td>
<td>Serious</td>
</tr>
<tr>
<td>Very Likely</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Serious</td>
<td>Serious</td>
<td>Serious</td>
</tr>
</tbody>
</table>
• How was the noncompliance discovered?

• What internal controls are in place?

• What is the root cause of the noncompliance?

• Describe your defense in-depth controls and protections.
• How many assets are affected?

• What is the function of each asset affected?

• Where are the affected assets?

• What business units are affected?
If you are unable to understand the cause of a problem, it is impossible to solve it.
An unauthorized individual gained access to a NERC-CIP area.
Unauthorized individual gained access to a NERC-CIP area

The door lock released

The operator walked by the door triggering the release lock

Inadequate testing
An unauthorized individual gained access to a NERC-CIP area

The individual did not know the door led to a NERC-CIP area

Inadequate signage to alert of the area
Release lock set at too high a sensitivity

- Replaced door lock sensor

Inadequate testing of access controls

- Increased testing procedure for new access controls during the first year of deployment

Inadequate signage

- Clearly marked entry points to NERC-CIP areas as requiring authorized access
**Preventive Controls**

Prevent an error or event from occurring

**Detective Controls**

Detect an error or event that may have occurred

**Corrective Controls**

Correct an error or event that may have been detected
What controls did the entity have?

- **Alarms**
  - Alarms sounded and notified security

- **Security staff**
  - Responded within seconds
  - Escorted individual out
  - Tested door controls and found them functioning
  - Created report and escalated to management

- **Visitor log**
  - Identified individual

- **Man trap**
  - Isolated unauthorized individual

- **Surveillance video**
  - Provided information on the noncompliance
What can an entity do to ensure the best outcome?

- Identify noncompliance through self-evaluation
- Immediate steps to address noncompliance
- Timely self-reporting
- Extent of condition review
- Root cause analysis
- Risk identification and mitigation
- Internal controls description
- Ongoing cooperative communication
Additional Resources

- Regional Entity representatives and case managers
- ERO Enterprise Mitigation Plan User Guide
- Posted and filed noncompliance on NERC’s Enforcement webpage
Background on CEs

• CEs built upon on the success of the FFT program.
• The use of this streamlined mechanism is informed by the facts and circumstances of the noncompliance, the risk posed by the noncompliance to the reliability of the bulk power system, and the deterrent effect of an enforcement action or penalty.
• Only minimal risk noncompliance is eligible for processing as a CE. Minimal risk noncompliance is eligible for CE treatment regardless of the discovery method.
• CEs must be mitigated within 12 months of the posting of the CE.
• There are no standards or requirements that automatically qualify or disqualify a noncompliance for CE treatment.

• Regional Entity criteria for CE treatment
  ▪ The underlying facts and circumstances of the noncompliance
  ▪ The level of risk to reliability (including mitigating factors during the pendency of the noncompliance)
  ▪ The registered entity’s preventive and corrective processes and procedures to handle noncompliance, management practices, and culture of compliance
  ▪ Appropriateness of mitigation activities
• CEs are not aggravating factors in an entity’s compliance history
  ▪ Exceptions
    o Subsequent serious risk violation with similar cause to prior CE
    o Recurrent conduct may disqualify a noncompliance from CE treatment

• Encourage self-monitoring
  ▪ At registered entity level
  ▪ At ERO Enterprise level
Risk
Questions and Answers
Break

Webinar participants: We will return at 2:45 p.m. Central
NERC Standards Development Update

