



MIDWEST
RELIABILITY
ORGANIZATION

Meeting Agenda

Security Advisory Council (SAC)

August 08, 2023

9:00 am to 3:00 pm central

*MRO Corporate Offices, King Conference Center
St. Paul, MN & Webex*

Classification: Public

CLARITY
Outreach & Engagement

ASSURANCE
Oversight & Risk Management

RESULTS
Reliability Performance

VIDEO AND AUDIO RECORDING

Please note that Midwest Reliability Organization (MRO) may make a video and/or an audio recording of this organizational group meeting for the purposes of making this information available to board members, members, stakeholders and the general public who are unable to attend the meeting in person.

By attending this meeting, I grant MRO:

1. Permission to video and/or audio record the meeting including me; and
2. The right to edit, use, and publish the video and/or audio recording.
3. I understand that neither I nor my employer has any right to be compensated in connection with the video and/or audio recording or the granting of this consent.

Classification: Public

MRO ORGANIZATIONAL GROUP GUIDING PRINCIPLES

These MRO Organizational Group Guiding Principles complement charters. When the Principles are employed by members, they will support the overall purpose of the organizational groups.

Organizational Group Members should:

1. Make every attempt to attend all meetings in person or via webinar.
2. Be responsive to requests, action items, and deadlines.
3. Be active and involved in all organizational group meetings by reviewing all pre-meeting materials and being focused and engaged during the meeting.
4. Be self-motivating, focusing on outcomes during meetings and implementing work plans to benefit MRO and MRO's registered entities.
5. Ensure that the organizational group supports MRO strategic initiatives in current and planned tasks.
6. Be supportive of Highly Effective Reliability Organization (HERO™) principles.
7. Be supportive of proactive initiatives that improve effectiveness and efficiency for MRO and MRO's registered entities.

Classification: **Public**



Agenda Item	
1	Call to Order and Determination of Quorum <i>Ian Anderson, Security Advisory Council Chair</i> <ul style="list-style-type: none">a. Determination of Quorumb. Robert's Rules of Order
2	Standards of Conduct and Anti-trust Guidelines <i>Steen Fjalstad, Director of Security, MRO</i> <ul style="list-style-type: none">a. OGOC updateb. HERO Awardc. Member Expectations
3	Advisory Council Work Plans <ul style="list-style-type: none">a. RACb. CMEPAC
4	MRO Regional Risk Assessment (RRA) <i>Mark Tiemeier, Principal Technical Advisor, MRO</i>
Break – 10:15 a.m. – 10:30 a.m.	
5	Regional Security Risk Assessment (RSRA) Working Session and Final Update <i>Lee Felter, Principal Security Engineer, MRO</i>
6	Stakeholder Survey <i>Ian Anderson, Security Advisory Council Chair</i>
7	MRO SACTF Update <i>Daniel Graham, Security Advisory Council Threat Forum Member</i> <ul style="list-style-type: none">a. MRO SACTF Threat Call and Annual Statisticsb. MRO SACTF Threat Call Feedbackc. MRO SACTF Open Source Information Sharing Document
8	MRO Representatives on NERC Subgroups Written Reports <i>Steen Fjalstad, Director of Security, MRO</i> <ul style="list-style-type: none">a. NERC Supply Chain Working Group (SCWG) – <i>Tony Eddleman</i>b. NERC Security Integration and Technology Enablement Subcommittee (SITES) - <i>Alan Kloster</i>c. NERC Reliability and Security Technical Committee (RSTC) – <i>Marc Child (providing update as this subgroup does not currently have an MRO representative)</i>
Lunch – 11:30 a.m. – 12:30 p.m.	
9	2023 Security Conference Planning Update <i>Cris Zimmerman, Manager of Outreach and Stakeholder Engagement, MRO</i>
10	Cloud Computing and Data Storage Training or Webinar <i>Patrick Glunz, Security Advisory Council Member</i>

Agenda Item	
11	Charter Updates <i>Ian Anderson, Security Advisory Council Chair</i> <ul style="list-style-type: none">a. MRO SAC Charterb. MRO SACTF Charter
12	2023 Work Plan Updates <i>Ian Anderson, Security Advisory Council Chair</i> <ul style="list-style-type: none">a. MRO SAC Work Planb. MRO SACTF Work Plan
Break – 2:00 p.m. – 2:15 p.m.	
13	Action Item Review <i>Margaret Eastman, Security Administrator, MRO</i>
14	Other Business and Adjourn <i>Ian Anderson, Security Advisory Council Chair</i>

AGENDA

Call to Order and Determination of Quorum

a. Determination of Quorum and Roster

Ian Anderson, Security Advisory Council Chair

Name	Role	Company	Term
Brett Lawler	Vice Chair	Xcel Energy	12/31/23
Chad Wasinger	Member	Sunflower Electric Power Corporation	12/31/23
Clayton Whitacre	Member	Great River Energy	12/31/25
Daniel Graham	Member	Basin Electric Power Cooperative	12/31/24
Douglas Peterchuck	Member	Omaha Public Power District	12/31/24
Ian Anderson	Chair	Oklahoma Gas and Electric	12/31/25
Jason Nations	Member	Oklahoma Gas and Electric	12/31/24
Justin Haar	Member	Minnkota Power Cooperative	12/31/23
Matthew Szyda	Member	Manitoba Hydro	12/31/23
Michael Meason	Member	Western Farmers Electric Cooperative	12/31/23
Norma Browne	Member	Ameren	12/31/24
Patrick Glunz	Member	Nebraska Public Power District	12/31/25
Peter Grandgeorge	Member	MidAmerican Energy Company	12/31/25
Rocky Tolentino	Member	Southwest Power Pool	12/31/25
Tim Anderson	Member	Dairyland Power Cooperative	12/31/24

Classification: **Public**

AGENDA

Call to Order and Determination of Quorum

b. Robert's Rules of Order
Ian Anderson, Security Advisory Council Chair

Parliamentary Procedures. Based on Robert's Rules of Order, Newly Revised, Tenth Edition

Establishing a Quorum. In order to make efficient use of time at MRO organizational group meetings, once a quorum is established, the meeting will continue, however, no votes will be taken unless a quorum is present at the time any vote is taken.

Motions. Unless noted otherwise, all procedures require a “second” to enable discussion.

When you want to	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and cannot reverse the intent of the main motion.
Reconsider a Motion already resolved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion. Second by anyone.
End debate	Call for the Question or End Debate	No	If the Chair senses that the committee is ready to vote, he may say “if there are no objections, we will now vote on the Motion.” Otherwise, this motion is not debatable and subject to majority approval.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.

Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively “kills” the motion. Useful for disposing of a badly chosen motion that cannot be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The “seconder” is not required to be recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee “owns” the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show “by unanimous consent.”
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member’s vote. Each member is called upon by the Secretary, and the member indicates either “Yes,” “No,” or “Present” if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a “Yes,” “No,” or “Present” is not shown are considered absent for the vote.

Classification: Public

MEETING AGENDA – Security Advisory Council – August 08, 2023

Notes on Voting.

Abstentions. When a member abstains, he/she is not voting on the Motion, and his/her abstention is not counted in determining the results of the vote. The Chair should not ask for a tally of those who abstained.

Determining the results. A simple majority of the votes cast is required to approve an organizational group recommendations or decision.

Unanimous Approval. Can only be determined by a Roll Call vote because the other methods do not determine whether every member attending the meeting was actually present when the vote was taken, or whether there were abstentions.

