Meeting Agenda

Security Advisory Council (SAC)

Monday, August 5, 2024
9:00 a.m. – 11:30 a.m. Central

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

MIDWEST RELIABILITY ORGANIZATION

380 St. Peter St, Suite 800
Saint Paul, MN 55102
651-855-1760
www.MRO.net

Public

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.

SECURITY ADVISORY COUNCIL (SAC) OPEN MEETING AGENDA

Agenda Item	
1	**Call to Order and Determination of Quorum** *Ian Anderson, SAC Chair*
2	**Standards of Conduct and Anti-trust Guidelines** *Steen Fjalstad, MRO Director of Security*
3	**Safety Briefing** *Shawn Keller, MRO Outreach Coordinator*
4	**Chair Remarks** *Ian Anderson, SAC Chair*
5	**MRO Staff Liaison Remarks** *Steen Fjalstad, MRO Director of Security*
6	**MRO Representatives on NERC Subgroups Written Reports** *Ian Anderson, SAC Chair*
Break – 10:00 a.m. – 10:15 a.m.	
7	**MRO SACTF Update** *Daniel Graham, Security Advisory Council Threat Forum Representative*
8	**RSRA Results: Focus Areas for 2024 and 2025** *Lee Felter, MRO Principal Security Engineer*
9	**SAC and SACTF Charter Review** *Ian Anderson, SAC Chair*
10	**SAC 2024 Work Plan Review** *Ian Anderson, SAC Chair*
11	**Action Item Review** *Margaret Eastman, MRO Security Administrator*
12	**Other Business and Adjourn** *Ian Anderson, SAC Chair*

Call to Order and Introductions

a. Determination of Quorum and Introductions - Roster

Ian Anderson, SAC Chair

Name	Role	Company	Term
OPEN	Member		12/31/26
OPEN	Member		12/31/24
Clayton Whitacre	Member	Great River Energy	12/31/25
Daniel Graham	Member	Basin Electric Power Cooperative	12/31/24
David Johnson	Member	OGE Energy Corp.	12/31/26
Douglas Peterchuck	Member	Omaha Public Power District	12/31/24
Ian Anderson	Chair	OGE Energy Corp.	12/31/25
Justin Haar	Member	Minnkota Power Cooperative	12/31/26
Kelly Crist	Member	Engie North America	12/31/26
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
Theresa Greene	Member	Great River Dam Authority	12/31/26
Tim Anderson	Member	Dairyland Power Cooperative	12/31/24

Call to Order and Introductions

b. Standards of Conduct and Anti-Trust Guidelines

Steen Fjalstad, MRO Director of Security

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.

Anti-trust 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.

Determination of Quorum

c. Robert's Rules of Order

Ian Anderson, SAC 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.

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
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.

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.

Safety Briefing

Shawn Keller, MRO Outreach Coordinator

Action

Information

Report

Shawn Keller, MRO Outreach Coordinator, will lead this agenda item.

Chair's Remarks

Ian Anderson, SAC Chair

Action

Information

Report

Chair Anderson will lead this discussion during the meeting.

MRO SAC Staff Liaison Remarks

Steen Fjalstad, MRO Director of Security

Action

Information

Report

Steen Fjalstad will provide an oral report during the meeting.

a. *Organizational Group Nominations (August 26 – September 6, survey link scheduled to be sent August 23)*
b. *HERO Award (nomination period September 18 – October 2)*
c. *OGOC Risk Round Table: Nation States – August 21*
d. *MRO Security Conference, GridSecCon*

MRO Representatives on NERC Subgroups – Written Reports

Tony Eddleman, NERC SCWG Representative
Marc Child, Evergy
Alan Kloster, NERC SITES Representative

Action

Information

Report

Representatives from NERC groups will provide oral and written reports.

MIDWEST RELIABILITY ORGANIZATION

NERC Supply Chain Working Group (SCWG) Update

Tony Eddleman, P.E.

Nebraska Public Power District

CLARITY | ASSURANCE | RESULTS

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.

SCWG Leadership

- Chair: Roy Adams, Consolidated Edison Company of New York
- Vice Chair - Dr. Thomas Duffey, ITegrity
- Secretary – Darrel Richardson (NERC)
- Administrator - Kelsi Boyd (NERC)
- RSTC Sponsor: Nathan Brown (GSOC)

SCWG meets monthly on the third Monday of each month at 12:00 p.m. (central time), except January, February, and June due to holidays

Supply Chain Security Gap Assessment and NERC 013-2 SAR Response (combined workstream)

SCWG was tasked to report back to the NERC Standards Committee through the NERC Reliability and Security Technical Committee (RSTC)

- **SCWG task team has been meeting since December 2023**
- **Small team of SCWG met with NERC RSTC Executive Committee on April 9, 2024 to discuss options**
- **Rich Hydzik, Chair NERC RSTC sent a letter to Todd Bennett, Chair NERC Standards Committee on May 7, 2024**

NERC RSTC Letter to NERC Standards Committee

- **In summary, the SCWG has identified three alternative options for addressing the reliability gaps in the CIP-013-2 SAR. Please note that these are not mutually exclusive:**
  - Create or update CMEP processes and practice guides to map to guidelines developed by NATF, EEI, EPRI, APPA, and RSTC SCWG.
  - Industry and the ERO can adopt practices consistent with the DHS/OMB/NIST Secure Software Development Framework to provide more consistency and clarity to suppliers through a digital supplier attestation process/format.
  - Enforcement practices should encourage entities to adopt a comprehensive SCRM/3rd Party risk plan.

NERC RSTC Letter to NERC Standards Committee

Lastly, should the Standards Committee elect to approve the SAR, the SCWG has offered the following

1. The standards drafting team should refer to guidelines developed by NATF, EEI, EPRI, APPA and RSTC SCWG as recommended language for standards enhancements.

Security Guidelines Status

- **Vendor Identified Incident Response Measures**
  - Team activity has been minimal
  - No update provided for recent meetings
- **Supply Chain Procurement Language**
  - Final revision was circulated for comments with review team in early June, but not discussed at either the June or July SCWG meeting


QUESTIONS

MIDWEST RELIABILITY ORGANIZATION

NERC Reliability & Security Technical Committee (RSTC) Update

Marc Child

Great River Energy

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.

