• Critical Infrastructure Protection (CIP) Standards – A Year of Version 5
  ▪ Compliance Performance Data
  ▪ Technical Feasibility Exceptions
  ▪ Remote Access Study Summary
• CIP-014-2 – Assessing Effectiveness
  ▪ High Impact Control Centers
  ▪ Security for Substations
• Looking Forward to 2018
  ▪ Risk-based Monitoring and Oversight
  ▪ Focus on Controls and Security Best Practices
• Trends
  - Five of the ten most violated Reliability Standards are CIP.
  - This is consistent with previous years’ performances.
• Trends
  ▪ 90 percent of noncompliance are self-identified.
  ▪ The ERO Enterprise is focusing on effective mitigation of self-identified noncompliance.

July 1, 2016 through July 1, 2017

Self-identified
Audit/Spot Check
The ERO Enterprise is focusing on effective organizational alignment:

- Compliance department integrated with operational business units
- Operational expertise reflected in procedures
- Subject matter experts understand compliance obligations
- Executive leadership engaged
- V3: 600 Critical Assets with Critical Cyber Assets
- V5: 3000 High and Medium Facilities Containing BES Cyber Systems
- V5: 500 Percent Scope Increase

Number of Violations by Year

- 2014: 700
- 2015: 600
- 2016: 500
- 2017: 400

**Noncompliance Rates Decreased**
Why has noncompliance decreased?

- Option for early adoption to Version 5;
- Small Group Advisory sessions;
- Risk-based Compliance Monitoring Enforcement Program (CMEP) activities appropriately scoped;
- Lessons learned and FAQs;
- Outreach, including on-site meetings with registered entities;
- Training for auditors;
- Standardized V5 audit evidence; and
- Continued review of the Reliability Standards.
• Technical Feasibility Exceptions (TFEs) reduced from 4323 in 2015 to 400 in 2017.
• 600,000 devices had TFEs associated with them in V3. This number has decreased to 2000 devices in V5.
• The CIP standards have less requirements that are eligible for TFEs.
• NERC is filing a report with the Federal Energy Regulatory Commission (FERC) in September to assess the status and effectiveness of the TFE program.
CIP-005-5 Noncompliance Types
July 1, 2016 through May 15, 2017

- Overly Permissive Access into ESP
- Ineffective Monitoring of Access Points
- Inadequate Authentication Controls
- Encryption Not Applied to Traffic Accessing BCS
- Electronic Access Point Change Management
- EACMS not Identified and Not Protected
- Direct Access from Outside of ESP to BCS
- BCS Not within an ESP
• The Remote Access Study Report was filed with FERC on June 30, 2017, in response to Order No. 822.

• Areas of Continued Focus identified with corresponding action items:
  
  - **Effective Mitigating Practices**: Positive observations to be leveraged across industry;
  
  - **Areas for Further Analysis**: Perform research, guidance, or standards modifications;
  
  - **Enhancement Opportunities**: Encouraging the use of best practices to comply with the CIP standards; and
  
  - **Training and Awareness**: General training and outreach.
Remote Access Study Action Items

- Webinars from NERC and the Regional Entities (REs) to highlight certain emerging risks or effective mitigating practices;
- Critical Infrastructure Protection Committee (CIPC) collaboration with NERC to address industry specific risk and trends identified in the study;
- NERC to present the focus areas that may warrant Reliability Standards consideration to the standards drafting team especially for those items already being address by active standards development activity; and
- The use of E-ISAC to convey specific mitigations to known threats or vulnerabilities.
• Continued focus on CIP-014
  ▪ CIP-014 is in scope for all Transmission Owner Compliance Audits and Spot Checks.
  ▪ The focus is on identification of appropriate facilities.
  ▪ FERC filing is due in September on the high-impact Control Centers covered by CIP-014.