Electronic Votes – For an e-mail vote to pass, the requirement is a simple majority of the votes cast during the time-period of the vote as established by the Committee Chair.

Majorities. Per Robert's Rules, as well as MRO Policy and Procedure 3, a simple majority (one more than half) is required to pass motions

Classification: **Public**

AGENDA

Standards of Conduct and Antitrust Guidelines *Steen Fjalstad, Director of Security, MRO*

Standards of Conduct Reminder:

Standards of Conduct prohibit MRO staff, committee, subcommittee, and task force members from sharing non-public transmission sensitive information with anyone who is either an affiliate merchant or could be a conduit of information to an affiliate merchant.

Antitrust Reminder:

Participants in Midwest Reliability Organization meeting activities must refrain from the following when acting in their capacity as participants in Midwest Reliability Organization activities (i.e. meetings, conference calls, and informal discussions):

- Discussions involving pricing information; and
- Discussions of a participants marketing strategies; and
- Discussions regarding how customers and geographical areas are to be divided among competitors; and
- Discussions concerning the exclusion of competitors from markets; and
- Discussions concerning boycotting or group refusals to deal with competitors, vendors, or suppliers.

Classification: Public

AGENDA

Advisory Council Work Plans

- a. RAC
- b. CMEPAC

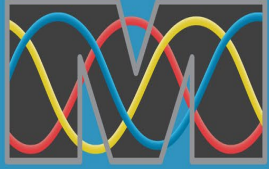
Action

Discussion

Report

Members from the RAC and CMEPAC will review their work plans during the meeting.

Classification: **Public**



MIDWEST
RELIABILITY
ORGANIZATION

2023 Reliability Advisory Council Work Plan

Bryan Clark, P.E.
Director of Reliability Analysis
August 8, 2023

CLARITY

ASSURANCE

RESULTS

#1 Conduct Outreach and Awareness

- Conduct a minimum of 2 webinars/outreach in 2023 to increase reliability and decrease risk to the reliable and secure operations of the bulk power system.



#2 Provide Reliability Standard Reviews

- Periodically attend NSRF meetings
 - *Energy Reliability Planning*
 - *Generation Unavailability During Extreme Cold Weather*



#3 Review Significant Events or Disturbances on the BES

- Review of an entity event at the Q3 Meeting
 - *Misoperations Due to Human Errors*
 - *Overhead Transmission Line Ratings*



#4 Development of the MRO Regional Risk Assessment

- Quarterly Risk Discussions
- Two resources provided from the RAC to support the Annual Risk Ranking exercise
 - *All MRO Reliability Risks*



#5 Support Regional Representation on NERC Organizational Groups

- Five different NERC groups with a representative
 - System Planning Impacts from Distributed Energy Resources Working Group (SPIDERWG)
 - Inverter Based Resource Performance Subcommittee (IRPS)
 - Energy Reliability Assessment Working Group (ERAWG)
 - Electric Gas Working Group (EGWG)
 - System Protection and Control Working Group (SPCWG)



#6 Review the Summary of Misoperations across the MRO Region

- Accomplished through the Protective Relay Subgroup (PRS)
 - *Misoperations Due to Human Errors*





Questions



MIDWEST
RELIABILITY
ORGANIZATION

Welcome from the CMEPAC

Terri Pyle, CMEPAC Chair

Tasha Ward, Director of Enforcement and External Affairs

Mark Flanary, Director of Risk Assessment and Mitigation

Bill Steiner, Director of Compliance Monitoring

Classification: **Public**

CLARITY

ASSURANCE

RESULTS

CMEP Advisory Council

Purpose

The MRO Compliance Monitoring and Enforcement Program Advisory Council (MRO CMEPAC) is an MRO Organizational Group that provides advice and counsel to MRO's Board of Directors (board), the board's Organizational Group Oversight Committee (OGOC), staff, members and registered entities on topics such as the development, retirement, and application of NERC Reliability Standards, risk assessment, compliance monitoring, and the enforcement of applicable standards. The MRO CMEPAC increases outreach and awareness in these key areas.



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

CMEPAC Outreach

- **MRO CMEP Conference (July 26, 2023)**
 - This year's theme: Understanding Risk for Reliability & Compliance
- **Other CMEPAC Outreach**
 - Monthly Calls
 - Newsletters
 - Webinars
- **Supports NERC Standards Review Forum (NSRF)**



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

CMEPAC Initiatives

1. Requirement Specific RFI – CIP-007 R2, FAC-008 R6
2. RRA and associated NERC Reliability Standards
3. Readiness Assessment – EOP-012-1 R2



CMEPAC Achievements

- **Held Hybrid MRO CMEP Conference (over 350 online/in-person attendees)**
- **Had kick off of requirement specific RFI initiative**
- **Held 7 monthly calls**
- **Held weekly NSRF calls**



AGENDA

MRO Regional Risk Assessment (RRA) Report

Mark Tiemeier, Principal Technical Advisor, MRO

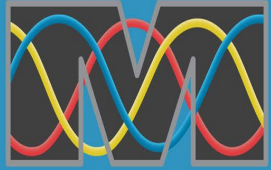
Action

Information

Report

Mark Tiemeier will provide an oral report during the meeting.