NERC RSTC Roster

Chair – Rich Hydzik (Avista)

Vice Chair – John Stephens (City of Springfield)

Secretary – Stephen Crutchfield, NERC

Exec Sponsor – Mark Lauby, NERC

Executive Committee

Marc Child – Great River Energy

Robert Reinmuller – Hydro One

Christine Ericson – IL Commerce Commission

Todd Lucas – Southern Co

Sector Elected Members	
1. Investor-owned utility	Vinit Gupta (ITC) – 2024-2026 Greg Stone (Duke Energy) – 2023-2025
2. State/municipal utility	David Grubbs (City of Garland) – 2024-2026 Saul Rojas (NYPA) – 2023-2025
3. Cooperative utility	Nathan Brown (GSOC) – 2024-2026 Marc Child* (Great River Energy) – 2023-2025
4. Federal or provincial utility / Federal Power Marketing Administration	Robert Reinmuller* (Hydro One) – 2024-2026 Edison Elizeh (Bonneville Power) – 2023-2025
5. Transmission dependent utility	John Lemire (NCEMC) – 2024-2026 Nicola Parrotta (Taunton Municipal Light Plant) – 2023-2025
6. Merchant electricity generator	Brett Kruse (Calpine Corporation) – 2024-2026 Mark Spencer (LS Power) – 2023-2025
7. Electricity Marketer	Jodirah Green (ACES Power) – 2024-2026 Seat converted to At-large – 2023-2025
8. Large end-use electricity customer	Seat converted to At-large – 2024-2026 Seat converted to At-large – 2023-2025
9. Small end-use electricity customer	Seat converted to At-large – 2024-2026 Darryl Lawrence (PA Office of Consumer Advocate) – 2023-2025
10. Independent system operator/ Regional transmission organization	Ahmed Maria (Ontario IESO) – 2024-2026 Eric Miller (MISO) – 2023-2025
12. State Government	Seat converted to At-large – 2024-2026 Christine Ericson* (Illinois Commerce Commission) – 2023-2025

At-large Members	
Ian Grant**	Tennessee Valley Authority – 2023-2025
Marc-Antoine Roy	Hydro Quebec – 2023-2025
William Allen**	Exelon – 2023-2025
Thomas Burns	PacifiCorp – 2023-2025
David Jacobson	Manitoba Hydro – 2023-2025
Srinivas Kapagantula**	Arevon Energy – 2023-2025
Todd Lucas*	Southern Company – 2023-2025
Venona Greaff	Oxy – 2024-2026
Wayne Guttormson**	SaskPower – 2024-2026
Dede Subakti	California ISO – 2024-2026
David Mulcahy	Illuminate Power Analytics, LLC – 2024-2026
Stephen George	ISO New England– 2024-2026
Monica Jain	SCE – 2024-2026
Truong Le	Acciona – 2024-2026
Ryan Quint	Elevate Energy Consulting – 2024-2026

RSTC Security Priorities

- RSTC Work Plan Priorities (themes)
  - Energy Assurance
  - Inverter-based Resources
  - Distributed Energy Resources
  - Supply Chain Security

Update: Work plan summit Jan 21-23 2025

Background

The RSTC Was presented a list of high priority work plan items at eh March RSTC meeting. The RSTC EC approved the high priority wok plan items along with the RSTC Work Plan. The high priority work plan items are:

- White Paper: Energy Reliability Assessments Vol. 2
- Monitor Performance of Electric-Gas Interface during Extreme Events
- Generating Unit Winter Weather Readiness Webinar
- Monitor and Share Development of EV Charging Model
- SAR: Revisions to FAC-001 and FAC-002—IBR Performance
- Reliability Guideline: Recommended Approach to Interconnection Study of BPS-Connected IBRs
- Reliability Guideline: EMT Modeling and Simulations of IBR
- White Paper: Case Study on Adoption of EMT Modeling
- White Paper: Probabilistic Planning for the Tails
- Response to Cold Weather Recommendations:
  - Effects of Load-Shedding during Long-duration Events
  - Impacts of Transfer Limits
  - Improvements to Load Forecasting
    - Impacts of Forecasting Intermittent Generation
- Monitor and Support NERC Alerts for Supply Chain Issues

Meeting highlights – June 2024

- Location: Amazon “Mayday” Headquarters, Seattle, WA
  - NERC BOT Guest: Sue Kelly
  - Joint session with Standards Committee
  - AWS Utilities Summit following RSTC meeting
    - Navigating regulatory change
    - Dispelling myths about operations in the cloud
    - Customer sharing: cloud use cases (BCSI, OT DR, Smart meters)

Action Items - Security

- **Security Integration & Technology Enablement Subcmte (SITES)**
  - Chair Brian Burnett, Sponsor Marc Child
  - White Paper: New Technology Enablement and Field Testing
    - Supplier-centric work product
    - Broadly discussing the role of technology innovation and adoption in the regulated electric industry
    - Explores topics including ‘production testing’ of new technologies
    - Proposes changes to ERO processes *‘…to further enable the transparent exploration of new technology risks and benefits’*
  - Action: Request RSTC Comments
    - Discussion: RSTC members will need time to formulate comments
    - 60-day comment period pushes public comment period to follow December meeting

Progress Reports

- **Security Working Group (SWG)**

Workplan Status *(6-month look-ahead)*

Milestone	Status	Comments
CIP IG for Incorporating Synchrophasor Data into Real-time Operations		
Communication Protection System Guideline		
NIST 800-53 to NERC CIP Standards mapping		
CIP Evidence Request Tool		
Physical Security Guideline Re-write		

- **Security Integration & Technology Enablement (SITES)**

Workplan Status *(6-month look-ahead)*

Milestone	Status	Comments
Whitepaper: New Tech Enablement		Submitting for RSTC comments
Security Guideline for Inverter-Based Resources		Launching Soon
Security Guideline for Distributed Energy Resource Aggregators		Launching Soon
Physical Security Guideline (with SWG)		Launching Soon

- **Supply Chain Working Group (SCWG)**

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Revising two guidelines (Vendor Incident Response and Procurement Language)		In Progress
Gap Assessment for Supply Chain Security Standards encompassing: • NERC CIP-013-2 Standard • NERC CIP-013-2 SAR • Trades/Stakeholder Coordination • Supplier Coordination • Regulator Feedback • Industry Perspective Further evaluation of multiple proposed risk mitigation options and viability of individual or combined choices		In Progress

