



MIDWEST  
RELIABILITY  
ORGANIZATION

# CIP-012 Readiness Assessment Pilot

Jess Syring, CIP Compliance Manager

CLARITY

ASSURANCE

RESULTS

# History of Project

- **CIP-012 Readiness Assessment was created in response to feedback received**
  - Requests for identifying best practices and lessons learned earlier
  - Provide understanding of requirement language
  - Potential to find some gray areas in the language to start ERO conversations to provide clarity



# Timeline

- **Early 2021**

- Proposed project to CMEPAC
- Requested volunteers from CMEPAC members
- Had four volunteers and accepted all

- **June 2021**

- Informal notifications sent to volunteer entities from CMEPAC



# Timeline

- **August 2021/September 2021**
  - Received evidence from volunteers
  - Reviewed and documented
- **October 2021/November 2021**
  - Requested additional information
  - SME interviews
- **December 2021/January 2022**
  - Went over conclusions



# Lessons Learned

## ● Evidence Request Tool

- Needed a lot of clarifications for the sampling tab
  - Received Cyber Asset/Device names on tab
  - Needed clarification on whether per applicable Registered Entity communication path
  - Sampling made it hard to answer Level 2 tab evidence requests
  - Clarification on what Level 2 information was being requested



# Lessons Learned

- **Needed clarity on agreements being utilized for transferring compliance responsibilities**
  - Many agreements were not finalized and therefore just a current example was provided of what was being proposed
  - Resources for clarification:  
<https://vimeo.com/208678157> or  
<https://vimeo.com/436056292>

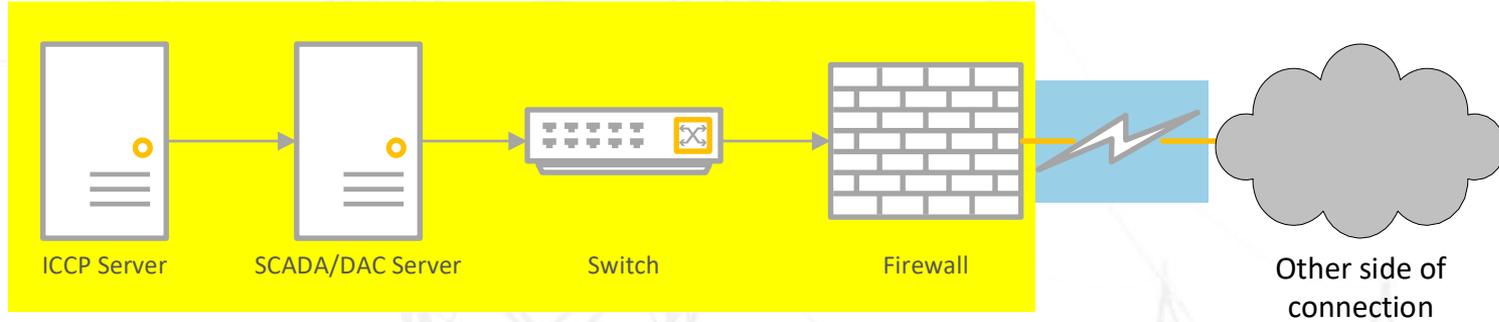


# Lessons Learned

- **Clarity on ensuring all applicable communications were being considered**
  - One entity provided a list of all of their other parties that were evaluated
  - Clarification for other potential applicable communications
- **More questions were asked when only physical or electronic protections were in place**