Classification: Public



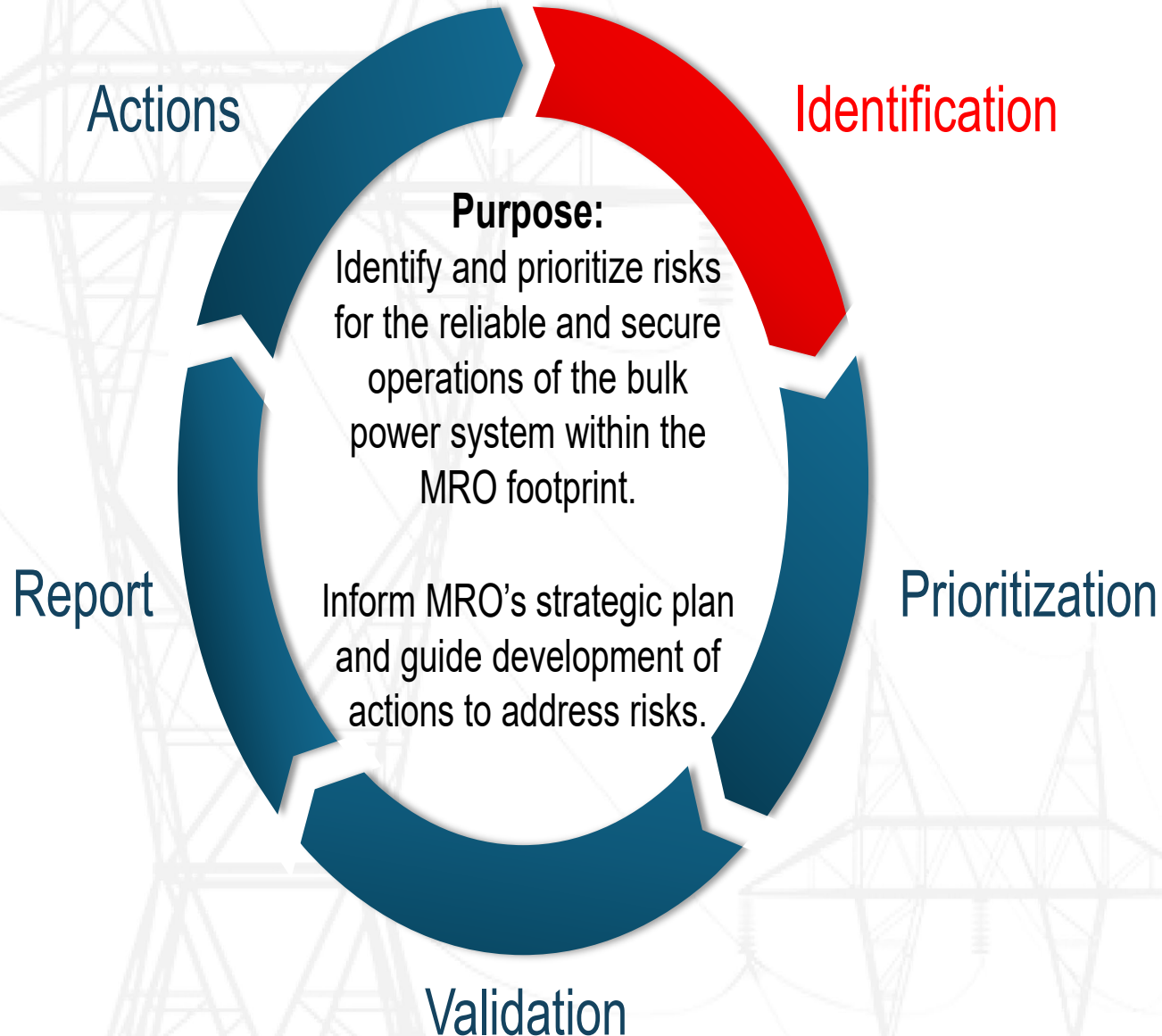
MIDWEST
RELIABILITY
ORGANIZATION

MRO 2024 Regional Risk Assessment

Mark Tiemeier

Principal Technical Advisor

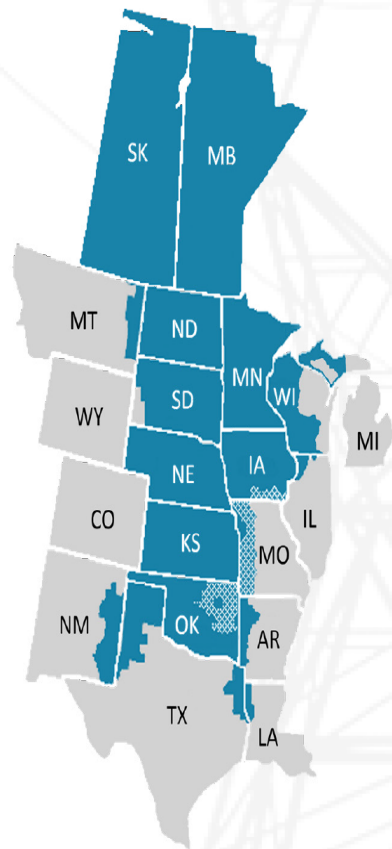
Regional Risk Assessment Process



MRO 2023 Regional Risk Assessment

Top risks to the reliable and secure operation of the North American bulk power system in MRO's regional footprint.

Territory



About Us

As part of the [ERO Enterprise](#), MRO is committed to a shared mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system in its regional footprint.

Read more at www.MRO.net

MRO Reliability Risk Matrix: Risk Rankings

Consequence / Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major				4,5,6,16	
C3	Moderate		2	9,12,13	1	
C2	Minor			3,7,8,10,14,17	15	
C1	Negligible			11		











Top risks are reflected in orange above and described below. A full list of risks assessed can be found in the final report.

Assessment Overview

- Extreme weather, consumer demand, and changes in technology and generation resources continue to present a rapidly increasing number of challenges to grid planners and operators. Physical and cyber security risks also continue to evolve at an unprecedented pace.
- MRO's annual *Regional Risk Assessment* considers continent-wide risks to reliability and security of the North American bulk power system and determines which are more likely to occur and would have a higher impact in MRO's region.
- This report is focused on risk identification, prioritization and mitigation and highlights for industry the priorities needed to collaboratively address these challenges. It also serves to inform key decision makers of challenges the industry faces and the policies and regulations that will help define a variety of proposed solutions.

READ MRO'S [2023 REGIONAL RISK ASSESSMENT](#)

Key Findings: Top Reliability and Security Risks in MRO's Territory

Model Assumptions	Planning Reserves	Energy Reliability	Generation Unavailability	Transmission Line Ratings	Insider Threats	Malware/Ransomware	Supply Chain Compromise
 <p>RISK 1. Assumptions used in bulk power models to plan and operate the grid have not accounted for the rapid increase in inverter-based and distributed energy resources, challenging industry's ability to accurately assess current and future system characteristics.</p>	 <p>RISK 4. Traditional methods to calculate Planning Reserve Margin are inadequate to properly plan for the generation capacity needed to meet increasingly uncertain system operations, especially during extreme weather events.</p>	 <p>RISK 5. Increased uncertainty from changing energy supply and customer demand challenge the grid's ability to meet load for all hours of the year. There is no comprehensive planning that assesses assurance of available energy and fuel sources over all time periods to maintain grid reliability.</p>	 <p>RISK 6. Generation availability assumed during cold weather, particularly in the southern U.S., has been shown to be unrealistically high due to a lack of generation winterization and natural gas curtailments.</p>	 <p>RISK 12. Use of constant overhead transmission line ratings year-round (non-seasonal) limits available transmission capacity and leads to inefficient real-time decisions when system conditions deviate from assumptions that drive rating calculations, such as cooler temperatures or during emergency operations.</p>	 <p>RISK 9. Employees or contractors using their knowledge and authorized access of critical systems to do harm to the bulk power system is a continued, substantial threat to organizations and the reliability of the grid.</p>	 <p>RISK 13. Phishing attacks can introduce malware or ransomware to corporate IT systems, which can impact critical systems necessary for reliable bulk power system operations through direct or in-direct connections those systems have to IT networks.</p>	 <p>RISK 16. A cyber security event carried out through the vendor supply chain can broadly impact bulk power system reliability, especially where the vendor is a market leader providing systems used for system operation.</p>

2024 RRA Risk Ranking Meetings

- **Risk Information Sessions**

- *Tuesday, 10/17 2-4:30pm (Ops/Planning risks)*
- *Wednesday, 10/18 2-4:30pm (Security risks)*
- Open to all council members

- **Risk Ranking Workshop**

- *Monday, 10/23 8:30am-3:30pm*
- Only council risk ranking volunteers



MRO 2024 RRA Risk Identification

- **MRO Regional Security Risk Assessment (RSRA) is an input to MRO's Regional Risk Assessment (RRA)**
- **Security risks from the RSRA with an impact to bulk power system reliability are included in the RRA**
 - Some risks from RSRA may be combined upon inclusion in the RRA

Mark Tiemeier, P.E.
**Principal Technical
Advisor**

mark.tiemeier@mro.net

651-855-1759



Questions

AGENDA

MRO Regional Security Risk Assessment (RSRA) Survey Update

Lee Felter, Principal Security Engineer, MRO

Action

Information

Report

Lee Felter will provide an oral report during the meeting.