2024 & 2025 schedules

2024 RSTC Meeting Calendar			
Meeting Dates	**Time**	**Format**	**Location**
September 11, 2024 September 12, 2024	8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	Hybrid	Hotel Alt Montreal Montreal, Canada
December 11, 2024 December 12, 2024	11:00 a.m. – 4:30 p.m. 11:00 a.m. – 4:30 p.m.	Virtual	N/A

2025 RSTC Meeting Calendar (Tentative)			
Meeting Dates	**Time**	**Format**	**Location**
January 21, 2025 January 22, 2025 January 23, 2025	1:00-5:00 p.m. 8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	Work Plan Summit Hybrid	TBD
March 12, 2025 March 13, 2025	8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	In Person	TBD
June 11, 2025 June 12, 2025 June 12, 2025	8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m. 1:00-4:00 p.m. (Joint SC)	Hybrid	TBD
September 10, 2025 September 11, 2025	8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	Hybrid	TBD
December 10, 2025 December 11, 2025	11:00 a.m. – 4:30 p.m. 11:00 a.m. – 4:30 p.m.	Virtual	N/A

MIDWEST RELIABILITY ORGANIZATION

NERC SITES Update

Alan Kloster

Evergy

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.

NERC SITES Update

- **The NERC Security Innovation and Technology Enablement Subcommittee (SITES) had their quarterly meeting on July 23 2024.**
- **The meeting featured two presentations by GE Vernova**
  - One on AI and machine learning product Adaptive Grid Automation
  - The 2nd on GE's GridOS DERMS system.
- **SITES white paper on New Technology Enablement & Field Testing is awaiting RSTC comments requested at the last RSTC meeting. Likely to go to RSTC in Q4 2024.**

NERC SITES Update (cont.)

- SITES has recently kicked off the drafting of a Security Guideline for Inverter-Based Resources (IBR) Architecture
- SITES will be kicking off the drafting of a Security Guideline for Distributed Energy Resource Aggregators (DERA) in August

MRO NERC SITES Representative Report

Alan Kloster – Evergy

Action
No actions needed at this time.

Report
This report covers the quarterly NERC SITES committee meeting held virtually on July 23, 2024. Here was the agenda.

Agenda Items

1. Presentation on Artificial Intelligence / Machine Intelligence from GE Vernova – Achalesh Pandey, Digital Grid Product Executive a. 20 min + 10 min Q&A

2. Presentation on Distributed Energy Resource Aggregation from GE Vernova – Kushal Shah, Digital Grid Product Manager a. 20 min + 10 min Q&A

3. Administrative – Secretary Larry Collier, NERC

a. 2025 Schedule for SITES upcoming
b. Seeking technical presentations for 2025 for SITES Quarterly Meetings
c. Next quarterly meeting October 22, 2024 @ 12:00-2:00p.m. Eastern

4. Subteam Updates:

a. Whitepaper: New Technology Enablement & Field Testing – Thomas Peterson i. 2-month RSTC commenting period through end of August

b. Security Guideline for Distributed Energy Resource Aggregators (DERA) – Thomas Peterson i. Launched & Volunteer Accepting

c. Security Guideline for Inverter-Based Resources (IBR) Architecture – Mike Lamb i. Launched & Volunteer Accepting

d. Collaboration with Security Working Group (SWG): Physical Security Guideline – Larry Collier i. SWG has sufficient volunteers

5. Open Session

a. SLIDO Word Cloud - Topics of Interest for SITES in 2025

6. Future Meetings

2024 Meeting Schedule		
Date	Time	Location
July 23, 2024	12:00-2:00 p.m. Eastern	Virtual - Webex
October 22, 2024	12:00-2:00 p.m. Eastern	Virtual - Webex
January 21, 2025	12:00-2:00 p.m. Eastern	Virtual - Webex

1. Avnaesh Jayantilal from the GE Vernova gave a presentation on their Adaptive Grid Automation product that adds AI and machine learning capability to utility field control systems like ADMS, EMS, DERMs, etc. They have been using it with initial customers for grid operations decision support to help operators be more effective. GE is not introducing it into the direct control loop, but using it to help with state estimator and system strength analysis. They are also using it with LIDAR and satellite data feeds for planning analysis, wildfires and storm preparation. They are seeing a lot of success with the LIDAR/satellite use cases. GE is applying physic based guard rails to the AI to build the confidence of operators and engineers in the AI's capabilities. GE has also been using it for AI-based load and DER forecasting as well as real-time metering and forecasting grid inertia.

2. Keshal Shah from GE Vernova made a presentation on the GE GridOS DERMS (DER Management) product. He reviewed what DERs and DERMS are and talked about how DERs are managed with their product. A main focus of the presentation was some of the security challenges today and considerations for the future. GE has implemented zero trust in this product. He divided the issue into four security related tiers – local DER controls, feeder level integration, distribution operations integration, and wholesale integrated markets.

3. Updates were provided on SITES activities

    a. SITES *New Tech Enablement and Field Testing* white paper was provided to the June RSTC meeting for RSTC comment and/or endorsement. The RSTC gave their members two-months to comment on the paper. Because of the long comment period, it will likely not be presented back to the RSTC for approval until the Q4 RSTC meeting. The paper proposes a field trial process with the ERO and regions that would involve compliance waivers for testing new technology in BES Cyber Systems.
    b. Sites will start work on a Security Guideline for DER Aggregators with a team of 12 volunteers and a kick off meeting will be held in two weeks.
    c. SITES has also kicked of work on a new Security Guideline for IBR Architecture and that work will be ongoing through the rest of the year.
    d. Larry Collier, the NERC liaison announced that the Security Working Group had received enough volunteers to work on their Physical Security Guideline and SITES will no longer be collaborating on that with the SWG.

4. **Areas of Focus**
   a) Vendor presentations on new technology
   b) New Tech Enablement and Field Testing whitepaper
   c) New whitepapers as noted above

Accomplishments

1. New Tech Enablement and Field Testing whitepaper currently be reviewed and commented on by the NERC RSTC.

Challenges

1. None at this time.

Future Meetings – It was announced that 2025 meeting dates will be sent out soon.