• Effective Controls for CIP-014:
  ▪ Intrusion detection systems,
  ▪ Video surveillance and analytics,
  ▪ Thermal cameras,
  ▪ Anti-climb/anti-cut fencing,
  ▪ Ballistic resistant fencing,
  ▪ Ballistic panels or walls,
  ▪ Transformer specific detection,
  ▪ Additional lighting,
  ▪ Vehicle barriers,
  ▪ Use of natural environment,
  ▪ Shot detection, and
  ▪ Crash gates.
• NERC and the REs will continue to focus on evaluating remote access security controls in 2018.
• There will be an increase in ERO Enterprise training on network assessment technical rigor.
• Monitoring will focus on architecture and process.
• There will be continued focus on real-world cyber events, such as WannaCry and CrashOverride, during CMEP activities.
• There will be increased coordination with the CIPC to address emerging issues.
Questions and Answers
ERO Enterprise Program Alignment Efforts

Ken McIntyre, Vice President and Director of Standards and Compliance
Compliance Committee Open Meeting
August 9, 2017
• Electric Reliability Organization (ERO) Enterprise program implementation and execution consistency is a common concern reported by stakeholders.

• The Board of Trustees Compliance Committee (BOTCC) supported a continued effort for NERC working with the Compliance Certification Committee (CCC), specifically to develop a proposal to identify and manage consistency issues.
• The CCC conducted a focused discussions on consistency (June and September 2016).

• NERC drafted the Consistency Framework (February 2017).

• The BOTCC conducted a discussion with NERC and the Regional Entities (REs) on the Consistency Framework (February 2017).

• NERC staff presented the Consistency Framework to the NERC Trustees and RE Board Officers meeting (May 2017).

• The CCC established the Consistency Working Group (May 2017).

• NERC staff developed and implemented the ERO Enterprise Program Alignment process (July 2017).
Program Alignment Process

Track
Identify & Capture Issues
- Program Oversight and Monitoring
- Survey Responses
- Stakeholder Reporting
- NERC Central Repository

Triage
Classify, Analyze & Prioritize
- NERC Initial Screening
- Regional Input and CCC Consistency Working Group engagement
- Determine materiality and priority
- Develop responses and recommendations

Transparent
Post & Report
- Program Alignment - Issues and Recommendations Tracking
- Quarterly Reporting
- Regional Program Information
Process Roles and Responsibilities

• NERC is responsible for the Program Alignment process:
  ▪ Consistency Reporting Tool, hosted by EthicsPoint by NAVEX Global;
  ▪ Offers anonymity;
  ▪ Captures and tracks all reported issues in central repository;
  ▪ Timely responses and updates; and
  ▪ Reports issues and recommendations (transparency).

• NERC and the REs ensure programs are aligned:
  ▪ Determine materiality and priority,
  ▪ Develop recommendations and implement them, and
  ▪ Provide regional program information.

• Provided by stakeholders:
  ▪ Feedback with details that are actionable, and
  ▪ CCC Consistency Working Group assistance to frame the issue and provide recommendations.
**EROS Enterprise Program Alignment Process**

The EROS Enterprise Program Alignment Process is intended to enhance efforts to identify, prioritize, and resolve alignment issues across the EROS Enterprise. This is a repeatable, transparent process that registered entities (or other relevant industry stakeholders) may use to report any perceived inconsistency in the approach, methods, or practices implemented and executed by the Regional Entities.

Using this process, NERC will capture identified issues from the various resources in a centralized repository. NERC will classify the issue through an initial screening process to ensure the appropriateness for this process, then work with Regional Entities and stakeholders (Compliance and Certification Committee) to analyze the issues and determine the scope and material impact. The EROS Enterprise will develop recommendations and determine the priority of the activities taking into consideration all EROS Enterprise efforts. Finally, NERC will post the issue along with the recommendations/results in the Program Alignment – Issues and Recommendations Tracking document and provide status updates on its activities.

The EROS Enterprise Program Alignment Process relies on input from NERC’s oversight and monitoring, regional observations, and registered entity reporting. The program aims to strengthen the EROS Enterprise’s collaborative and transparent approach to resolving consistency issues.

**Submitting an Issue using the Consistency Reporting Tool**

NERC implemented the Consistency Reporting Tool using a third-party application, EthicsPoint, which allows stakeholders to submit consistency issues—anonymously, if desired. While issues may be submitted anonymously, the submitter may also choose to provide their name and contact information, which may help expedite the process in understanding the scope and material impact of the reported issue. If the submitter chooses to remain anonymous, they should check their request six-to-seven business days after submittal via the Consistency Reporting Tool for additional information requested by NERC. If the submitter provides their name and contact details, NERC will contact them directly.