Classification: **Public**



MIDWEST
RELIABILITY
ORGANIZATION

2023 Regional Security Risk Assessment

2023.07.12 Working Session Debrief

Lee Felter

Principal Security Engineer

Classification: **Public**

CLARITY

ASSURANCE

RESULTS

Ranking by Response Average

1 - Insider Threat	10.63
2 - Physical – Large equipment damage e.g. Transformers and Generators	8.46
3 - Supply chain compromise	8.08
4 - Coordinated attack over a large geographic area	7.74
5 - Initial access - Phishing	7.33
6 - Physical – Access controls (compromise to systems that would allow unauthorized access)	6.72
7 - Malware / Ransomware Attack on OT Systems	6.51
8 - Vulnerability/patch management	6.20
9 - Data dump exposing sensitive information	6.10
10 - Initial access – internet accessible devices	5.66
11 - Attack that corrupts backups integrity or makes backups unavailable	5.27
12 - Attack that Inhibits response functions e.g. – DDOS, System firmware, Manipulate I/O images (configuration files)	5.26
13 - Attack that Impairs process controls e.g. meter, relay, server	5.17
14 - Initial access – exploitation of remote services	5.16
15 - Malware / Ransomware Attack on IT Systems	4.67



Heatmap by Response Average

Risk			Likelihood				
			L1	L2	L3	L4	L5
			Very Unlikely	Unlikely	Possible	Likely	Almost Certain
Consequence	C5	Severe					
	C4	Major					
	C3	Moderate		3, 4, 6	1, 2		
	C2	Minor		7, 8, 9, 10, 11, 12, 13, 14, 15	5		
	C1	Negligible					
			Averages				



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

Heatmap by Organization Size

Risk			Likelihood				
			L1	L2	L3	L4	L5
			Very Unlikely	Unlikely	Possible	Likely	Almost Certain
Consequence	C5	Severe					
	C4	Major		L: 4 M: 4	L: 3 M: 1	L: 1	
	C3	Moderate		L: 13 M: 3, 7 S: 4, 7	L: 2, 6, 7 M: 2 S: 1, 2, 3		
	C2	Minor	S: 13	L: 10, 11 M: 8, 9, 10, 11, 12, 13, 14, 15 S: 6, 8, 9, 10, 11, 12, 14, 15	L: 8, 9, 12, 14, 15 M: 5, 6 S: 5	L: 5	
	C1	Negligible					

Organization Size: L (>3000), M (700 ... 3000), S (<700)



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

Take Aways

- **The surveyed ranking (from May - June) didn't change after the working session. There was broad acceptance of the top risks**
- **The perception of risk may vary depending on organization characteristics - we can approach mitigation activities with more granularity**
- **We will publish a report that rolls up the meeting notes - risk text, scenarios, mitigations**



Next Year

- The risk rankings help determine activities in the workplan
- Heatmaps - help facilitate discussions
- Expanded risk descriptions / scenarios - help drive common understanding for the survey
- Pull on the IT/OT dependency thread
- Collaborate with the SAC to determine if any emerging risks need to be surveyed
- Look for efficiencies in the process



Lee Felter, P.E.
Principal Security Engineer
Lee.Felter@mro.net
651.256.5170



Questions

AGENDA

Stakeholder Survey
Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: Public

MEETING AGENDA – Security Advisory Council – August 08, 2023

AGENDA

Security Advisory Council Threat Forum (SACTF Update)

a. Threat Call Statistics

Daniel Graham, MRO SAC and SACTF Member

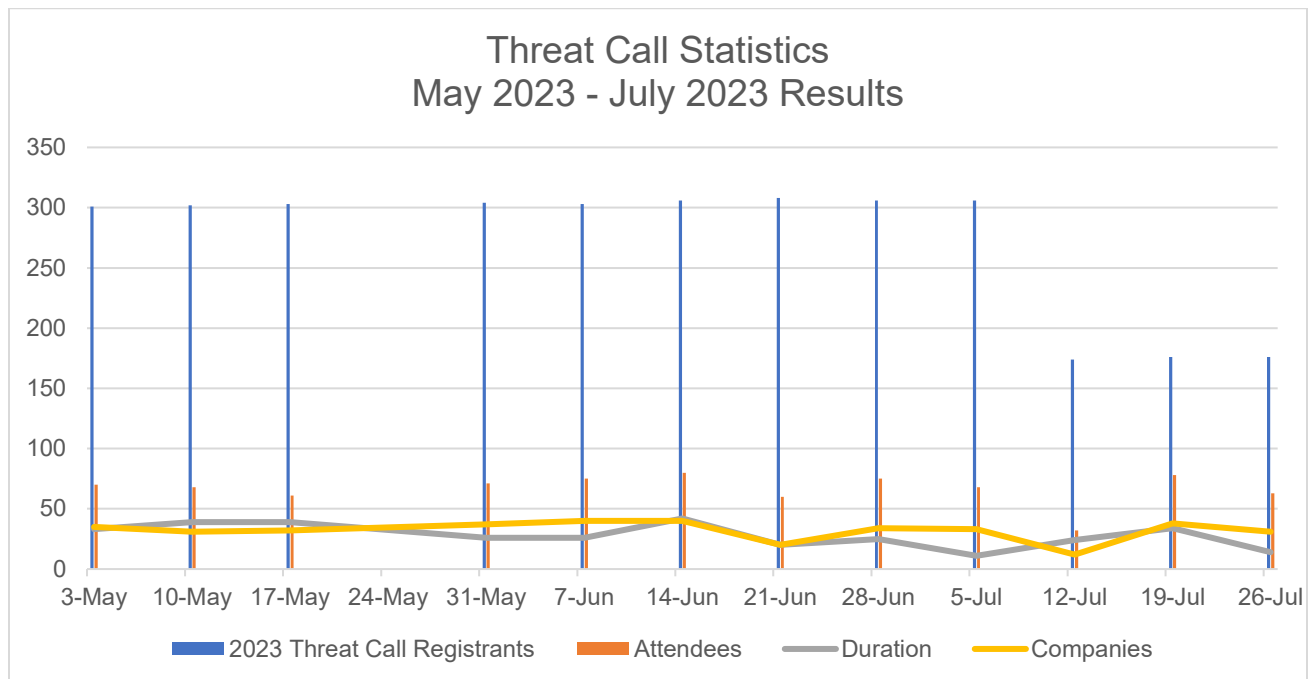
Action

Information

Report

Threat Call

Date	Approved Registrants	Duration	Attendees	Unique Companies
May 3, 2023	301	33 Minutes	70	35
May 10, 2023	302	39 Minutes	68	31
May 17, 2023	303	39 Minutes	61	32
May 31, 2023	304	26 Minutes	71	37
June 7, 2023	303	26 Minutes	75	40
June 14, 2023	306	42 Minutes	80	40
June 21, 2023	308	20 Minutes	60	20
June 28, 2023	306	25 Minutes	75	34
July 5, 2023	306	11 Minutes	68	33
July 12, 2023	174	24 Minutes	32	12
July 19, 2023	176	34 Minutes	78	38
July 26, 2023	176	14 Minutes	63	31
Averages	297	29 Minutes	68	3

