The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

CIP-014 Update

A lot has happened in the seven years since CIP-014, Physical Security, became effective. The ERO Enterprise (NERC and the six Regional Entities) now have significant experience with how industry implemented CIP-014. Note that on June 16, 2022, FERC approved CIP-014-3, which became effective on that date. As CIP-014-3 does not change any of the enforceable language of CIP-014-2, all references in this article will be applicable to both versions. In this article we'll discuss some of the things we've learned about CIP-014 and some new reference materials that apply to CIP-014. I'll review existing reference materials and bring out-of-date references up to date.

CIP-014 Summary

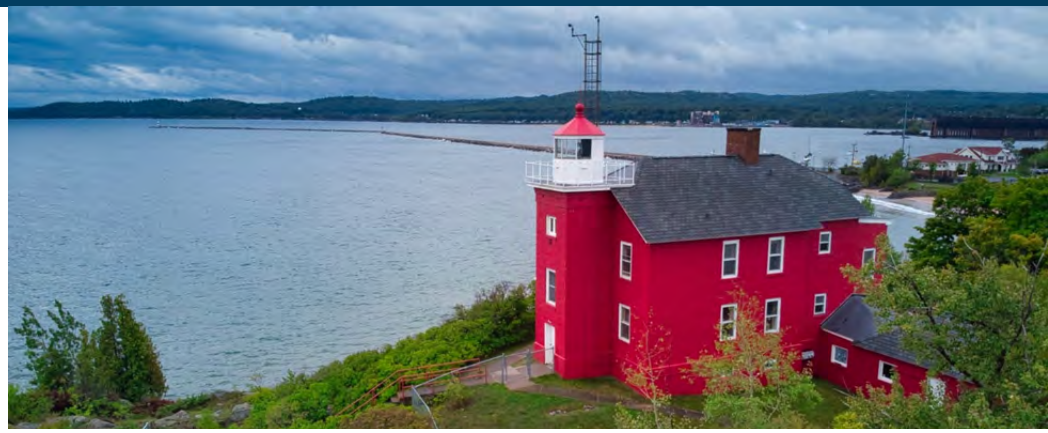
CIP-014 was created in response to the attack on the Metcalf Substation in California on April 16, 2013 [link in Reference 1]. The purpose of CIP-014 is to identify and protect high-consequence BES targets, including substations and Control Centers. CIP-014 requires, in part, risk assessments to identify applicable substations and Control Centers (R1), threat and vulnerability analysis (R4), and development and implementation of physical security plans (R5).

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your Entity. It may also help you and your Entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs. There are times that I also may discuss areas of the Standards that other Entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

CMEP Practice Guide for CIP-014

A CMEP Practice Guide (PG) for CIP-014 R1 [link in Reference 1] was published on Nov. 21, 2021. This PG goes into depth describing how audit teams should evaluate an entity's performance of the risk assessments required by R1. The reason for this attention to R1 is that it is critical to have an accurate list of applicable Transmission stations and substations for the remainder of this Standard. The PG is divided into three main topics:

- **Reviewing the list of substations to be studied:** The PG details how to determine if CIP-014 is applicable to a given Transmission station or substation. The PG also discusses aspects of identifying assets that must be protected, including operating voltages, physical proximity, common facilities, diverse ownership and other considerations.
- **Selection and preparation of the models used in risk assessments:** The PG discusses topics such as the completeness of the model, characteristics of the model such as the load levels assumed and the appropriateness of the model for the risk assessments required.
- **Determining the completeness of the technical analysis performed:** The PG directs audit teams on how to review the entity's performance of system stability analyses, uncontrolled separation assessments and cascading analyses.



Marquette Harbor, MI – Photo: Lew Folkerth

Although the CMEP Practice Guide's intended audience is CMEP staff (e.g., audit teams), the document is publicly available. You can gain a lot of insight into how you will be audited on CIP-014 R1 by studying it.

RSAW

The first version of the CIP-014 Reliability Standard Auditor Worksheet (RSAW) [link in Reference 1] contained instructions to the auditors that presumed reliance on the third-party verifications required by CIP-014 R2 and R6. The RSAW is being revised to remove impediments to fair and consistent auditing, enabling use of the CIP-014 R1 CMEP Practice Guide and the Evidence Request Tool during the audit. I expect the RSAW including these revisions, and updated for CIP-014-3, to be published soon after the publication of this Newsletter.