2024 Meeting Schedule		
Date	Time	Location
July 23, 2024	12:00-2:00 p.m. Eastern	Virtual - Webex
October 22, 2024	12:00-2:00 p.m. Eastern	Virtual - Webex
January 21, 2025	12:00-2:00 p.m. Eastern	Virtual - Webex

MRO Security Advisory Council Threat Forum (SACTF) Update

Daniel Graham, SACTF Member

Action

Information

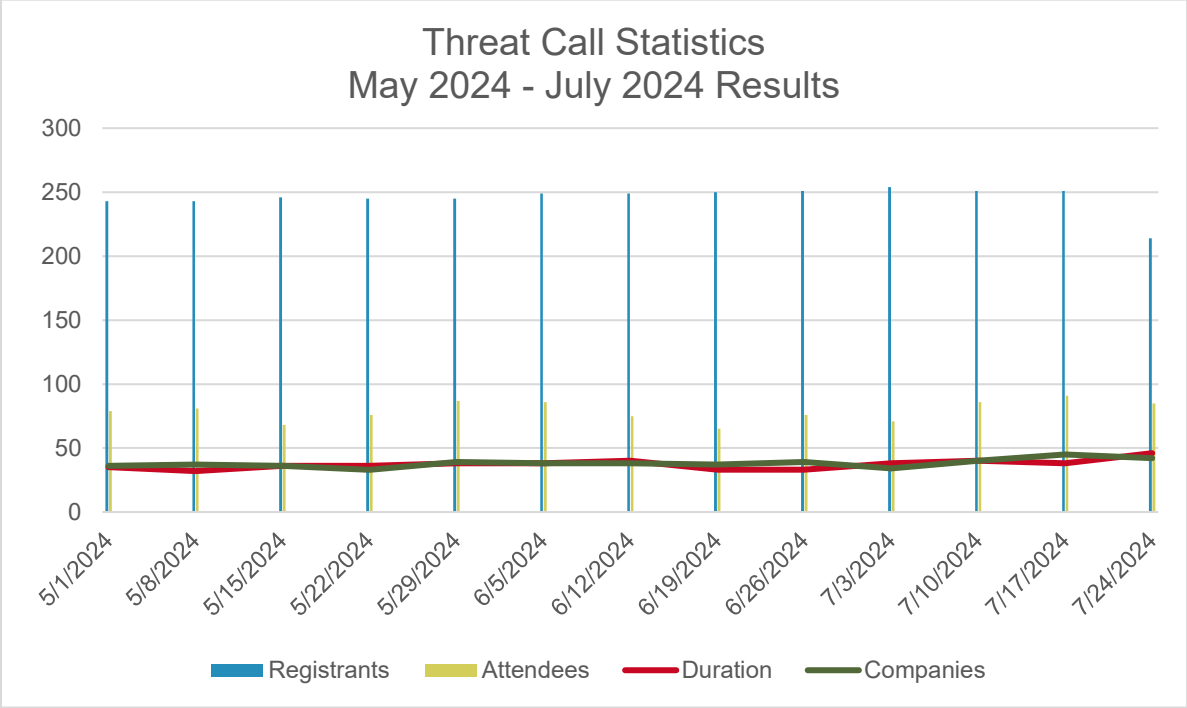
Report

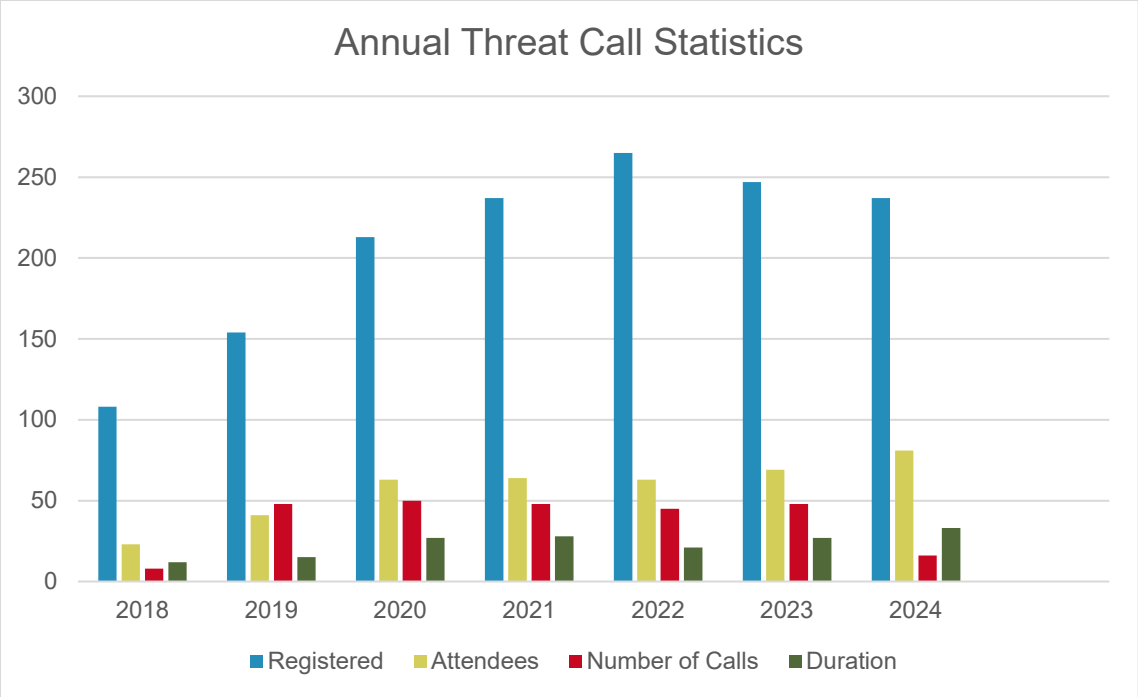
SACTF Member Daniel Graham will provide an update on the SACTF Threat Call.

a. *MRO SACTF Threat Call and Annual Statistics*
b. *MRO SACTF Threat Call Feedback*
c. *MRO SACTF Open Source Information Sharing Document*

Threat Call Statistics

Date	Approved Registrants	Duration	Attendees	Unique Companies
May 1, 2024	243	35	79	36
May 8, 2024	243	32	81	37
May 15, 2024	246	36	68	36
May 22, 2024	245	36	76	33
May 29, 2024	245	38	87	39
June 5, 2024	249	38	86	38
June 12, 2024	249	40	75	38
June 19, 2024	250	33	65	37
June 26, 2024	251	33	76	39
July 3, 2024	254	38	71	34
July 10, 2024	251	40	86	40
July 17, 2024	251	38	91	45
July 24, 2024	214	46	85	42
Averages	**245**	**37 Minutes**	**79**	**38**