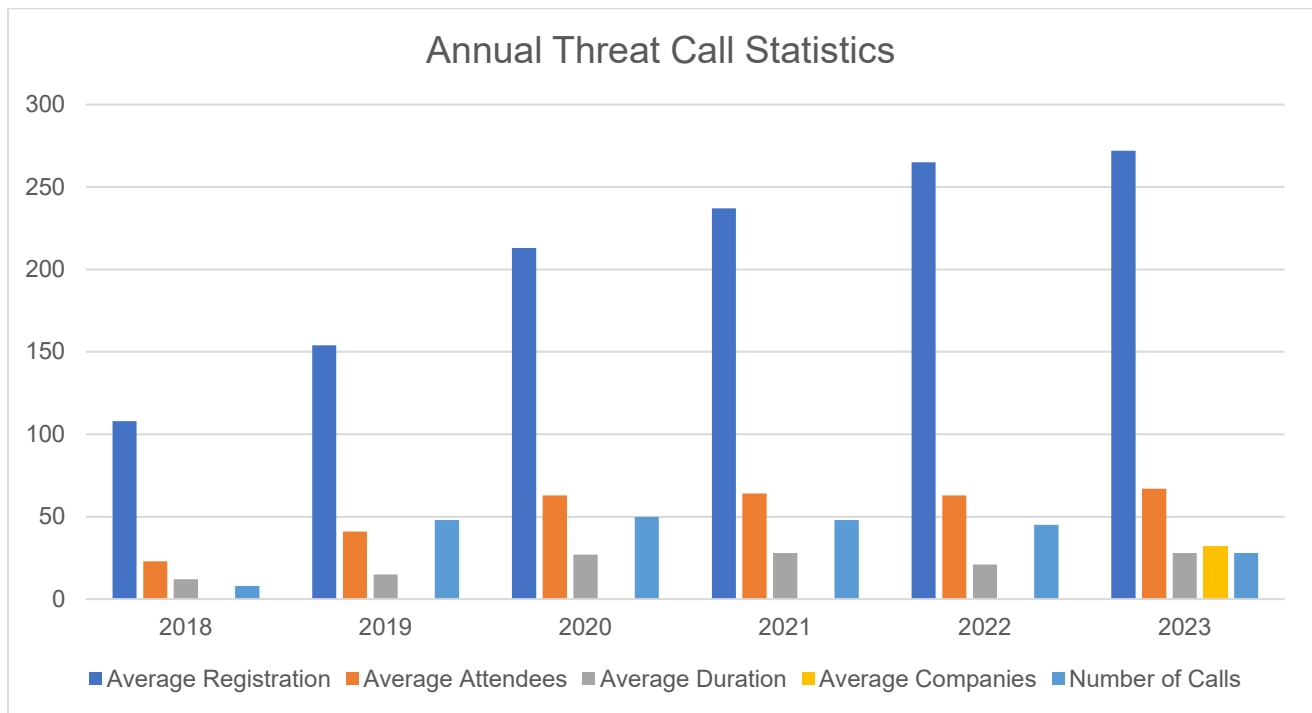


Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

Annual Threat Call Statistics

Year	Average Registrants	Average Attendees	Average Duration	Average Companies	Number of Calls
2018	108	23	12 Minutes		8 Calls
2019	154	41	15 Minutes		48 Calls
2020	213	63	27 Minutes		50 Calls
2021	237	64	28 Minutes		48 Calls
2022	265	63	21 Minutes		45 Calls
2023	272	67	28 Minutes	32	28 Calls



Classification: **Public**

AGENDA

Security Advisory Council Threat Forum (SACTF Update

b. Threat Call Feedback

Daniel Graham, MRO SAC and SACTF Member

Action

Discussion

Report

SAC and SACTF Member Daniel Graham will lead this discussion during the meeting.

Question A:

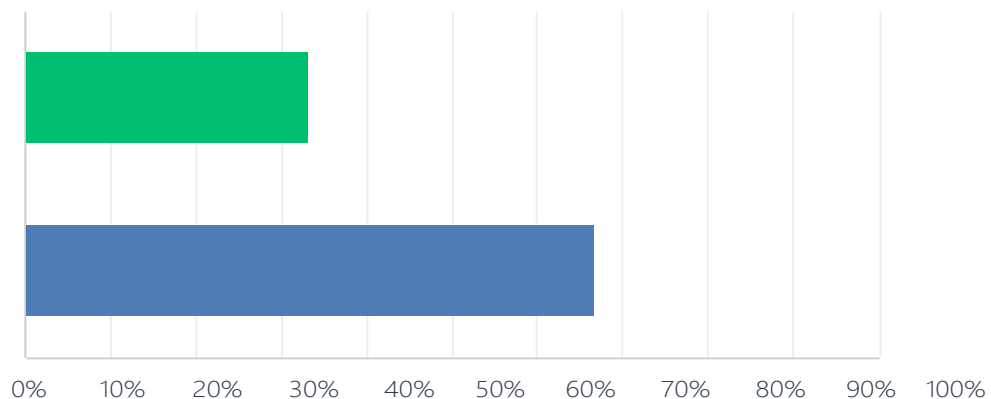
Q1 During the last 3-6 months, I have taken some sort of action in my company based on information received on the MRO SAC Threat Call?

Answered: 3

Skipped: 0

Yes

No

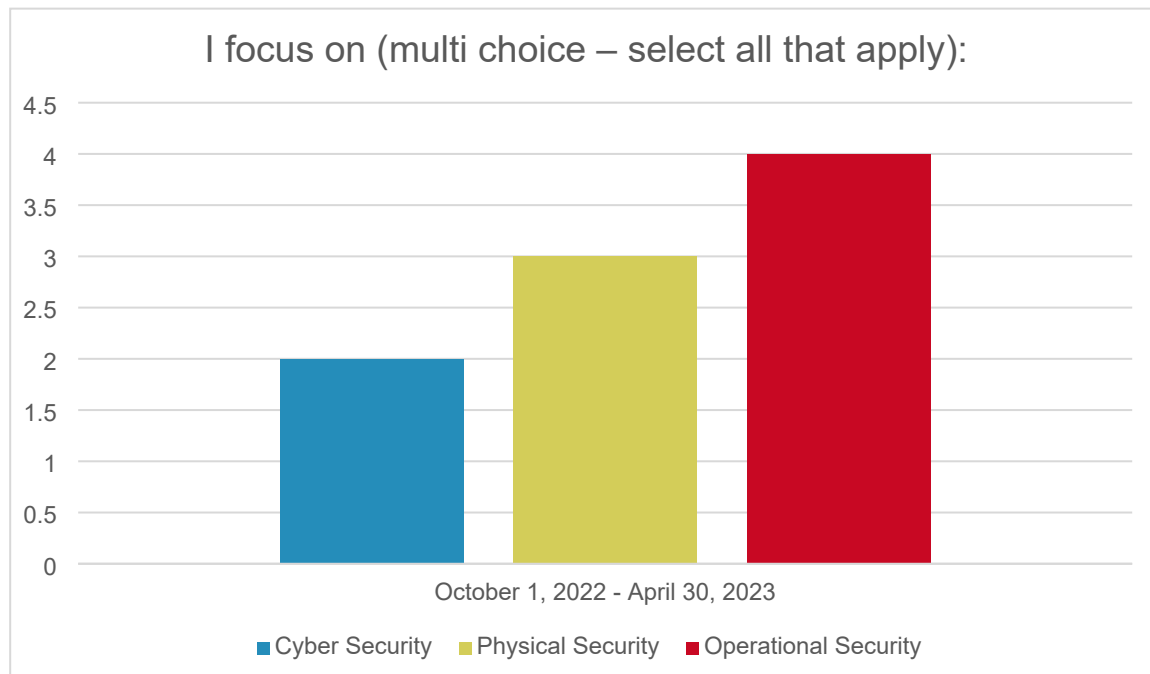


- Information shared during the Threat Call is shared with need-to-know staff.
- I am a new member. this is my 3rd meeting.

Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

Question B: No new responses since April 30, 2023.