Continued on page 11

Continued from page 10

Implementation Guidance

The ERO has endorsed three Implementation Guidance documents for CIP-014 pertaining to R1, R4 and R5 [links in Reference 1]. All three were authored by the North American Transmission Forum (NATF) and provide guidance on identifying and assessing Transmission Facilities (R1), identifying and assessing threats to Transmission Facilities (R4), and developing and implementing a physical security plan (R5).

The Implementation Guidance for R5, "NATF Practices Document for NERC Reliability Standard CIP-014-2 Requirement R5," contains a good list of resources for developing physical security plans. In Reference 2 I've provided updates to these references as well as my description of each reference. Reference 3 contains my suggested additional references for your use.

Low Impact Considerations

If you compare the CIP-014 Transmission Owner applicability criteria 4.1.1.1 through 4.1.1.4 to CIP-002-5.1a Impact Rating Criteria 2.4 through 2.7 you will find they are identical. This may lead you to conclude that if you haven't identified any medium impact BES Cyber Systems at a substation, then you're not in scope for CIP-014-3. This is not necessarily correct. You should review these three considerations to determine if your substations are in scope for CIP-014:

1. Unlike CIP-002, CIP-014 is not about BES Cyber Systems, but instead is about physical assets. You need to evaluate your substations for CIP-014 applicability independent of your CIP-002 evaluation.
2. If you own a substation that is physically near another substation, you and the owner of the other substation should assess whether the two substations combined will meet any of the CIP-014 applicability criteria. If so, those substations are in scope for CIP-014 and must comply with at least Requirements R1 and R2.
3. Also unlike CIP-002, you must consider existing substations and also substations planned to be in service within 24 months from the time of your assessment. If those planned changes will bring a substation into scope for CIP-014, you must perform the R1 assessment and R2 third-party review for that substation.

Requests for Assistance

If you are an Entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here. Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Reference Documents

Reference 1

- ***CIP-014-3:*** ***Click here***
- ***Metcalf sniper attack:*** ***Click here***
- ***CMEP Practice Guide CIP-014-2 R1:*** ***TBD***
- ***CIP-014-2, R1 Transmission System Risk Assessment (NATF):*** ***Click here***
- ***CIP-014-2 R4 Evaluating Potential Physical Security Attack (NATF):*** ***Click here***
- ***CIP-014-2, R5 Developing and Implementing Physical Security Plans (NATF):*** ***Click here***
- ***Petition for Modification to Compliance Section of CIP-014:*** ***Click here***
- ***Order Approving Modifications to the Compliance Section of Reliability Standard CIP-014, FERC Docket RD22-03-000, June 16, 2022:*** ***Click here***
- ***RSAWs:*** ***Click here***

Reference 2

Reference List (Additional Resources) from *NATF Practices Document for NERC Reliability Standard CIP-014-2 Requirement R5* (Lew's Updates and Descriptions)

ASIS

- ***Physical Asset Protection Standard (ASIS PAP-2021):*** ***Click here***
  - Softcover Member $35/Non-member $70; eBook $0/$35
  - 61 Pages
  - The documents referenced by the NATF Practices Document, *ASIS Facilities Physical Security Measures 2009* and *ASIS Security Management Standard: Physical Asset Protection 2012* have both been replaced by *ASIS PAP-2021*. *ASIS PAP-2021* walks the reader through developing and implementing a continuous improvement framework for a physical security program. An annex (appendix)

Continued on page 12

Continued from page 11

provides a high-level overview of physical protection techniques and technologies that can be employed.

DHS/CISA

- ***Energy Sector-Specific Plan 2015:*** ***Click here***
  - No charge
  - 39 Pages
  - While somewhat dated, the Energy Sector-Specific Program (SSP) provides a general risk overview that is still useful. It also provides a picture of where the Electric Subsector fits in the overall Energy Sector. This is one of the few documents in this list that mentions the importance of incident response.

IEEE

- ***IEEE Guide for Physical Security of Electric Power Substations (IEEE 1402-2021):*** ***Click here***
  - PDF $49/$61 Softcover $61/$76
  - 38 Pages
  - *IEEE 1402-2021* is a guideline written specifically to address considerations for physical protection of substations. Of particular interest are the sections on threat assessment, design considerations for threat mitigation, and a template for a substation physical security vulnerability assessment checklist.

