



## **Minutes of the MRO Security Advisory Council Meeting**

*MRO Offices, 380 St. Peter Street, Suite 800, Saint Paul, MN 55102*

*Thursday, March 15, 2018*

### **1. Call to Order**

MRO Security Advisory Council (SAC) Outgoing Chair Mike Kraft called the meeting to order at 8:30 a.m. He extended a warm welcome to meeting attendees.

- a. *Determination of Quorum*. The meeting secretary, Cynthia Kneisl, MRO Standards, Certification and Registration Administrator, determined that a quorum was present. A complete list of attendees is included as Exhibit A.
- b. *Standards of Conduct, and Anti-Trust Guidelines*. Pursuant to Policy and Procedure 4, MRO's Standards of Conduct, Conflict of Interest and Anti-Trust Guidelines were presented to attendees by Kraft.
- c. *Additions to the Agenda*. Outgoing Chair Kraft asked attendees if there were any additional topics to add to the agenda. Council members proposed no additions to the agenda.

*Upon a motion duly made and seconded, the MRO SAC unanimously approved the agenda as written.*

### **2. Consent Agenda**

*Review and approve Minutes from December 6, 2017, MRO Security Advisory Council Meeting*. Outgoing Chair Kraft discussed that the December meeting was closed due to the fact TLP Amber details were discussed. The TLP Amber details were removed from the minutes. The closed meeting minutes were shared even though the SAC is not obligated to share minutes from a closed meeting.

*Upon a motion duly made and seconded, the MRO SAC unanimously approved the minutes from the December 6, 2017, MRO SAC Meeting, as written.*

### **3. Election**

- a. *MRO SAC Chair-Elect: John Hochevar*

Kraft explained the electronic election process and announced the MRO SAC members' selection of John Hochevar to serve as 2018 MRO SAC Chair.

- b. *MRO SAC Vice Chair-Elect: Jodi Jensen*

In addition to the selection of Chair Hochevar, the MRO SAC members selected Jodi Jensen to serve as 2018 MRO SAC Vice Chair.

Both Chair Hochevar and Vice Chair Jensen expressed thanks for the opportunity to serve.

### **4. Staff Report**

- a. *Review of MRO Organizational Groups and Current Initiatives*. Steen Fjalstad, MRO Security and Mitigation Principal, talked about the NERC ORS/CIPC task team producing guidance for



380 St. Peter Street, Ste. 800, Saint Paul, MN 55102      MidwestReliability.org      P.651.855.1760      F.651.855.1712

control center operators in the case of an event like the Ukrainian event occurred and encouraged everyone to be a resource for that. The name of this document is *Reliability Guideline for Operator Recognition Cyber Intrusion into Operating System*.

- b. Roster Review - MRO SAC and CIPC Representatives. Fjalstad informed members that two MRO NERC CIPC representative seats and three MRO SAC seats will open for the 2019 calendar year and welcomed anyone interested to serve.
- c. Reorganization of MRO SAC Portal. Fjalstad mentioned the SAC portal and pointed out its usefulness for the MRO SAC. Fjalstad also reviewed the Webinar Request Form.
- d. New MRO SAC email address. Fjalstad announced the [mrosac-admin@midwestreliability.org](mailto:mrosac-admin@midwestreliability.org) as the general contact for SAC administrative business. Chair Hochevar talked about the ways to communicate this new contact information.

## 5. Administrative Matters/Org Docs

### a. Charter

The MRO SAC reviewed the redlined Charter document with Kraft's proposed changes. Kraft suggested, as terms roll out to consider limiting one member per entity instead of two to allow room for new entity members to serve on the Council. Fjalstad explained the reason for two members per entity is to allow different areas from one entity to be covered, cyber, physical, and control system. Fjalstad recommended a change in the guiding principles, in lieu of changing the charter.

### b. Guiding Principles

Kraft provided reasoning for his wordsmithing and specifying "voting" members. Fjalstad talked about making sure the people who are supporting the SAC (primary constituents) are able to participate in events, and find value in what the SAC does.

*Upon a motion duly made and seconded, the MRO SAC unanimously approved the Guiding Principles as written.*

### c. Goals and Objectives

Kraft stressed that the MRO SAC goals and objectives need updating, and his proposed changes warrant further discussion. Kraft explained that the essence of his redlines were making changes to reflect how the MRO SAC is moving forward. Chair Hochevar mentioned the MRO SAC is, in his opinion, overproducing Reliability Matters articles and could do more white papers. Kraft discussed goal 4 and extending the partner list.