- Information from the SACTF is shared with need-to-staff.
- Great meeting, lots of good discussion as always.

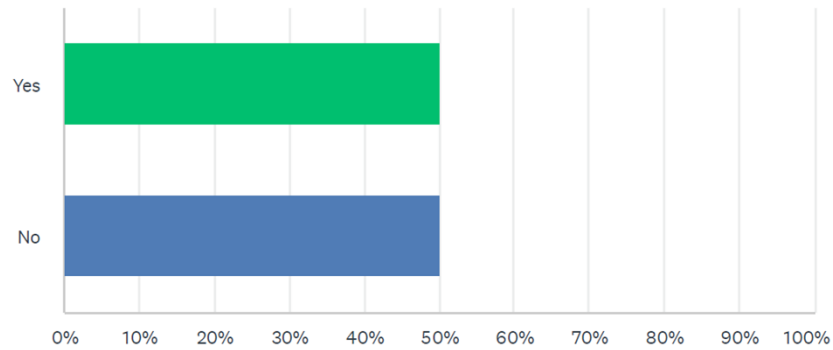
Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

Question C:

Q1 Me or my company have directly contributed to the conversation during the threat call in the last 3-6 months.

Answered: 2 Skipped: 0



- Weekly SACTF information is shared with need-to-know staff.
- Only my 2d meeting.

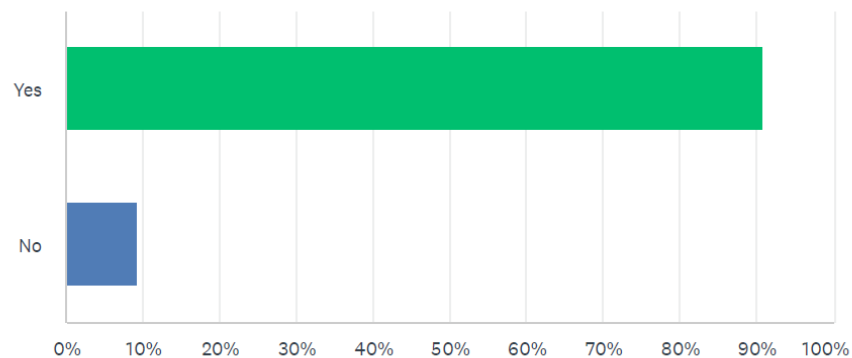
Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

Question D:

Q1 I have learned something new from the threat call in the last 3-6 months.

Answered: 11 Skipped: 0



- The forum seems to be open to anyone with discussion topics, it would be nice to have recurring speakers or topics to discuss.
- Thank you
- Information shared during the SACTF is shared with need-to-know staff.
- I enjoy the intel discussion every week.
- Great discussions as always. I often leave with something new to look into or consider to keep my org more secure.
- Information is shared with need-to-know staff.

Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

AGENDA

Security Advisory Council Threat Forum (SACTF) Update

c. Threat Forum Open Source Information Sharing

Daniel Graham, MRO SAC and SACTF Member

Action

Discussion

Report

SAC and SACTF Member Daniel Graham will lead this discussion during the meeting.

Classification: Public

AGENDA

MRO Representative on NERC Subgroups Written Reports

- a. NERC Supply Chain Working Group (SCWG)
Tony Eddleman, NERC SCWG Representative

Action

Information

Report

The SCWG reports to the NERC Reliability and Security Technical Committee (RSTC). SCWG meets monthly on the third Monday of each month at 12:00 p.m. (central time), except for the months of January, February, and June. Due to holidays in January and February, SCWG met on the second Monday of each month. The June 2023 meeting was rescheduled to June 26th due to the Juneteenth holiday.

1. Christopher Strain of Florida Power & Light Company (FPL) is the Chair of the SCWG and Dr. Thomas Duffey, ITegrity is the SCWG Vice Chair. Tom Hofstetter (NERC) is the Secretary. Stephanie Lawrence (NERC) is the Administrator. Christine Ericson (Illinois Commerce Commission) is the RSTC Sponsor.
2. SCWG is preparing four Security Guidelines for posting and public comments:
 - 1) **Vendor Identified Incident Response Measures**
 - a) Team Lead: Mike Prescher, Black & Veatch
 - b) The draft is complete as far as the development team is concerned and ready for posting for public comments.
 - 2) **Supply Chain Risks Related to Cloud Service Providers**
 - a) Team Lead: Matt Szyda, Manitoba Hydro
 - b) The current guideline will remain on the SCWG website until the SITES whitepaper is approved and posted, then it will be removed. SCWG team is developing a new guideline that will complement the new SITES whitepaper on cloud computing.
 - 3) **Procurement Language**
 - a) Team Lead: Shari Gribbin, CNK Solutions
 - b) The team distributed the updated guideline to SCWG prior to the June SCWG meeting for review.
 - 4) **Sourcing Issues with Supply Chain Procurements**
 - a) Team Lead: Tobias Whitney, Fortress Information Security
 - b) The team has met several times and the draft is close to being posted for public comments.
3. The RSTC assigned a Whitepaper on NERC Reliability Standards Gap Assessment to the SCWG. The team is forming now with some volunteers already identified. **If you have an**

Classification: Public

interest in this work, please contact Tom Hofstetter (tom.hofstetter@nerc.net) to join the team. The gap assessment will review the current Supply Chain requirements to determine what is already in the requirements versus what needs to be in the requirements. If there are gaps on Supply Chain security, a possible SAR will be developed to fix the gaps. A new Security Guideline may be used to cover the gaps in lieu of a SAR.

4. E-ISAC is planned to attend and provide a briefing at the next SCWG meeting on August 21st.

Areas of Focus

1. Maintain a roster of technical cyber and operations security experts.
2. Identify known supply chain risks and address through guidance documentation or other appropriate vehicles including input to NERC Alerts or the E-ISAC advisories.
3. Partner with National Laboratories to identify vulnerabilities in legacy equipment and develop mitigation practices.
4. Assist NERC staff by providing input and feedback associated with the development and execution of supply chain documents.
5. Coordinate with the North American Transmission Forum (NATF) and other industry groups as appropriate to ensure bulk power system (BPS) asset owner supply chain security requirements are clearly articulated.

Accomplishments

1. Continuing to review and post for comments Security Guidelines

Challenges

1. SCWG has multiple review teams working concurrently on Security Guidelines.
2. Monitoring and staying current on Supply Chain developments in the federal government and industry

Classification: Public

AGENDA

MRO Representative on NERC Subgroups – Written Reports

- b. NERC Security Integration and Technology Enablement Subcommittee (SITES)
Alan Kloster, NERC SITES Representative

Action

Discussion

Report

Classification: **Public**



MIDWEST
RELIABILITY
ORGANIZATION

NERC Security Integration and Technology Enablement Subcommittee (SITES) Update

Alan Kloster

Evergy, Inc.

Disclaimer

The Midwest Reliability Organization (MRO) Security Advisory Council (SAC)(or CMEPAC or RAC) 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 SAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation are presented by these MRO SAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

NERC SITES Updates

- The NERC SITES subcommittee has a quarterly meeting cadence with the last meeting held virtually on July 25, 2023.
- The NERC RSTC authorized publication of SITES Zero Trust Security for Electric OT white paper at their June meeting. It can be found on the RSTC Guidelines site [here](#).
- SITES is planning to update its membership roster in the near future and provided a new voting methodology for future meetings.
- Added a new white paper work plan item to be worked on now that the zero-trust paper is done. It will be focused on Risk-Based Physical and Cybersecurity Threats and Their Impacts to BPS Reliability and Resilience.