Annual Threat Call Statistics

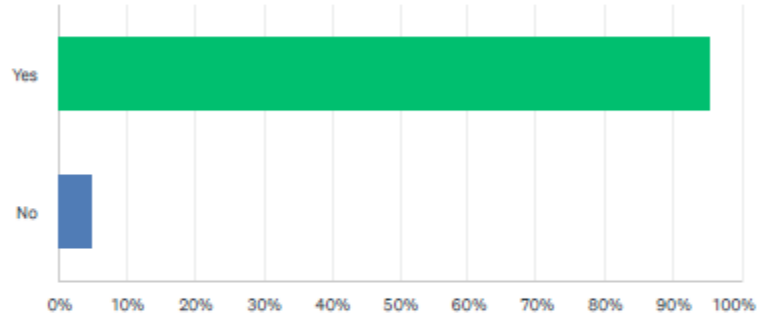
Year	Average Registrants	Average Attendees	Average Duration	Number of Calls
2018	108	23	12 Minutes	8 Calls
2019	154	41	15 Minutes	48 Calls
2020	213	63	27 Minutes	50 Calls
2021	237	64	28 Minutes	48 Calls
2022	265	63	21 Minutes	45 Calls
2023	247	69	27 Minutes	48 Calls
2024	237	81	34 Minutes	29 Calls

Threat Call Feedback

MRO SAC Threat Call (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: 21 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	95.24%	20
No	4.76%	1
TOTAL		21

Q2 Comments:

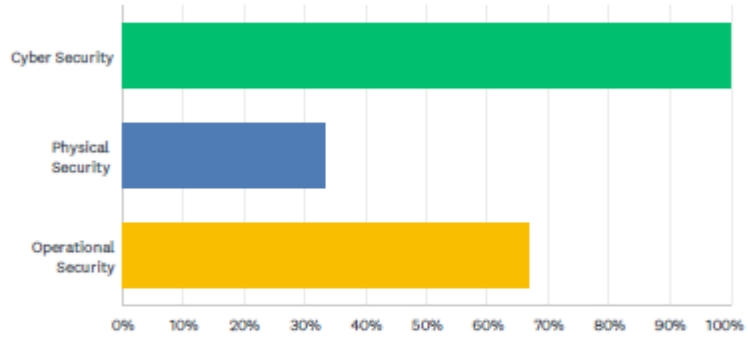
Answered: 9 Skipped: 12

#	RESPONSES	DATE
1	Information from the SACTF is shared with need-to-know staff.	7/3/2024 8:53 AM
2	Information from the SACTF is shared with need-to-know staff.	6/19/2024 8:50 AM
3	Thank you!	6/12/2024 9:12 AM
4	This is my first call.	6/12/2024 8:50 AM
5	Information from the SACTF is shared with need-to-know staff.	6/12/2024 8:50 AM
6	Information from the MRO SACTF is shared with need-to-know staff.	5/22/2024 8:48 AM
7	the discussion on AD traversal related to PRC LoTL is one example	5/8/2024 8:46 AM
8	Forwarding out the articles are helpful and timely.	5/8/2024 8:46 AM
9	No actual configuration changes, but I have taken information gained in this call and the PRC calls to the rest of the Company with great feed back, we are making plans to address.	5/1/2024 8:53 AM

MRO SAC Threat Call (Question B)

Q1 I focus on (multi choice – select all that apply):

Answered: 6 Skipped: 0



ANSWER CHOICES	RESPONSES	
Cyber Security	100.00%	6
Physical Security	33.33%	2
Operational Security	66.67%	4
Total Respondents: 6		

Q2 Comments:

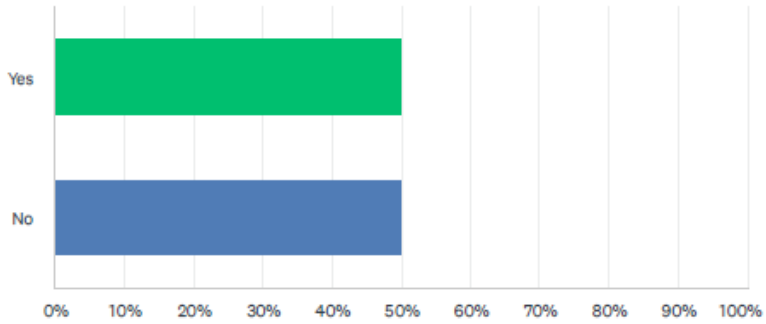
Answered: 0 Skipped: 6

#	RESPONSES	DATE
	There are no responses.	

MRO SAC Threat Call (Question C)

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

Answered: 4 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	50.00%	2
No	50.00%	2
TOTAL		4

Q2 Comments:

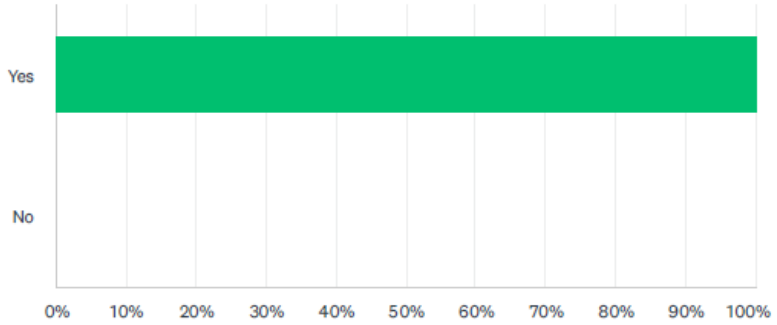
Answered: 1 Skipped: 3

#	RESPONSES	DATE
1	I am more on the learning side rather than the able to contribute side.	5/1/2024 8:51 AM

MRO SAC Threat Call (Question D)

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

Answered: 5 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	100.00%	5
No	0.00%	0
TOTAL		5

Q2 Comments:

Answered: 3 Skipped: 2

#	RESPONSES	DATE
1	Information from the SACTF is shared with need-to-know staff.	6/26/2024 8:48 AM
2	I really wish there was a note taker in the meeting that could then e-mail out a summary (or highlights) with links and resources to participants (especially if with the summer we have a lot more people taking PTO at different times).	6/5/2024 8:56 AM
3	Information from the SACTF is shared with need-to-know staff.	5/1/2024 8:49 AM

RSRA Results: Focus Areas for 2024 and 2025

Lee Felter, MRO Principal Security Engineer

Action

Information

Report

MRO Principal Security Engineer Lee Felter will lead this discussion during the meeting.