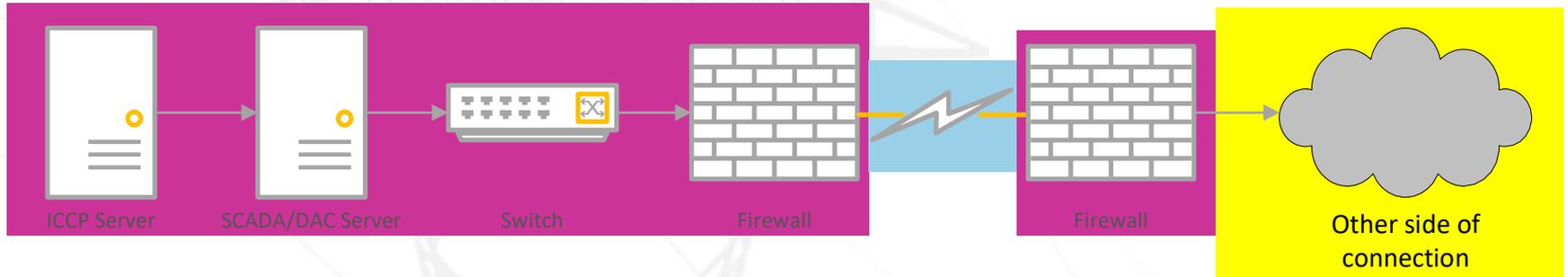
# Example of path identification



Yellow indicates physical protections in place  
Blue indicates electronic protections in place



# Example of path identification



Pink indicates physical and electronic protections in place  
Blue indicates electronic protections in place  
Yellow indicates physical protections in place



# Lessons Learned

- **Clarity on ensuring what communications were applicable**
  - Evidence received was TOP and IRO specifications
    - Had to pull in O&P staff to understand what was applicable
  - Ensuring that protections were in place from start of communications to where the communications ended (not just when it left the control center)



# Lessons Learned

## ● Time flexibility

- The extended timeline allowed for flexibility at various different aspects of the project in order to make evidence available as well as respond to RFIs
- Additional time was still needed to have clarifying conversations, but the holidays had an effect for getting the additional information



# Lessons Learned

- **Positive Observations:**

- Diagram provided that showed the various physical or electronic protections at each point of the communications
- Utilizing higher encryption levels
- Loss of link for failure of encryption
  - There were additional redundancies as well before this would occur



# Future version of CIP-012

- **Version 2 is still out for ballot**
- **Introduces availability of data aspect**
  - Technical rationale defines as “Ensuring timely and reliable access to and use of information”
- **Introduces recovery of applicable links**
  - Technical rationale indicates potential to incorporate into CIP-008 and CIP-009 standards
- **Technical Rationale is a good source**



# Future of Readiness Assessments

- **MRO and the CMEPAC will work together to present a review of the investments in time and energy in this pilot to the value this pilot brought to MRO staff and the MRO registered entities**
- **MRO will present this analysis to the OGOC as we consider continuing this program**



# Disclaimer

**The Midwest Reliability Organization (MRO) CMEPAC is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) developed any materials, including presentations, through the MRO CMEPAC from member organizations within the MRO Region and other government and industry security experts. The views in the following presentations are presented by these MRO CMEPAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.**





MRO CIP-012 Readiness Assessment

# ATC's Experience



CLARITY

ASSURANCE

RESULTS

# ATC's Experience

## Process

- **MRO sought volunteers for a CIP-012 Readiness Assessment**
- **ATC volunteered with transparency that our testing and implementation plan could not meet the proposed schedule**
- **MRO adjusted the timeline so we could participate (6-month period)**
  - Jun 14, 2021: Official MRO Level 1 and Level 2 RFIs received
  - Jul 31, 2021: Level 1 submitted (CIP-012-R1-L1-01, CIP-012-R1-L1-02)
  - Oct 1, 2021: Level 2 submitted (CIP-012-R1-L2-01)
  - Oct 18, 2021: MRO provided feedback and two additional RFIs
  - Nov 15, 2021: ATC response to ad-hoc RFIs
  - Jan 13, 2022: MRO, RF, ATC call to discuss outcomes