NERC SITES Zero Trust Security for Electric OT White Paper

- **The purpose of this white paper is to inform the electricity sector about zero trust (ZT) concepts and to provide considerations and recommendations regarding the adoption of ZT controls in operational technology (OT) and industrial control system (ICS) environments. It is currently slated to go before the RSTC in June for endorsement.**



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

NERC SITES Zero Trust Security for Electric OT White Paper (cont.)

- It expounds on the following topics:
 - A discussion of what Zero Trust means and gives the basic tenets of a zero-trust system
 - A discussion of the CISA Zero Trust Maturity Model
 - Using zero trust in an OT or ICS environment and how that is different from current models
 - Benefits, challenges and recommendations for using zero trust for OT/ICS
 - Compliance considerations
 - Zero trust controls guidance
 - Network segmentation, application layer deep packet inspection gateways and other security controls



NERC SITES Membership and Voting Update

- **The NERC SITES roster will be updated to include all members of the group. Currently it only includes SITES leadership and NERC facilitators.**
- **Formal membership will be granted to individuals who wish to actively participate in the decision-making process and engage in work efforts.**
 - Members can submit and vote on motions. Including nomination of future work items
 - Only formal members are eligible for SITES leadership
 - Observers will not be able to vote but can join any meeting and participate in discussions. They can ask to become members at any time.



NERC SITES Membership and

Voting Update (cont.)

- **A minimum quorum of 10 members must be present. Nay votes will be taken first to allow for objections to be raised and discussed appropriately. For a motion to pass, it must receive Aye votes from two-thirds of those present and non-abstaining members.**



AGENDA

NERC Reliability and Security Technical Committee (RSTC) Update *Marc Child, NERC RSTC Representative*

Action

Discussion

Report

The NERC Reliability and Security Technical Committee (RSTC) met in-person at the MRO offices on June 21-22 for their second quarter meeting. While the majority of the agenda topics were related to operations and planning, there were a few notable items of interest to the MRO SAC:

- RSTC SAR Development Process: The committee has drafted a formal process for management of SARs developed by their sub-groups. Absence of such guidance has resulted in some delays in the process during these first few years since RSTC was formed. The document, currently under committee review, will provide a structure that should speed the development, review, and endorsement of SARs prior to them being submitted to the NERC Standards Committee.
- Implementation Guidance: Usage of Cloud Solutions for BES Cyber System Information (BCSI) was endorsed by the RSTC and will be submitted to the ERO for formal review & acceptance. Note: This is the 3rd or 4th attempt at getting guidance passed, and this effort dates back to the CIPC committee. Industry needs this guidance and hopefully this iteration will be acceptable by the ERO.
- National Institute of Standards and Technology Cyber Security Framework to NERC CIP On-Line Information Resource Mapping. The security working group provided an update on this project. The SWG provided expertise to map the relevant CIP Reliability Standards to the NIST CSF v1.1. The OLIR mapping was recently published and is available for public review and comment.
- Whitepaper: Zero Trust – approved for posting
- White Paper: Security Risks Posed by DER and DER Aggregators – this is a white paper written by ERO staff and is being circulated among the RSTC members and trade organizations for comment.
- 2023 ERO Reliability Risk Priorities Report RSTC Strategic Plan and RSTC Work Plan Priorities – the RSTC is ramping up a tiger team to review the latest RISC report, assign tasks to subgroups, and update the RSTC Work Plan accordingly. This will result in new priorities for the three security working groups – Security Integration & Technology Enablement Subcommittee (SITES), the Security Working Group (SWG), and the Supply Chain Working Group (SCWG).
- Rich Hydzik from Avista (former Vice Chair) was elected RSTC Chair. John Stephens from City of Springfield was elected RSTC Vice Chair.

Update from March 2023 RSTC meeting:

- The package of information “BCSI in the Cloud Tabletop Exercise (Technical Reference)” that was approved by the RSTC in March has not yet been posted to the NERC website due to some technical difficulties. Those issues have been identified and addressed, and NERC will send out an announcement shortly with a link to the package.

AGENDA

2023 Security Conference Update

Cris Zimmerman, Manager of Outreach and Stakeholder Engagement, MRO

Action

Information

Report

Cris Zimmerman will provide a report during the meeting.

Classification: **Public**



MIDWEST
RELIABILITY
ORGANIZATION

MRO Q3 SAC Outreach Update

Cris Zimmerman

Manager, Outreach & Stakeholder Engagement

MRO Upcoming Events

- **Aug 29th Webinar IT/OT Convergence**
 - Doug Peterchuck, Director - Enterprise Operational Technology, OPPD
- **Sept 26-28 MRO Hybrid Security Conference**
 - Oklahoma City Sheraton Downtown Hotel



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

MRO Hybrid Security Conference

● Tuesday Sept 26th

- MRO Security Training Conference 11:00 am – 4:00 pm

Idaho National Labs (INL) ICS Cyber Escape Room Tuesday - Wednesday

Kelly Johnson, Chris Johnson – INL Network Discovery

Scot Donecker – Sunflower Electric Dragos Implementation lessons Learned

- Welcome Reception Social Hour 5:00 -7:00 pm – Sheraton Hotel
Bryson Bort, CEO Founder at SCYTHE – Purple Team Training
Researching Ice Breakers – Trivia, Picture Booth, etc



Classification: **Public**

CLARITY

ASSURANCE

RESULTS

MRO Hybrid Security Conference

● Wednesday Sept 27th

- MRO Security Hybrid Conference 8:00 am - 4:30 pm
Keynote Speaker , Rob M. Lee, CEO Co-Founder , Dragos

Sean Trauschke, Chairman, President CEO, OGE Energy Corp

Richard Burt, Senior VP Chief Operating Officer , MRO

Patrick Tatro- Army Ranger Threat Hunt Lead – Dark Knight Solutions

Ed Gray, Special Agent in Charge, FBI Oklahoma City Field Office

Sonia Garcia, Assistant Special Agent in Charge, FBI OKC Field Office

Casey Cox, Supv Special Agent, Counterintelligence, FBI OKC Field Office

Dr. Jennifer Hesterman, Colonel USAF (ret), Physical Security

Norma Browne, Corp Security Reliability Stds Compliance Mgr, Ameren

Classification: Public

CLARITY

ASSURANCE

RESULTS



MRO Hybrid Security Conference

● Thursday Sept 28th

SAC Threat Forum Security Briefing 8:00 am – 12:00 pm

In-person only, open to MRO members, regional entities, and approved guests. Invitations and details will go out separately; all attendees need to be approved

Currently have SITES Group confirmed for 1.5 – 2 hr. presentation

We have a conference room that holds 50 people

2 hour “Pens Down” Security Risk Round Table discussion.



Classification: **Public**

CLARITY

ASSURANCE

RESULTS



AGENDA

Cloud Computing and Data Storage Training or Webinar *Patrick Glunz, Security Advisory Council Member*

Action

Discussion

Report

SAC Member Patrick Glunz will lead this discussion during the meeting.

Classification: **Public**

MEETING AGENDA – Security Advisory Council – August 08, 2023

AGENDA

Charter Review

a. SAC Charter

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: Public



Security Advisory Council Charter

January 2023

I. Purpose

The MRO Security Advisory Council (SAC) is an MRO Organizational Group that provides advice and counsel to MRO's Board of Directors (board), the board's Organizational Group Oversight Committee (OGOC), staff, members and registered entities on cybersecurity, physical security, and control system security. The MRO SAC increases outreach and awareness in these key areas.