Steven Noess, Director of Standards Development
Sean Cavote, Manager of Standards Development
July 12, 2017
• Reliability Standards Development Plan (RSDP)
• Periodic Review Overview
• Periodic Review Process
• Periodic Review Template
• Standards Grading
• 2017 Periodic Reviews Projects
• 2018 and beyond
• The Draft 2018-2020 RSDP
  ▪ Satisfies standards development reporting obligations
  ▪ More forward looking
    o Apprises industry of expected standards development activity for resource allocation and planning
  ▪ Shifts focus to several key areas:
    o Periodic Reviews
    o Regulatory directives
    o Emerging risks and changing technologies
    o Standard Authorization Requests (SARs)
    o Standards Grading initiative
• 2017 Standards Development Activity Reporting
  ▪ Five projects from previous RSDP expected to continue into 2018
    o 2013-03 Geomagnetic Disturbance Mitigation
    o 2015-09 Establish and Communicate System Operating Limits
    o 2015-10 Single Points of Failure
    o 2016-02 Modifications to CIP Standards
    o 2016-EPR-01 Enhanced Periodic Review of PER-001, PER-003, and PER-004
  ▪ Four additional projects identified and expected to continue from 2017 into 2018
    o 2016-04 Modifications to PRC-025-1
    o 2017-03 FAC-008 Periodic Review
    o 2017-04 Periodic Review of INT-004, INT-006, INT-009 and INT-010
    o 2017-05 Periodic Review of NUC-001-3
• Periodic Reviews
  - Four active Periodic Reviews in 2017
  - At least two additional Periodic Reviews are expected in 2018
    - 31 standards will be eligible

• Regulatory Directives
  - 29 outstanding FERC directives
  - Additional FERC directives expected through 2018

• Standards Grading Metric
• 2018-2020 RSDP Time Line
  ▪ Standards Committee (SC) endorsed on June 21, 2017
  ▪ Posted for comment June 26 to July 25, 2017
  ▪ Final SC endorsement expected on September 2017
  ▪ NERC Board of Trustees November 2017
  ▪ Final 2018-2020 posting expected December 2017
    o Includes final 2017 standards grades
Periodic Review Overview

- Periodic Review projects initiated in 2016
  - PER-001, PER-003, PER-004
  - VAR-001 and VAR-002 (complete)

- Periodic Review projects initiated in 2017
  - FAC-008-3
  - INT-004-3.1, INT-006-4, INT-009-2.1, and INT-010-2.1
  - NUC-001-3
• RSDP requires NERC to conduct Periodic Reviews to address:
  ▪ Emerging risks
  ▪ Regulatory directives
  ▪ SARs

• Periodic Review inputs include:
  ▪ Standards grading results
  ▪ Technical analyses
  ▪ Emerging risks and changing technologies
  ▪ Reliability Issues Steering Committee (RISC) identified emerging risks
  ▪ Compliance violation statistics
  ▪ Inputs from industry on feedback loops
Periodic Review Overview

• Feedback loops
  ▪ Lessons Learned and FAQs
  ▪ Rationales and guidelines
  ▪ Measures
  ▪ Request for interpretations
  ▪ Reliability Standard Audit Worksheet development and Compliance Input
  ▪ Audit feedback
  ▪ Regional variances
  ▪ Construct of standards
  ▪ Surveys and polls
  ▪ Coordination with the North American Energy Standards Board
Periodic Review Overview

- Elements of consideration for periodic review prioritization:
  - RISC category rankings
  - Feedback on risk
    - NERC
    - Technical committees
    - Industry
  - Outstanding regulatory directives
  - Requirements that are candidates for retirement
Periodic Review Process

- Measured pace with in-depth review to improve quality and content of standards
- Commence with a period of study and data evaluation of three to six months
- Evaluate standards grading results and analyses
- Seek opportunities to make standards more concise
• Reliability Standards Eligibility Criteria for Periodic Reviews
  ▪ All requirements in effect for at least one year
  ▪ Compliance expectations are not clear
  ▪ Standard is not being consistently monitored
  ▪ Feedback loops indicate risk
  ▪ Outstanding Paragraph 81 requirements not previously addressed
  ▪ Implementation of the Standards Independent Experts Review Project - Final Report recommendations
Periodic Review teams (PRT) consists of two subgroups:

- **Standing Review Team**
  - Standards Committee
  - Operating Committee
  - Planning Committee
  - Critical Infrastructure Protection Committee
  - Regions
  - NERC staff

- **Subject Matter Expert Review Team**
  - Appointed by the SC
  - Smaller teams of 8-10 industry subject matter experts
**Periodic Review Process**

- Each subgroup completes its respective portion of the periodic review template
  - Affirm
  - Retire
  - Revise

- Recommendation of the Periodic Review team
  - Posted for a 45-day comment period
  - Comment responses posted
  - Final recommendation to the SC
Standards graded from the 2017-2019 RSDP