# ATC's Experience

## Participating to Learn

- **Approach – Open minded with a questioning attitude:**
  - ATC had immediate questions about the NERC Evidence Request Tool (ERT), and the use of the BES Asset tab for CIP-012
  - MRO made themselves available to discuss, and were flexible in finding a path forward
  - Several opportunities for improvement were identified, and an interim plan was agreed upon to advance the pilot
- **MRO RFIs – fresh perspective for consideration**
  - Plan details: More specificity recommended for cyber security methods
  - Encryption: Healthy curiosity about why we had varied levels on routers vs firewall
  - Clarity on split responsibilities: Use of Memorandums of Understanding (MOU)



# ATC's Experience

## Outcomes, Lessons Learned, and Preparedness

- **ATC's RFI Response – Seized the Opportunities**

- Plan details: Additional specificity on cyber security methods made our plan clearer
- Encryption: Internal conversations led to additional testing of encryption capabilities vs potential operational impact. We gained internal alignment and more robust technical controls.
- Clarity on split responsibilities: MOUs are our intent and gaining perspective on our template helped foster additional conversations with our connected Responsible Entities, as well as standardization of our implementation.

- **Value – Reasonable Assurance and Program Improvements before CIP-012-1 is Enforceable**

- Participation provided affirmation of interpretation that CIP-012 is end to end and can be a combination of physical and cyber security controls, as we have articulated in our plan and MOUs.
- Our inclination to leverage our detailed TOP-001-5 R20 diagrams as the basis to build supporting CIP-012-1 diagrams paid off, leading to a clear depiction of all entity communications and the protections in place for each portion of that communication
- Practice with the ERT format led to enhancements in our configuration management system, giving us capability to inventory ATC-owned infrastructure as 'CIP-012 path-only' or 'CIP-012 security protection point', and report on that infrastructure in one click.
- We have documented our internal controls and have confidence our processes will result in a timely, complete, and accurate population of communication infrastructure.
- We are leveraging our CIP-010 Change Management processes to provide assurance the technical controls implemented for 'CIP-012 security protection point' continue to operate as designed. We are also leveraging monitoring and alerting tools for visibility of failovers.



CLARITY

ASSURANCE

RESULTS



MIDWEST  
RELIABILITY  
ORGANIZATION

# **CIP-012-1, Communications between Control Centers**

**MGE's overview of the MRO Readiness  
Assessment**

CLARITY

ASSURANCE

RESULTS

# Starting with the end in mind

- **CMEPAC members requested to volunteer for a CIP-012-1 Readiness Assessment (pilot program), MGE was selected.**
- **The Readiness Assessment would be carried out by the MRO CIP Audit team lead by Jess Syring, MRO Compliance Monitoring Manager, CIP.**
- **Submitted 2 sets of RFIs.**
- **Felt like a normal data review from MGE's point.**
- **Transitioned through the review very smoothly.**
- **Received feed back, discussed internally, updated where warranted.**



# MGE Lessons Learned

- FERC approved CIP-012-1 on 23 Jan 2020.
- 2 Aug 2019, collected internal maps and routes between MGE primary and backup Control Centers with SMEs.
- 1 Aug 2020, Made drawing of internal and external connections.
- 13 Nov 2020, reviewed Standard, Guidance, and wrote plan.
  - Mapped all Control Centers internally and external, stated such in plan.
  - Clarified that ICCP data (TOP-003 and IRO-010) was the data to protect.
- 19 May 2021, requested guidance from HEROS, answer received 20 May 2021.
- First plan approved 9 Jul 2021.
- Second plan approved 28 Dec 2021 based on MRO feedback.



# Approach to comply with CIP-012-1

- **NSRF involvement**

- Tracked development via NSRF
- Spoke with connected entities on their approach
- Spoke to CIPC (now RSTC) for technical guidance, working with industry experts

- **CMEPAC involvement**

- Approached by MRO Staff for this test Readiness Assessment and volunteered.

- **Proactive plan before FERC Approved (mapping)**

- Worked on initial plan prior to FERC approval and continuously updated our mapping.