MIDWEST RELIABILITY ORGANIZATION

2024 Regional Security Risk Assessment

Survey Results

Survey

- **116↑ responses (59 in 2023)**
- **~23↑ minutes average (14 in 2023)**
- **Simplified survey**
  - Designed for input into the RRA
  - Went from 30 pages to ~4 significant
  - BPS impacts from an IT and OT perspective
- **Company characteristics**
- **Open responses**

2024 by size

Broad Risks	*avg*	*>3k (27 responses)*	*<3K >700 (40)*	*<700 (49)*
Cyber actors	5.73	Cyber actors	Cyber actors	Cyber actors
Supply Chain-delivery	5.10	Speed of transition	Supply Chain-delivery	Supply Chain-delivery
Physical actor	4.79	Workforce sufficiency	Physical actor	Policy/Laws/Regulation
Speed of transition	4.68	Supply Chain-delivery	Speed of transition	Physical actor
Policy/Laws/Regulation	4.38	Physical actor	Natural disaster	Workforce sufficiency
Workforce sufficiency	4.26	Policy/Laws/Regulation	Policy/Laws/Regulation	Speed of transition
Natural disaster	4.18	Security alignment	Security alignment	Natural disaster
Security alignment	3.58	Natural disaster	Workforce sufficiency	Security alignment
Compromises in IT - risk to BPS	*avg*			
Phishing / Ransomware	5.54	Phishing / Ransomware	Phishing / Ransomware	Phishing / Ransomware
Phishing / Malware	5.48	Phishing / Malware	Phishing / Malware	Phishing / Malware
Nation State Adversaries	4.77	Nation State Adversaries	Nation State Adversaries	Unpatched vulnerabilities
Supply Chain Compromise	4.74	Supply Chain Compromise	Supply Chain Compromise	Supply Chain Compromise
Unpatched vulnerabilities	4.64	Unpatched vulnerabilities	Malicious Insider Threat	Data Dump
Malicious Insider Threat	4.25	Malicious Insider Threat	Unpatched vulnerabilities	Nation State Adversaries
Data Dump	3.99	Data Dump	Data Dump	Malicious Insider Threat
Cloud Migration	3.09	Cloud Migration	Cloud Migration	Cloud Migration
Compromises in OT - risk to BPS	*avg*			
Malicious Insider Threat	7.72	Malicious Insider Threat	Nation State Adversaries	Phishing / Ransomware
Unpatched vulnerabilities	7.71	Unpatched vulnerabilities	Malicious Insider Threat	Phishing / Malware
Nation State Adversaries	7.69	Physical Attack	Supply Chain Compromise	Unpatched vulnerabilities
Supply Chain Compromise	7.66	Supply Chain Compromise	Phishing / Ransomware	Supply Chain Compromise
Phishing / Ransomware	7.60	Nation State Adversaries	Unpatched vulnerabilities	Physical Attack
Phishing / Malware	7.26	Inadequate Physical Controls	Phishing / Malware	Malicious Insider Threat
Physical Attack	7.08	Coordinated Cyber Physical Attack	Coordinated Cyber Physical Attac	Nation State Adversaries
Coordinated Cyber Physical Attack	6.45	Phishing / Ransomware	Physical Attack	Data Dump
Inadequate Physical Controls	6.09	Phishing / Malware	Internet Connected Devices	Inadequate Physical Controls
Internet Connected Devices	5.72	Data Dump	Inadequate Physical Controls	Internet Connected Devices
Data Dump	5.65	Internet Connected Devices	Data Dump	Coordinated Cyber Physical Attack
Cloud Migration	3.54	Cloud Migration	Cloud Migration	Cloud Migration

2023

Insider Threat
Large Equipmemnt
Supply Chain
Coordinated Attack
Phisihing
Physical Access Controls
Malware/Ransomware OT
Vulnerability/Patch Mgmt
Data Dump
Internet Acecssible Devices
Backups
Inhibited Response Function
Impaired Process Controls
Remote Services
Malware/Ransomware IT

2024 by function

Broad Risks	*avg*	*G&T (62 responses)*	*G only (24)*	*T only (20)*
Cyber actors	5.73	Cyber actors	Cyber actors	Supply Chain-delivery
Supply Chain-delivery	5.10	Speed of transition	Physical actor	Cyber actors
Physical actor	4.79	Supply Chain-delivery	Policy/Laws/Regulation	Physical actor
Speed of transition	4.68	Policy/Laws/Regulation	Supply Chain-delivery	Speed of transition
Policy/Laws/Regulation	4.38	Physical actor	Workforce sufficiency	Policy/Laws/Regulation
Workforce sufficiency	4.26	Natural disaster	Speed of transition	Workforce sufficiency
Natural disaster	4.18	Workforce sufficiency	Security alignment	Natural disaster
Security alignment	3.58	Security alignment	Natural disaster	Security alignment
Compromises in IT - risk to BPS	*avg*			
Phishing / Ransomware	5.54	Phishing / Malware	Phishing / Ransomware	Supply Chain Compromise
Phishing / Malware	5.48	Phishing / Ransomware	Phishing / Malware	Cloud Migration
Nation State Adversaries	4.77	Nation State Adversaries	Unpatched vulnerabilities	Data Dump
Supply Chain Compromise	4.74	Supply Chain Compromise	Data Dump	Nation State Adversaries
Unpatched vulnerabilities	4.64	Unpatched vulnerabilities	Malicious Insider Threat	Phishing / Malware
Malicious Insider Threat	4.25	Malicious Insider Threat	Nation State Adversaries	Phishing / Ransomware
Data Dump	3.99	Data Dump	Supply Chain Compromise	Unpatched vulnerabilities
Cloud Migration	3.09	Cloud Migration	Cloud Migration	Malicious Insider Threat
Compromises in OT - risk to BPS	*avg*			
Malicious Insider Threat	7.72	Nation State Adversaries	Unpatched vulnerabilities	Malicious Insider Threat
Unpatched vulnerabilities	7.71	Supply Chain Compromise	Phishing / Ransomware	Physical Attack
Nation State Adversaries	7.69	Malicious Insider Threat	Malicious Insider Threat	Phishing / Ransomware
Supply Chain Compromise	7.66	Unpatched vulnerabilities	Nation State Adversaries	Supply Chain Compromise
Phishing / Ransomware	7.60	Phishing / Ransomware	Phishing / Malware	Phishing / Malware
Phishing / Malware	7.26	Phishing / Malware	Coordinated Cyber Physical Attack	Unpatched vulnerabilities
Physical Attack	7.08	Physical Attack	Inadequate Physical Controls	Data Dump
Coordinated Cyber Physical Attack	6.45	Coordinated Cyber Physical Attac	Physical Attack	Internet Connected Devices
Inadequate Physical Controls	6.09	Inadequate Physical Controls	Supply Chain Compromise	Inadequate Physical Controls
Internet Connected Devices	5.72	Internet Connected Devices	Data Dump	Nation State Adversaries
Data Dump	5.65	Data Dump	Internet Connected Devices	Cloud Migration
Cloud Migration	3.54	Cloud Migration	Cloud Migration	Coordinated Cyber Physical Attack