*Action item: Kraft will finalize draft of SAC charter and present for approval at next meeting.*

*Action item: Chair Hochevar will remove 3.6 and replace with "Advisor to the Q3 NERC CIPC meeting."*

*Upon a motion duly made and seconded, the MRO SAC unanimously approved the Goals and Objectives as written, with the modification of 3.6.*



d. Proposed 2018 Calendar

Fjalstad provided an overview of the 2018 calendar, and mentioned that the calendar is a way for the MRO SAC to be prepared for upcoming events. Fjalstad also mentioned the web calendar and stressed that the proposed 2018 calendar is not a replacement for that, but is an internal document for the MRO SAC and will be updated on a frequent basis

*Action Item: MRO Staff will upload SAC webinar recordings to MRO's website.*

*Action Item: MRO Staff will add Kraft, Chair Hochevar and Fjalstad as responsible SAC members for Work Plan Item 23 and change Warren LaPlante to Kraft in Work Plan Item 25.*

*Action Item: Chair Hochevar will explore ideas to introduce the SAC independently to new MRO registered entities.*

e. 2018 Work Plan and Assignments

The MRO SAC reviewed the new layout of the work plan. Kraft suggested listing all three primary CIPC reps as a responsible party in the work plan.

Chair Hochevar mentioned the need for additional articles for the newsletter and expressed appreciation to Tim Anderson and Justin Haar for their articles. Fjalstad mentioned the possible inclusion of the article: "The missing chief security officer" by Andy Bochman in a future newsletter. Chair Hochevar reiterated that all articles do not necessarily need to be original articles.

Discussion ensued on webinar hosting and review of the webinars. Kraft talked about rescheduling LaPlante's webinar. It was reiterated that the process for a successful webinar should begin four to six weeks in advance of the webinar date. Chair Hochevar asked for volunteers to provide additional webinars. Fjalstad showed the council members where the public SAC webinar videos are available on MRO's website.

Sharon Koller provided ideas about training and outreach opportunities, discussion ensued and ATC offered to champion the idea of setting the stage for how Gridex is used currently for better preparedness.

Chair Hochevar mentioned that the stakeholder survey should be complete before the Quarter 4 meeting and used to form the 2019 work plan, and be included in the MRO annual board report.

Chair Hochevar announced that the *Introduction to MRO* event on May 22, 2018 includes a presentation on the MRO SAC. Fjalstad and Vice Chair Jensen will be presenting on behalf of the SAC.

*Action Item: MRO Staff to add two additional CIPC names as responsible parties, for a total of three, in the Work Plan for the quarterly reports to the SAC and MRO Board.*

## 6. Project Updates

a. SCADA Training

Vice Chair Jensen provided brief feedback on the SCADA training at MRO in February and stressed that these trainers are best in their class, and the opportunity for MRO to host it was a victory. It was agreed that the MRO SAC would bring INL back as soon as it is financial



feasible since the training was a perfect mix of introductory principles and application, and the consensus was that the training was great.

*Action Item: MRO Staff will seek out support on the SAC presenting another workshop/training.*

b. Webinar Updates

This agenda item was covered during agenda item 5d.

c. ICCP Security

Discussion, led by MRO SAC members, Brown, Anderson and Vice Chair Jensen regarding a secure and flexible data exchange approach for communication between control centers, including ICCP exchange, ensued. Vice Chair Jensen will reschedule a presentation from Paul Skare for a future meeting and will share it on the portal. The 2011 document is entitled *Secure Data Transfer Guidance for Industrial Control Data Systems*,

*Action Item: Vice Chair Jensen will arrange for Paul Skare to attend a future SAC meeting to discuss ICCP.*

d. Region Risk Assessment

The TLP Amber report from the MRO's Regional Security Risk Assessment conducted with the E-ISAC is final. Kraft asked for volunteers to draft a TLP white version of that report.

*Action Item: Chair Hochevar and Kraft will work together with volunteers to create a TLP white version of MRO's Regional Security Risk Assessment.*

e. Region Security Contacts (RSC)

Kraft described how the RSC list includes contacts at each entity for security issues and is used to send security-related communications. Discussion ensued on ensuring an annual review and update of the RSC list.

f. Threat Call Pilot Evaluation

Kraft reviewed the threat call information statistics and explained the premise of the calls. Kraft further explained that by following the guidelines, the goal of having the threat calls be entity-driven and led was accomplished.