- BAL-003
- COM-001
- COM-002
- FAC-001
- FAC-002

- IRO-009
- MOD-032
- TPL-001
• Standards Grading Scoring:
  ▪ 0-3 quality score
  ▪ 1-13 content score
  ▪ Alignment with other standards
• Evaluation Criteria

  ▪ Content score of 0-3 based on:
    o Score of 1 – Is the content of the requirement technically correct, including identifying who does what and when?
    o Score of 2 – Are the correct functional entities identified?
    o Score of 3 – Are the appropriate actions, for which there should be accountability, included or is there a gap?

  ▪ Quality score of 0-13 based on:
    o Should the requirement stand alone as-is, or should it be consolidated with other standards?
    o Is it drafted as a Results-based Standard (RBS) requirement (performance, risk (prevention) or capability) and does it follow the RBS format (e.g., sub-requirement structure)?
Figure 1: Evaluation Flow Chart
• Standards Grading Process
  ▪ Identify eligible standards
  ▪ Conduct initial grading session
  ▪ Stakeholder comment period
  ▪ Finalize standards grades
  ▪ Publish final grades in RSDP
2017 Periodic Reviews Projects

• 2017 Periodic Reviews commencing in 2017
  ▪ FAC-008-3
  ▪ INT-004-3.1, INT-006-4, INT-009-2.1, and INT-010-2.1
  ▪ NUC-001-3

• Anticipated Project Time Lines
  ▪ May 2017: SC authorizes PRT nomination solicitation
  ▪ July 2017: SC considers PRT recommendations
  ▪ Q4 2018: Expected project completion dates
• Component of future RSDPs
• Optimize standards
• Identify new risks and emerging technologies
  ▪ Continue collaboration with industry and technical committees
• Address regulatory directives
• Respond to SARs
• React to compliance and enforcement data
Questions and Answers
Implementation of Modified TOP and IRO Standards

Soo Jin Kim, NERC Manager of Standards Development
2017 Standards and Compliance Workshop
July 12, 2017
• FERC approved two Reliability Standards on April 17, 2017 addressing TOP and IRO directives from Order No. 817
  ▪ IRO-002-5 – Reliability Coordination – Monitoring and Analysis
  ▪ TOP-001-4 – Transmission Operations

• IRO-002-5 effective October 1, 2017
• TOP-001-4 effective July 1, 2018
• Modifications address three objectives from Order No. 817:
  ▪ Transmission Operator monitoring of some non-BES facilities
  ▪ Redundancy and diverse routing of data exchange capabilities
  ▪ Testing for data exchange capabilities used in primary control centers

• Applicable to Reliability Coordinators (RC), Transmission Operators (TOP), and Balancing Authorities (BA)
Monitoring Non-BES Facilities

- **Directive:** Modify requirements to address monitoring non-BES facilities within or outside the TOP area as necessary for determining System Operating Limit (SOL) exceedances
  - Addresses potential gap during BES exception processing, or situations where some non-BES facilities should be monitored for reliability purposes
  - Brings TOP requirements in line with monitoring requirements for RC’s

- TOP-001-4 Requirement R10 addresses the directive
**R10.** Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area:

**10.1** Monitor Facilities within its Transmission Operator Area;

**10.2** Monitor the status of Remedial Action Schemes within its Transmission Operator Area;

**10.3** Monitor non-BES facilities within its Transmission Operator Area identified as necessary by the Transmission Operator;

**10.4** Obtain and utilize status, voltages, and flow data for Facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator;

**10.5** Obtain and utilize the status of Remedial Action Schemes outside its Transmission Operator Area identified as necessary by the Transmission Operator; and

**10.6** Obtain and utilize status, voltages, and flow data for non-BES facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator.
• The objective is to monitor all facilities necessary for determining SOL exceedances.