# Advise to other Entities

- **Start early with all new/updated Standards.**
- **Internal conversations help design a plan of attack.**
- **Utilize all your tools to make your determinations of scope.**
  - HEROS
  - CIPC (RSTC)
  - Other like Entities
  - Industry experts
- **Be a CMEPAC Member in order to be “involved”**



# **Overall Benefits of the CIP-012-1 Readiness Assessment to MGE**

- **Reasonably Assured that MGE will be compliant on 1 Jul 2022.**
- **Briefed the MGE NERC Steering Committee that our compliance risk has been reduced due to participation in the Readiness Assessment.**
- **Have notes and working copies of plans to assist in our conversation when MGE is audited on CIP-012-1.**
- **Tracking CIP-012-2 and have draft updated plan based on Readiness Assessment plan.**





**We Energize Life**  
.....

# MRO CIP-012 Readiness Assessment

Oklahoma Gas & Electric

---

March 18, 2022



# OG&E's Experience

## OG&E's perspective on being part of the MRO Readiness Assessment:

- Participating would give OG&E the opportunity to work with MRO SMEs
- OG&E would receive feedback from MRO that would assist in being compliant by the enforcement date
- Made OG&E be proactive and to start the project with a higher priority



# Resources needed - Scoping

## *Relevant Links:*

[CIP-012-1 Standard](#)

[CIP-012-1 Technical Rationale](#)

[ERO Endorsed Implementation Guidance](#)

[2021 Virtual CMEP Conference \(pg. 124-130\)](#)

# Resources needed - Scoping

## MISO Plan for CIP-012

### **MISO is updating MSAs to include language for CIP-012 R1.3**

- Requires an addendum to the MSA to be executed prior to CIP-012 enforcement date (July 1, 2022)
- Effort requires 100% response as both MISO and entities need this documentation to meet their NERC CIP-012 requirements
- They also plan to be the central source of communication as SPP is planning to do (see diagrams included in slides), which will require router replacements for member companies as well.

# CIP-012 Auditor Presentation



HOME | ABOUT US | CAREERS | TRAINING | RESOURCE HUB

COMPLIANCE | ENFORCEMENT | REGISTRATION | RELIABILITY SERVICES | STANDARDS



**talk with TEXASRE**

**Odessa Disturbance: Lessons Learned and Best Practices**  
**March 3, 2022**

#### Upcoming Events

Date	Title
02/23/2022	Member Representatives Committee Meeting
02/23/2022	Audit, Governance, and Finance Committee Meeting
02/23/2022	Board of Directors Meeting
02/24/2022	NSRF Meeting



# CIP-012 Auditor Presentation

[Align Release 2 TFE and Self-Certification Training](#) | [Recording](#)

## Workshops

[2021 Winter Weatherization Workshop](#) | [Recording](#)

[2021 GO/GOP Outreach](#) | [Recording](#)

[2021 CIP Workshop](#) | [Recording](#) | [CIP Workshop Q&A](#)



## Fall Standards and Compliance Workshop

[2021 Fall Standards and Compliance Workshop](#) | [Recording](#)



## Spring Standards and Compliance Workshop

[2021 Spring Standards and Compliance Workshop](#) | [Recording](#)



## Reliability 101



# OG&E Experience

## *Evidence of Compliance:*

***CIP-012 Communications Between Control Centers Plan  
Diagrams***

***Documentation demonstrating plan implementation and  
adherence***

***Testing documentation of controls implemented (SPP  
testing during implementation)***

# Working With O&P SMEs

**Document departments that ID communication paths**

**Document how the information is being used**

## **TOP-001 Data Exchange Infrastructure Redundancy Layers**

Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.