IES

- ***The Lighting Library:*** ***Click here***
  - Annual Subscription $400/$800
  - *The Lighting Library* is the replacement for *The Lighting Handbook, 10th edition* (out of print, 1087 pages) referenced by the *NATF Practices Document*. *The Lighting Library* is a subscription-based service that provides access to the resources of the Illuminating Engineering Society. By my count, there are 140 documents in the *Library* covering all aspects of lighting science and engineering. I found the document listed below to be of particular interest.

- ***Security Lighting for People, Property, and Critical Infrastructure:*** ***Click here***
  - PDF $84/$120
  - 87 Pages
  - This document provides an in-depth look at the design of lighting for physical security purposes. It discusses basic principles of security lighting, visibility concerns, security zones, lighting equipment and applications.

NERC

- ***NERC Security Guideline for the Electricity Sector: Physical Security 2012:*** ***Click here***
  - 13 Pages
  - No longer available on the NERC website.
- ***NERC Security Guideline for the Electricity Sub-sector: Physical Security Response 2013:*** ***Click here***
  - 13 Pages
  - This was a draft version of the above document. No longer available on the NERC website.

Reference 3 – Lew's Additions to the Reference 2 List and Other References from Around the ERO

ASIS

- ***Protection of Assets – Physical Security, 2021 edition (PoA):*** ***Click here***
  - $159/$225
  - 643 Pages
  - The standards and guidelines above discuss "what" to do to provide physical protection for assets, this volume provides the "how" and "why." It provides an in-depth look at security risk management, security practices, design principles, tools, techniques and many other topics.
- ***Implementing Physical Protection Systems, A Practical Guide, 2nd edition:*** ***Click here***
  - David G. Patterson, CPP, PSP
  - $55/$65 (also available in Kindle $40)
  - 197 Pages
  - This book concentrates on the practical aspects of installation and operation of physical security systems.

Continued on page 13

Continued from page 12

O'Reilly

- ***Incident Management for Operations:*** ***Click here***
  - Schnepp, Vidal & Hawley
  - $18.41
  - 156 Pages
  - Beyond incident response there is incident management. This book discusses why incident management is needed and how to set up an incident management program.

NERC

- ***Security Guideline: Physical Security Considerations at High Impact Control Centers, December 12, 2018:*** ***Click here***
  - 13 Pages
  - This guideline discusses threat assessment, planning and security measures for control centers. While written with high impact BES Cyber Systems in mind, this guideline is useful at all impact ratings.
- ***Physical Security Guideline for the Electricity Sector, June 2019:*** ***Click here***
  - *Assessments and Resiliency Measures for Extreme Events*
  - 22 Pages
  - This guideline takes a different look at physical security from the perspective of extreme events. It includes discussions of planning for extreme events, vulnerability assessments, physical security assessments, drills and exercises, and information sharing.

MRO

- ***CIP-014-2 R1 Assessment Observations and Common Practices, November 2019:*** ***Click here***
  - 10 Pages
  - This presentation discusses audit considerations and common practices for CIP-014.

- ***CIP-014-2 Physical Security, R1, R2, R3 1st Quarter 2016 Guided Self-Certification 1Q 2016:*** ***Click here***
  - 13 Pages
  - This document was used for a 2016 self-certification in MRO.It contains a compliance checklist that may prove valuable.

- ***CIP-014-2 R1 Assessment Observations and Common Practices - ATC Assessment Practices, October 2019:*** ***Click here***
  - 13 Pages
  - This is a discussion of considerations regarding the risk assessment required by R1.

WECC

- ***Internal Controls Failure Points and Guidance Questions CIP-014-2, September 2020:*** ***Click here***
  - 8 Pages
  - This paper discusses internal controls and possible failure points in CIP-014 compliance.

RF

- ***CIP-014 R1 Methodologies, September 2015:*** ***Click here***
  - 18 Pages
  - An entity's perspective of the NATF guidance.
- ***CIP-014-X Update, April 2015:*** ***Click here***
  - 13 Pages
  - A discussion of the foundations of CIP-014.

SERC

- ***CIP-014-2 Audit Approach,*** **September 2019:** ***Click here***
  - 17 Pages
  - A discussion of audit approaches for CIP-014 with humorous touches.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, can be reached here.