Discussion ensued on the logistics of, and moving forward with, the weekly Threat Call. Volunteers were identified to participate in updating the threat call guidelines.

*Action Item: MRO Staff will add the Threat call as an agenda item for the SAC's second Quarter meeting.*

*Upon a motion duly made and seconded, the MRO SAC unanimously approved continuing the threat calls.*

*Action Item: Vice Chair Jensen and members, Kraft and Haar will work together to update the Threat Call guidelines.*



## 7. MRO CIPC Reps

### a. NERC CIPC Report

MRO Representative on the NERC CIPC, Paul Crist, filled in for Marc Child and provided the CIPC report highlighting, among others, the response to Hurricane Irma, cyber intrusion guideline for operators, implementation guidance for synchrophasers and a presentation on the recent North East “cyclone bomb” which was a cold weather event. Discussion ensued on access to encrypted information and improved compliance and a possible white paper on these topics.

### b. NERC CIPC Representation Guidance

Kraft reviewed the redlined document and submitted for MRO SAC approval.

*Upon a motion duly made and seconded, the MRO SAC unanimously approved the Representation Guidance document as submitted by Kraft.*

*Action Item: MRO Staff will finalize the Representation Guidance document and send to the GPC for approval*

## 8. Security Conference

Fjalstad provided an update on the September 26, 2018 MRO Security Conference. Fjalstad shared the chosen theme: *Plan for Failure, Prepare for Success*. Discussion ensued.

## 9. Cybersecurity Update

### a. Spectre/Meltdown

Haar explained the impact Spectre and Meltdown are both having on organizations, heightened by exploits to the vulnerabilities leveraged by bad actors. Discussion ensued.

### b. Cryptocurrency Malware and Mitigation

Chair Hochevar presented on and explained how cryptocurrency mining is used in pop-ups with disclaimers and that people utilizing websites infected by malware are mining cryptocurrency. Discussion ensued on vulnerabilities being leveraged from a cryptocurrency perspective and possible solutions.

## 10. Physical Security Update

### a. Design Basis Threat Implementation

Kraft shared a document describing a TLP: Green workshop entitled *Design Basis Threat Assessment* and led a discussion about having the same workshop hosted in the MRO Region, with facilitation from E-ISAC and sponsorship from the MRO SAC. Kraft explained that interested parties would submit names and then, due to the sensitive nature of the material, a group of individuals would be invited to participate in the initial phase of this training. Kraft also indicated that he has willing volunteers to work on it and he is willing to lead it.

*Action item: Kraft will put together a proposal for a Design Basis Threat Assessment workshop.*

### b. Security Management in the Electricity Sub-Sector Guideline 2018 Update

Kraft provided a report on Security Management in the North American Electricity Sub-Sector, meant as a physical security guideline for electric utilities. Highlights include: Active Shooter



Preparedness, Generic Threat Response Plan, Construction Security and an overview of GridEx. Discussion ensued regarding NERC Alerts from the physical security side, and GridSecCon.

*Action item: Chair Hochevar will reach out to Ross Johnson related to creating a webinar or other outreach related to Security Management in the Electricity Sub-Sector Guideline 2018 Update.*

## 11. EMS

### a. EMS Security

Jensen presented on Triton/Trisis/Hatman malware discovered in mid-November and reported in mid-December. Her presentation provides links to reports and bulletins, and the presentation is available as an agenda attachment on the MRO website. Tyler Stinson elaborated on patches and walked through the devices, mitigation efforts and impact. Discussion ensued. Hochevar shared some things Dragos has done, adding that the information is online here: [www.dragos.com/yearinreview/2017](http://www.dragos.com/yearinreview/2017).

## 12. Partner Updates

### a. E-ISAC

Philip Daigle presented information on what E-ISAC has been dealing with regarding phishing and spear-phishing, and cryptocurrency mining. He also discussed how E-ISAC is using the following tools and that anyone with questions about them can email [operations@eisac.com](mailto:operations@eisac.com) for more information on any of the programs.