**Note:** NERC encourages stakeholders and registered entities to first work to resolve any issues with the Regional Entity Involved. If the registered entity is unable to resolve the issue with their Regional Entity, then they may consider submitting the issue using the Consistency Reporting Tool.

**Contact Us**

For more information about Program Alignment, please email consistency@nerc.net
• Host: EthicsPoint by NAVEX Global
• Anonymity Option

Make a Report
Follow up on a Report
NERC Resources
FAQs

To Make a Report

- Select the "Make a Report" link at the top of this web page.

After you complete your report you will be assigned a unique code called a "report key." Write down your report key and password and keep them in a safe place. You have five (5) business days to amend the report.

Organization/Tier: North American Electric Reliability Corporation

* Do you wish to remain ANONYMOUS for this report?
  - Yes
  - No
• Stakeholder Input
• Research and Frame Issues
• Provide Recommendations
**Issues and Recommendations**

- Track and Report
- Transparency of Responses and Activities

---

### Program Alignment - Issues and Recommendations Tracking

<table>
<thead>
<tr>
<th>Item #</th>
<th>Short Description</th>
<th>Long Description</th>
<th>Issue Discovery</th>
<th>Discovery Date</th>
<th>Planned Resolution Date</th>
<th>Status</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 24</td>
<td>RSAWs</td>
<td>The RE is using a modified version of some NERC RSAWs rather than the ones posted on the NERC website. Most of the differences are in formatting. In one standard (FPE-005-G), the subject RE’s version is better because it includes a compliance timetable (when compliance with individual requirements must be achieved). However, given the amount of Multi-Region Regional Entities, a single RSAW per NERC standard should be used by all Regions for administrative efficiency.</td>
<td>Reporting Tool</td>
<td>04/26/17</td>
<td>08/2017</td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

1. No content differences (e.g., to the evidence requested or compliance approach) were identified in the RE’s RSAW. The RE’s RSAWs included minor formatting differences as well as the compliance implementation timetable at the beginning of one RSAW. The RE has since removed the compliance implementation timetable from the RSAW. NERC and the regions are updating legacy versions of RSAWs to ensure all RSAWs are on the current template to address formatting differences between RSAWs.

2. All Regions should continue to use the current NERC RSAW evidence requested and compliance approaches posted on the NERC public website.
• NERC Rules of Procedure allow some flexibility for REs when designing and implementing certain procedures.

• The Regional Program Information Matrix captures where these differences exist and seeks to increase overall transparency.

• Its focus is on the main process and interactions (not all).
Next Steps

• Process is live!
• ERO Enterprise Program Alignment Process Page is here:
• For more information about the Program Alignment, contact us at consistency@nerc.net.
Questions and Answers
CMEP Highlights

- Program Alignment on CMEP Activities
- CMEP Technology Program
- CMEP Mitigation Plan Process Review
• Annual FFT/CE Review Completed
• Enforcement staff filed one Full Notice of Penalty covering two moderate risk violations for a total penalty of $201,000.
• Mitigation completion rates remain an area of focus.
  ▪ Over 99 percent of violations discovered in 2014 and prior have been mitigated.
• The average age of noncompliance in inventory is under eight months.
• Self-identification of noncompliance is 93.6 percent.
• There are 65 registered entities in the Self-Logging Program.
  ▪ FRCC added its first registered entity.
• The updated guide provides the following:
  ▪ Principles for evaluating controls,
  ▪ Value of effective controls, and
  ▪ Clarification around documentation.

• Outreach at the NERC Standards and Compliance Workshop
  ▪ Industry Panel on Internal Controls
• Implementation Guidance
  ▪ 18 Endorsed, 7 Non-Endorsed, 1 Retired, 5 Open

• Industry Webinar Conducted on May 31, 2017

• Outreach at the NERC Standards and Compliance Workshop
Questions and Answers