• Examples of analyses performed by TOPs to identify non-BES facilities that should be monitored:
  ▪ Operational Planning Analysis (OPA);
  ▪ Real-time Assessments (RTA);
  ▪ Analysis performed by the TOP as part of BES Exception processing for including a facility in the BES; and
  ▪ Analysis which may be specified in the RC's outage coordination process that leads to the identification of a non-BES facility that should be temporarily monitored for determining SOL exceedances.
• **Directive:** Modify standards to include requirements for redundancy and diverse routing of data exchange capabilities used by RC, TOP, and BA

• IRO-002-5 Requirement R2 and TOP-001-4 Requirements R20 and R23 address the directive
R2. Each Reliability Coordinator shall have data exchange capabilities, *with redundant and diversely routed data exchange infrastructure within the Reliability Coordinator's primary Control Center*, for the exchange of Real-time data with its Balancing Authorities and Transmission Operators, and with other entities it deems necessary, for performing its Real-time monitoring and Real-time Assessments.
• Redundant and diversely routed data exchange capabilities **preclude single points of failure** in primary Control Center data exchange infrastructure from halting the flow of Real-time data.
  - Instantaneous fail-over of data exchange capabilities is not required
  - Provides for continued data exchange functionality during outages, maintenance, or testing of data exchange infrastructure. For periods of planned or unplanned outages of individual data exchange components, the proposed requirements do not require additional redundant data exchange infrastructure components solely to provide for redundancy.

• Requirements apply to infrastructure **within the primary Control Center only**
• **Directive:** Modify standards to require testing of alternate data exchange capabilities used by RC, TOP, and BA in primary control centers

• IRO-002-5 Requirement R3 and TOP-001-4 Requirements R21 and R24 address the directive
R3. Each Reliability Coordinator shall test its primary Control Center data exchange capabilities specified in Requirement R2 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Reliability Coordinator shall initiate action within two hours to restore redundant functionality.
A test demonstrates that data exchange capabilities will continue to operate despite the malfunction or failure of an individual component

- (e.g., switches, routers, servers, power supplies, and network cabling and communication paths between these components in the primary Control Center).

Tests do not need to address all failure modes each quarter

- “An entity's testing practices should, over time, examine the various failure modes of its data exchange capabilities.”
• IRO-002-5 effective October 1, 2017 (3 months following regulatory approval)

• TOP-001-4 effective July 1, 2018 (12 months following regulatory approval)
  ▪ Longer implementation period is needed due to new requirement for TOPs to monitor some non-BES facilities (R10)
Questions and Answers
• Order approving **IRO-018-1** and **TOP-010-1** (RD16-6-000; 9/22/16)

• Order No. 830 approving **TPL-007-1** (RM15-11-000; 9/22/16)

• Letter Order approving **COM-001-3** (RD16-9-000; 10/28/16)

• Letter Order approving revisions to VRFs for **IRO-018-1** and **TOP-010-1** (RD16-6-001; 12/14/16)

• Letter approving an interpretation of Reliability Standard **CIP-002-5.1a** (RD17-2-000; 12/27/16)
Order No. 835 approving Reliability Standard **BAL-002-2** (RM16-7-000; 1/19/17)

Letter Order approving an interpretation to regional Reliability Standard **BAL-002-WECC-2a** (RD17-3-000; 1/24/17)

Letter Order approving Reliability Standards **IRO-002-5** and **TOP-001-4** (RD17-4-000; 4/17/17)

Letter Order approving regional Reliability Standard **VAR-501-WECC-3** (RD17-5-000; 4/28/17)
• Letter Order approving retirement of regional Reliability Standard **PRC-002-NPCC-01** (RD16-8-000; 8/19/16)

• Letter Order approving retirement of Reliability Standard **BAL-004-0** (RD17-1-000; 1/18/17)

• Letter Order approving retirement of regional Reliability Standard **TOP-007-WECC-1a** (RD16-10-000; 3/10/17)
• Notice of Inquiry Regarding Cyber Systems in Control Centers (RM16-18-000, 7/21/16)
• NOPR to approve Reliability Standards **BAL-005-1** and **FAC-001-3** (RM16-16-000; 9/22/16)
• NOPR proposing to approve Reliability Standard **PRC-012-2** (RM16-20-000; 1/19/17)
• Order No. 829 directing development supply chain risk management reliability standard (RM15-14-001; 7/21/16)