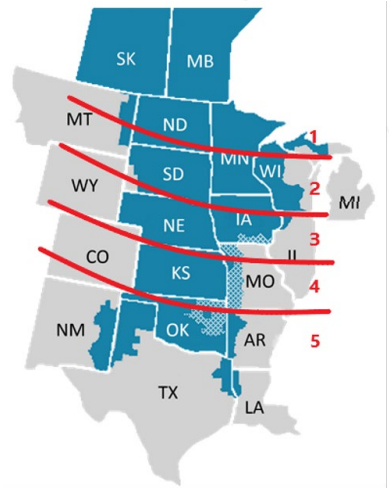
2023

Insider Threat
Large Equipmemnt
Supply Chain
Coordinated Attack
Phisihing

Physical Access Controls
Malware/Ransomware OT
Vulnerability/Patch Mgmt
Data Dump
Internet Acecssible Devices

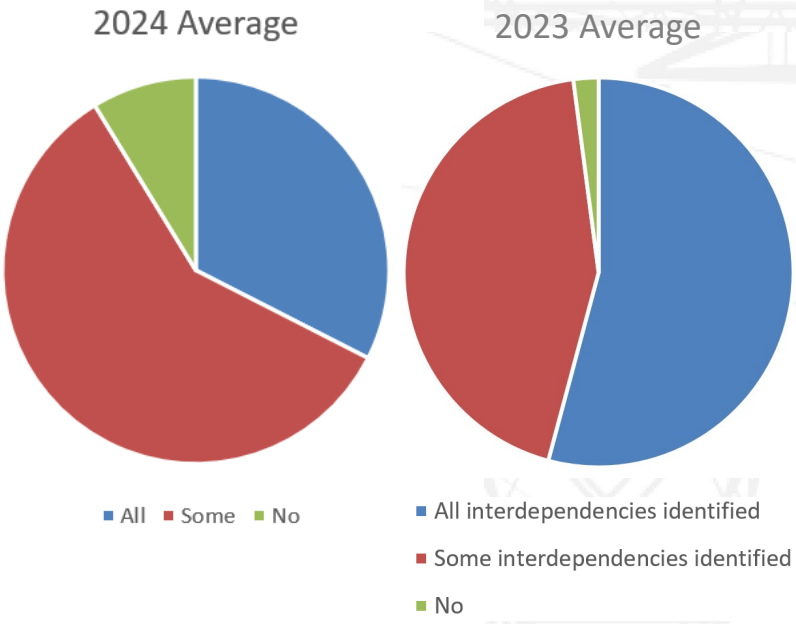
Backups
Inhibited Response Function
Impaired Process Controls
Remote Services
Malware/Ransomware IT