- Cyber Risk Information and Sharing Program (CRISP)
  - CRISP is a way for cyber experts to share information. The cost of CRISP has come down considerably since its inception. This has been around for many years, is fee based.
- Cyber Automated Information and Analysis System (CAISS)
  - CAISS is a system of solutions facilitating machine-to-machine indicator sharing and is currently using ThreatConnect (a commercial product). This is in pilot with 60 entities so far and it is expected to expand this year. There is currently no cost to entities for CAISS.
- Malware Analysis Repository and Threat Information Engine (MARTIE)
  - MARTIE is similar to VirusTotal where a hash file or the actual malware file can be uploaded. MARTIE can be used to send a malware sample to E-ISAC. Just upload it to MARTIE, and let E-ISAC know that the download is complete and they will process it. This is in pilot and expected to go to broader audience in 2018. There is currently no cost to entities for MARTIE.

Elizabeth Mairs of Xcel asked where the industry was at with Coyote. Daigle explained that Coyote is currently a Department of Energy (DoE) project and that they are working through some issues about receiving and reviewing data from the OT network.



Kraft asked about Russian election influence and resulting policies, targeted attacks, using industry protocols against itself, etc., asking if any of the systems Philip is working with are being used against the utility industry at this point.

He responded that, in order to have the kind of effect similar to the Ukrainian event, it would have to be on a much larger scale than E-ISAC has seen at this point. Kraft asked if there are policies and protocols in place for the E-ISAC or another government entity to reach out in the case of a major cyber attack, and Daigle assured him there are. E-ISAC is at 26 people, and he announced that the plan is to more than double that in the next few years.

b. Other Partners

No other partners were in attendance. Kraft noted that three partners informed him they had other commitments during the meeting time.

*Action item: Fjalstad will facilitate bidirectional conversations with industry partners in the MRO region.*

### 13. Other Business

Fjalstad mentioned that an interview and a Reliability Matters article will be done for each SAC member in 2018 to support additional promotion of the MRO SAC.

*Action item: Fjalstad will contact SAC members to obtain bios and photos.*

### 14. Adjourn

Having no further business to discuss, the meeting adjourned at 3:00 p.m.

Prepared by: Cynthia Kneisl, Council Secretary.

Reviewed and Submitted by: Richard Burt, Vice President of Risk Assessment, Mitigation and Standards



## Exhibit A – Meeting Attendees

<b>Council Members Present on Web Meeting</b>	
<b>Name</b>	<b>Organization</b>
Mike Kraft, Interim Chair	Basin Electric Power Cooperative
John Hochevar, Chair-Elect	American Transmission Company
Tim Anderson, Interim Vice Chair	Dairyland Power Cooperative
Jodi Jensen, Vice Chair-Elect	Western Area Power Administration
Brian Kollmansberger	Alliant Energy
Justin Haar	Minnkota Power Cooperative
Stephen Brown	Xcel Energy
Tyler Stinson	Xcel Energy
<b>MRO Staff Present on Web Meeting</b>	
<b>Name</b>	<b>Title</b>
Steen Fjalstad	Security and Mitigation Principal
Cynthia Kneisl	Standards, Certification, and Registration Administrator
Dana Klem	Risk Assessment and Mitigation Administrator
<b>Guests on Web Meeting</b>	
<b>Name</b>	<b>Organization</b>
Amy Shatek	Cedar Falls Utility
Brian Zavesky	Missouri River Energy
Casy Hancock	Minnkota Power Cooperative
Chris Evans	Southwest Power Pool
Damon Ounsworth	SaskPower
Ellen Lamb	Xcel Energy
Grant Adams	Avant Energy
Ian King	Xcel Energy
Jennifer Holmes	Alliant Energy
Joe Petaski	Manitoba Hydro
John Carns	McKenzie Electric
John Chang	Manitoba Hydro
Mark Lucas	Great River Energy
Mike Shaughnessy	Xcel Energy
Nathan Shults	Kiewit
Paul Crist	Lincoln Electric System
Rich Kruthoff	Missouri River Energy
Rick Stava	Omaha Public Power District
Ron Bender	Nebraska Public Power District
Sam Chanoski	E-ISAC
Sam Ellis	Southwest Power Pool
Scott Davis	Homeland Security HQ
Seth Shoemaker	Muscatine Power and Water
Sharon Koller	American Transmission Company
Shawn Eck	Liberty Utilities



Tony Eddleman	Nebraska Public Power District
<b>Council Members Not Present</b>	
<b>Name</b>	<b>Organization</b>
Warren LaPlante	Minnesota Power (ALLETE, Inc.)