• Letter Order Approved Amendments to FRCC Regional Reliability SDPM (RR17-1-000; 3/3/17)

• Letter Order Approving Amendments to the Texas RE Bylaws and RSDP (RR17-3-000; 5/30/17)
• Petition for approval of proposed Reliability Standards **PRC-027-1** and **PER-006-1** (RM16-22-000; 9/2/16)

• Petition for approval of proposed Reliability Standard **CIP-003-7** (RM17-11-000; 3/3/17)

• Petition for approval of proposed Reliability Standards **EOP-004-4, EOP-005-3, EOP-006-3** and **EOP-008-2** (RM17-12-000; 3/27/17)
### Proposed Revisions to NERC Rules of Procedure

<table>
<thead>
<tr>
<th>Status</th>
<th>Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending Regulatory Approval</td>
<td>• Revisions to Section 400 and Appendices 2 and 4C of ROP regarding</td>
</tr>
<tr>
<td></td>
<td>consolidated hearing process (filed December 2016)</td>
</tr>
<tr>
<td>Pending NERC Board Approval or</td>
<td>• Revisions to Sections 600 (Personnel Certification and 900 (Training</td>
</tr>
<tr>
<td>Filing</td>
<td>and Education)</td>
</tr>
<tr>
<td>In Progress</td>
<td>• Revisions to Appendix 3A (Standard Processes Manual) of ROP:</td>
</tr>
<tr>
<td></td>
<td>Section 6.0 (Processes for Conducting Field Tests and Collecting and</td>
</tr>
<tr>
<td></td>
<td>Analyzing Data); Section 7.0 (Interpretations); and Section 11.0 (</td>
</tr>
<tr>
<td></td>
<td>Reference Documents)</td>
</tr>
</tbody>
</table>
NERC and NERC members shall comply with these Rules of Procedure. Each Regional Entity shall comply with these Rules of Procedure as applicable to functions delegated to the Regional Entity by NERC or as required by an appropriate governmental authority or as otherwise provided.

Each bulk power system owner, operator, and user shall comply with all NERC Rules of Procedure that are applicable to such entities by approval pursuant to applicable legislation or regulation or pursuant to agreement.

Any entity that is unable to comply or that is not in compliance with a NERC Rule of Procedure shall immediately notify NERC in writing, stating the rule of concern and the reason for not being able to comply with the rule.

NERC shall evaluate each case and inform the entity of the results of the evaluation. If NERC determines that a rule has been violated, or cannot practically be complied with, NERC shall notify the applicable governmental authorities and take such other actions as NERC deems appropriate to address the situation.

NERC shall comply with each approved Reliability Standard that identifies NERC or the electric reliability organization as a responsible entity. Regional Entities shall comply with each approved Reliability Standard that identifies Regional Entities as responsible entities. A violation by NERC or a Regional Entity of such a Reliability Standard shall constitute a violation of these Rules of Procedure.

Rules of Procedure

<table>
<thead>
<tr>
<th>Appendix Number</th>
<th>Title/Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Revisions to NERC Rules of Procedure – Alignment of Appendix 2 to NERC Glossary – June 12, 2015 Posting (14)</td>
<td></td>
</tr>
<tr>
<td>Proposed Revisions to NERC Rules of Procedure – Risk-Based CMSP Compliance Filing – April 6, 2015 Posting (20)</td>
<td></td>
</tr>
<tr>
<td>Proposed Revisions to NERC Rules of Procedure – Risk-Based Registration Initiative Compliance Filing – April 13, 2015 Posting (15)</td>
<td></td>
</tr>
<tr>
<td>Proposed Revisions to NERC Rules of Procedure – Section 317 – August 7, 2015 Posting (5)</td>
<td></td>
</tr>
<tr>
<td>Rules of Procedure in Effect (14)</td>
<td></td>
</tr>
</tbody>
</table>

http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx
Filings & Orders

The Filings & Orders pages contain documents that pertain to FERC and Canadian authorities. They relate to FERC Delegated Orders and Notices and FERC and provincial filings and are arranged by date. These documents are necessary for promoting the reliability of the bulk power system in North America.

http://www.nerc.com/FilingsOrders
Questions and Answers
General Question and Answer