II. Membership

Pursuant to [Policy and Procedure 3 - Establishment, Responsibilities, and Procedures of Organizational Groups and MRO Sponsored Representative on NERC Organizational Groups](#), membership on councils is based on experience and expertise. No more than two members of the MRO SAC may be an employee of a single entity or affiliated entities. At least three sectors will be represented on the MRO SAC. To the extent practicable, membership will reflect geographic diversity and balanced sector representation. MRO staff will solicit volunteers from MRO members.

Individuals with expertise and experience in the areas of cybersecurity, physical security, and control system security serve on the MRO SAC.

The MRO SAC is comprised of 15 members. Nominations for open positions on the MRO SAC will be submitted to the MRO SAC for review. The MRO SAC, with input from MRO staff, will recommend the candidate(s) best suited for open position(s) based on experience, expertise, geographic, and sector representation diversity to the board's OGOC, which will appoint the members of the MRO SAC.

The MRO SAC will annually elect its chair and vice chair pursuant to the process and terms outlined in Policy and Procedure 3.

III. Key Objectives and Responsibilities

Key objectives and responsibilities of the MRO SAC include:

- Annually develop a work plan in coordination with MRO staff to support the MRO Strategic Plan and Metrics for approval by the OGOC and report performance progress.
- Serve as subject matter experts for MRO registered entities, members, other organizational groups, staff, as well as the board and its committees.
- Support the development of the annual MRO Regional Risk Assessment by identifying risks, trends, and mitigating activities.
- Recommend the establishment of subgroups to support the SAC work plan as appropriate. Oversee and provide direction to any subgroups.
- Maintain awareness of efforts by industry, NERC and other Regional Entity organizational groups to avoid or minimize duplicative efforts and to partner and coordinate where appropriate.
- Conduct outreach and awareness to increase security and decrease risk to the reliable and secure operations of the bulk power system:

Approved by the MRO OGOC 2021



- Strengthen relationship between MRO registered entities; E-ISAC, DHS, FBI, ICS-CERT, Fusion Centers and other similar agencies; trade associations and forums such as CEA, EPRI, EPSA, NATF, NAGF, NRECA, EEI, APPA and IEEE; and other U.S. or Canadian federal partners such as DOE, FERC and DoD, Public Safety Canada, RCMP, Canadian Cyber Incident Response Centre.
- Facilitate and lead the design of the Annual MRO SAC Conference(s) by identifying topics and speakers. Present at the workshop as appropriate.
- Support Midwest Reliability Matters by writing articles.
- Share best practices and other pertinent information via webinars.
- Create, consolidate and distribute highly relevant security information to region security contacts, primary compliance contacts, and others in the region as appropriate.
- Develop a Highly Effective Reliability Organization (HERO) outreach effort to help registered entities assess and improve their own security practices.
- Recommend individuals to represent MRO as representatives on NERC organizational groups to the OGOC.
- Provide guidance and communicate expectations to MRO NERC representatives, receive reports from MRO NERC representatives, and disseminate the information as directed by the board's OGOC.
- Support the applicable NERC program areas.
- Annually review the charter and propose changes as needed to the OGOC
- The SAC will provide strategic support and guidance to the SACTF, review the SACTF Work Plan and Charter, and collaborate in an effort to ensure cohesion and mitigate duplicate efforts with SAC

IV. Meetings

The MRO SAC will meet quarterly or as necessary, in person or via conference call and/or web meeting.

All MRO council chairs and vice chairs will meet with the OGOC the day before the fourth quarter regularly scheduled board meeting to review the council's accomplishments during the past year and to develop work plans for the following year.

Meetings of the MRO SAC are open to public attendance; however, the meeting may be called into closed session by the chair or vice chair. Additional meeting requirements related to agendas and minutes, voting and proxy, and rules of conduct are outlined in MRO Policy and Procedure 3.

V. Costs

Meeting costs incurred by MRO SAC members are reimbursable by MRO according to MRO Policy and Procedure 2 – Expense Reimbursement.

VI. Reporting Requirements

The chair or vice chair of the MRO SAC will provide an oral report to the OGOC regarding the council's work as well as any emerging issues during the annual scheduled in person meeting. During the other quarterly meetings, the chair or vice chair of the MRO SAC will provide a written report to the OGOC. The

Approved by the MRO OGOC 2021



chair or vice chair of the MRO SAC will provide a report to the OGOC during the fourth quarter meeting of the OGOC reviewing past accomplishments and highlighting work for the coming year.

Approved by the MRO OGOC 2021

AGENDA

Charter Review

a. SACTF Charter

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: Public



MRO Security Advisory Council Threat Forum Charter

January 1, 2023

I. Purpose

The MRO Security Advisory Council Threat Forum (SACTF) is an MRO organizational group that addresses regional risks by facilitating the sharing of threat information pertaining to cyber, physical, and operational security, arising from government or industry sources.

II. Membership

Pursuant to MRO's Policy and Procedure 3: Establishment, Responsibilities, and Procedures of Organizational Groups and MRO Representation on NERC Committees (MRO Policy and Procedure 3), the SACTF shall recommend members to the Security Advisory Council (SAC) based upon experience, expertise, and geographic diversity to the board's Organizational Group Oversight Committee (OGOC) for approval. There will be up to five SACTF members.

The SACTF will annually elect its chair and vice chair pursuant to the process and terms outlined in Policy and Procedure 3. The SACTF Chair or Vice Chair will be a SAC member.

III. Key Objectives/Activities

- Establish and support regional forums for the exchange, discussion, and collaboration on threat information.
- Identify and develop key contacts and sources from MRO members and government to leverage their security knowledge within the regional forums.
- Host a weekly threat call in accordance with the MRO SAC Threat Call Guidelines.
- Work in conjunction with MRO and the SAC to develop training on security threats to the industry.
- Support the efforts of the SAC to conduct outreach and awareness to increase security and decrease risk to the reliable and secure operations of the bulk power system as requested.

IV. Meetings

The SACTF will meet as necessary, typically via conference call or web meeting. Meetings of the SACTF are only open to individuals approved pursuant to the MRO SAC Threat Forum Guidelines. Additional meeting requirements related to the rules of conduct can be located in MRO Policy and Procedure 3. The chair, vice chair, or meeting secretary of the SACTF will compile meeting minutes, which include when a meeting took place, the duration of the meeting, the number of attendees, and a general overview of the meeting but no confidential security information. SACTF meetings are not recorded.

V. Reporting Requirements

The SACTF chair or vice chair will provide a written and/or oral report quarterly describing the activities and actions of the SACTF to the SAC. Annually, the SACTF shall perform a review of this charter and recommend any changes to the SAC for approval by the OGOC. The SACTF shall also perform an annual review of the SAC Threat Forum Call Guidelines and recommend any changes to the SAC for approval. The SACTF shall provide an annual summary report to the SAC for the SAC's fourth quarter meeting.

Approved by the MRO OGOC 2022

AGENDA

SAC Work Plan Update

- a. SAC Work Plan
- b. SACTF Work Plan

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: **Public**

AGENDA

Action Item Review

Margaret Eastman, Security Administrator

Action

Discussion

Report

Margaret Eastman will lead this discussion during the meeting.

Classification: **Public**

AGENDA

Other Business and Adjourn
Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: Public