## **IRO-010/ TOP-003 Reliability Coordinator Data Specification and Collection**

- Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Load-Serving Entity, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using:
  - A mutually agreeable format
  - A mutually agreeable process for resolving data conflicts
  - A mutually agreeable security protocol



# OG&E Experience

## *CIP-005*

Logical implementation

Example: Data encryption, firewall, ICCP, VPN , defense in depth, types of encryption

## *CIP-006*

Physical implementation

Example: locked cabinets , card readers, Key management

---



# Working With SPP - BA

In preparation for ICCP communications to the new Operating Center, SPP informed OG&E that they are in the process of upgrading the existing Cisco 2011 routers deployed at entities with new Juniper devices.

OG&E has replaced SPP routers. One capability of the new SPP equipment will be support of router-router encryption. This will allow SPP to implement encryption (through SPP encryption keys between the routers) of the ICCP data between their routers and OG&E

The SCADA team will continue working with partner utilities to redirect communications through SPP as a central source.



# Working with SPP -BA

**SPP Organize a working group for implementation updates and documentation planning and install all 236 Juniper routers at member companies, then testing**

**OGE Work with partner companies to use shared ICCP links with SPP only (Western Farmers, OMPA, Southern CO.).  
Need to have conversations to gauge willingness to funnel the communications through SPP.**

**SPP and OG&E worked on MOU**

---



MIDWEST  
RELIABILITY  
ORGANIZATION

# **CIP-012-1, Communications between Control Centers**

**WFEC's overview of the MRO Readiness  
Assessment**

CLARITY

ASSURANCE

RESULTS

# WFEC Structure

- **Compliance overview and integration into multiple departments**
  - Cyber Compliance Specialist monitors changes in NERC CIP Standards
  - Notified departments of the new standard



# Origination of Being Compliant with CIP-012-1

- **Security first, Compliance second**
  - Changes from 2014 – 2022 and the early adoption of future compliance with CIP-012-1
  - Basic security hygiene will improve posture for future regulations
- **SPP**
  - Evolution of communication links to become compliant with CIP-012-1 and centralize communication among entities
  - Single external encrypted communication link was the result
- **Redundancy**
- **Gap Analysis**



# Readiness Assessment

- **Why volunteer?**

- Opportunity to engage audit team with no repercussions for new standard
- Learn how auditors will interpret and apply the standard for the region
- Understand the process and participate in making it better for all utilities

- **Preparatory work**

- Conduct internal meetings and review requirements while interacting with MRO personnel for answers to questions arising from the new standard
- Understand your process and what changes will need to be made

- **Process overview**

- Gather evidence and articulate how the evidence supports the foundational position you have taken towards the standard
- Conduct interviews with SMEs and other people
- Walk through results and final comments regarding the overall implementation of the new standard



# Takeaways

- **Clearly define Demarcation Points**
  - Understand the logical and physical demarcation points and properly articulate the data flows
- **Secure ICCP**
  - Secure the payload beyond just layer-2 and layer-3
- **Clarity and Understanding**
  - Understanding the auditor's perspective
  - Aligning expectations to reality
  - Preparing and updating evidence for first time audit of CIP-012-1
- **Forward thinking to 12-2**
  - Understanding CIP-012-1 to better prepare for CIP-012-2



# Questions



CLARITY

ASSURANCE

RESULTS

MRO

Jess Syring

Compliance Monitoring Manager, CIP

[Jess.syring@mro.net](mailto:Jess.syring@mro.net)

(651) 855-1762

ATC

Sharon Koller

Lead Compliance Strategist & CIP Senior Manager

[skoller@atcllc.com](mailto:skoller@atcllc.com)

262-832-8647

MGE

Joseph DePoorter

Director – NERC Compliance and Generation Operations

[jdepoorter@mge.com](mailto:jdepoorter@mge.com)

608-252-1599

OGE

Patrick T Wells

Manager NERC CIP Compliance

[WellsPT@OGE.com](mailto:WellsPT@OGE.com)

(405) 553-3921

WFEC

Trae Norman

IT Infrastructure Manager

[t\\_norman@wfec.com](mailto:t_norman@wfec.com)

405-247-4412



CLARITY

ASSURANCE

RESULTS