2024 latitudinal

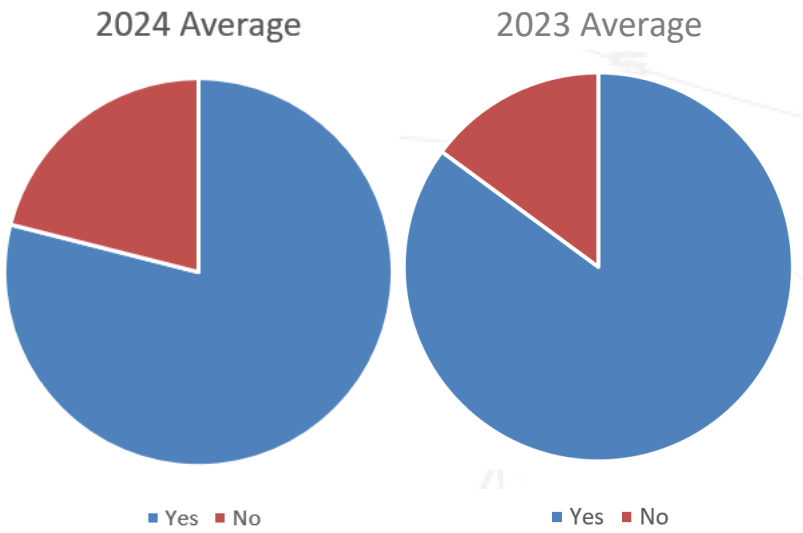


Broad Risks	avg	1-2 (21 responses)	3 (30)	4-5 (15)
Cyber actors	5.73	Cyber actors	Cyber actors	Cyber actors
Supply Chain-delivery	5.10	Supply Chain-delivery	Supply Chain-delivery	Physical actor
Physical actor	4.79	Physical actor	Physical actor	Supply Chain-delivery
Speed of transition	4.68	Speed of transition	Natural disaster	Policy/Laws/Regulation
Policy/Laws/Regulation	4.38	Policy/Laws/Regulation	Speed of transition	Natural disaster
Workforce sufficiency	4.26	Natural disaster	Policy/Laws/Regulation	Speed of transition
Natural disaster	4.18	Workforce sufficiency	Security alignment	Workforce sufficiency
Security alignment	3.58	Security alignment	Workforce sufficiency	Security alignment
Compromises in IT - risk to BPS	**avg**			
Phishing / Ransomware	5.54	Phishing / Malware	Phishing / Ransomware	Phishing / Ransomware
Phishing / Malware	5.48	Phishing / Ransomware	Phishing / Malware	Phishing / Malware
Nation State Adversaries	4.77	Malicious Insider Threat	Supply Chain Compromise	Unpatched vulnerabilities
Supply Chain Compromise	4.74	Unpatched vulnerabilities	Unpatched vulnerabilities	Data Dump
Unpatched vulnerabilities	4.64	Nation State Adversaries	Data Dump	Malicious Insider Threat
Malicious Insider Threat	4.25	Supply Chain Compromise	Nation State Adversaries	Supply Chain Compromise
Data Dump	3.99	Data Dump	Malicious Insider Threat	Nation State Adversaries
Cloud Migration	3.09	Cloud Migration	Cloud Migration	Cloud Migration
Compromises in OT - risk to BPS	**avg**			
Malicious Insider Threat	7.72	Malicious Insider Threat	Nation State Adversaries	Malicious Insider Threat
Unpatched vulnerabilities	7.71	Supply Chain Compromise	Supply Chain Compromise	Coordinated Cyber Physical Attack
Nation State Adversaries	7.69	Nation State Adversaries	Phishing / Ransomware	Nation State Adversaries
Supply Chain Compromise	7.66	Coordinated Cyber Physical Attack	Unpatched vulnerabilities	Physical Attack
Phishing / Ransomware	7.60	Unpatched vulnerabilities	Phishing / Malware	Phishing / Ransomware
Phishing / Malware	7.26	Physical Attack	Malicious Insider Threat	Inadequate Physical Controls
Physical Attack	7.08	Internet Connected Devices	Coordinated Cyber Physical Attack	Phishing / Malware
Coordinated Cyber Physical Attack	6.45	Phishing / Ransomware	Physical Attack	Unpatched vulnerabilities
Inadequate Physical Controls	6.09	Phishing / Malware	Internet Connected Devices	Data Dump
Internet Connected Devices	5.72	Inadequate Physical Controls	Data Dump	Supply Chain Compromise
Data Dump	5.65	Data Dump	Inadequate Physical Controls	Internet Connected Devices
Cloud Migration	3.54	Cloud Migration	Cloud Migration	Cloud Migration

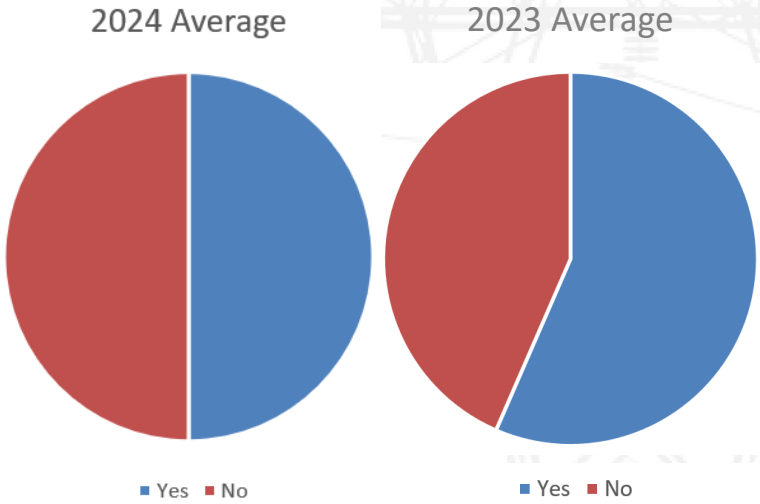
IT/OT Dependency



IT/OT Isolation Testing

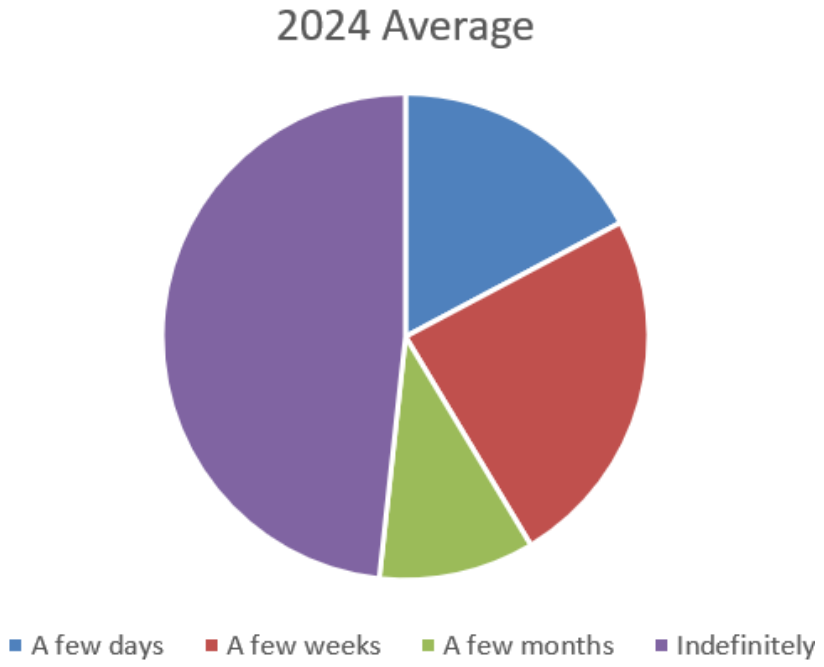


Could IT Impact OT?



78 responses

If yes, how long can you continue operations?



What keeps us up at night?

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

Questions

SAC and SACTF Charter Review

Ian Anderson, SAC Chair

Action

Information

Report

Security Advisory Council Chair Ian Anderson will lead this discussion during the meeting.

a. *SAC Charter*
b. *SACTF Charter*
c. *SACTF Threat Call Guidelines*

MIDWEST RELIABILITY ORGANIZATION

380 St. Peter St, Suite 800
Saint Paul, MN 55102
www.MRO.net
651-855-1760

Security Advisory Council Charter

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.

Field Code Changed

Field Code Changed

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:

  - 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

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.

MIDWEST RELIABILITY ORGANIZATION

380 St. Peter St, Suite 800
Saint Paul, MN 55102
www.MRO.net
651-855-1760

MRO Security Advisory Council Threat Forum Charter

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.

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 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 SATCF 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 May 22, 2024

SAC 2024 Work Plan

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Anderson will lead this discussion during the meeting.

Action Item Review

Margaret Eastman, MRO Security Administrator

Action

Discussion

Report

Margaret Eastman, MRO Security Administrator, will review the action items captured during the meeting.

Other Business and Adjourn

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Anderson will lead this discussion during the meeting.