The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

BCSI Revisions

On December 7, 2021, FERC issued a letter order approving CIP-004-7 (Cyber Security – Personnel & Training), CIP-011-3 (Cyber Security — Information Protection) and the associated Implementation Plan. The revised Standards implement changes in how BES Cyber System Information (BCSI) is protected. These changes were initiated by industry to address the growing need to be able to store BCSI in cloud environments. Vendor systems such as work management and trouble ticketing are migrating to cloud-only environments, and you need to use these systems to be able to fulfill other CIP requirements.

The revisions to CIP-004-7 move authorization for BCSI access from Requirement R4 to a new Requirement, R6. R6 explains what is meant by the term "access" and introduces a new term, "provisioned access."

The language in CIP-011-3 Requirement R1 has been simplified to provide greater clarity and flexibility in implementing information protection.

CIP-004-7 sets requirements for managing access to BCSI, and CIP-011-3 requires an information protection program (IPP) to protect the confidentiality of BCSI. You should design your programs for CIP-004-7 R4, R5 and R6 and for CIP-011-3 R1 to work in concert to prevent compromising the confidentiality of BCSI.

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.

Crisp Point, MI – Photo: Lew Folkerth

"Obtain and Use"

One of the key concepts introduced in CIP-004-7 R6 is the clarification of the meaning of the word "access." R6 states, "To be considered access to BCSI in the context of this requirement, an individual has both the ability to *obtain* and *use* BCSI." [emphasis added] The "obtain and use" concept focuses our attention on the actual information being protected, rather than the storage locations for the information, and gives us the ability to store BCSI in cloud computing environments.

Think of BCSI as a car parked in your locked garage. Only you and your family may obtain (be able to touch) the car. However, this level of access is worthless without the ability to get into the car and drive away.

That requires that you can both *obtain* the car and have the keys to unlock and

Continued on page 11

Continued from page 10

drive (*use*) the car. You might park the car on a street (cloud environment) so that an unauthorized individual could *obtain* the car, but if you lock (encrypt) the car, no unauthorized individual can *use* the car.

The car might be towed away, denying you the ability to obtain the car, but whoever towed the car still cannot use the car without the keys.

"Provisioned Access"

CIP-004-7 R6 also introduces the concept of *provisioned access*. Based on the language in R6, *provisioned access* has these attributes:

- The access is for an individual (not a system);
- The access is granted as the result of "specific actions";
- The access is authorized;
- The access is needed ("based on need, as determined by the Responsible Entity");
- The access is either:
  - "Electronic access to electronic BCSI," or
  - "Physical access to physical BCSI".

Provisioned access must be authorized (Part 6.1), periodically reviewed (Part 6.2) and revoked as needed (Part 6.3). Access that is not provisioned access, such as unauthorized access, system access, etc. should be addressed by your CIP-011-3 IPP.

The use of the term *provisioned access* in R6 lets your BCSI access management program focus on the actions it is intended to perform – access by authorized individuals to BCSI within your control. All other forms of access should be addressed by your IPP.

Information Protection

CIP-011-3 R1 still requires an IPP, but the two Parts specifying the content of the IPP have been modified. Part 1.1 requires that your IPP have one or more methods to identify BCSI.

Part 1.2 requires one or more methods to mitigate the risks of the loss of confidentiality of BCSI. This new language makes CIP-011-3 R1 a limited risk-based Requirement, in that only confidentiality is addressed by R1. BCSI integrity and availability are not in scope for R1.

I recommend that you apply and document risk management techniques (see sidebar for references) to the tasks of protecting and securing your BCSI.

Consider IPP provisions based on risk that include:

- Prevention of unauthorized forms of access to BCSI;
- Loss of confidentiality of BCSI, perhaps to trigger an incident response and a compliance self-report; and
- Key management, for BCSI protected by encryption.

References

NIST SP800-209, Security Guidelines for Storage Infrastructure, October 2020

Security Guideline for Electricity Sector,Primer for Cloud Solutions and Encrypting BCSI, June 10, 2020

ERO Enterprise CMEP Practice Guide:BES Cyber System Information, April 26, 2019

Lessons Learned from Commission-Led CIP Reliability Audits

- 2019
- 2020
- 2021

A Structure for CIP Risk Management Plans, The Lighthouse, Jan/Feb 2019

SERC/RF Online Risk Management Training

NIST Publication SP800-209, Security Guidelines for Storage Infrastructure, lists various threats and risks to stored information that can be applied to BCSI. SP800-209 also provides insight into the attack surfaces that could be exploited by an attacker to compromise BCSI. The sidebar lists additional resources to help you in updating your IPP for the new Standards.

Continued on page 12

Continued from page 11

Authorization Paths

The revised Standards allow multiple paths for authorization of access to BCSI.

1. BCSI can and frequently does reside on the applicable BES Cyber Systems, EACMS and PACS themselves. When that is the case, provisioned access to that electronic and physical BCSI can be authorized by your CIP-004-7 R4 access management program and does not need to be repeated by your CIP-004-7 R6 BCSI access management program.

2. Other provisioned access to BCSI, such as document management systems, cloud storage, etc., is authorized by your CIP-004-7 R6 BCSI access management program.

3. Access not covered by CIP-004-7 R4 and R6 should be addressed by your CIP-011-3 IPP. The IPP should consider:
    a. Authorized access to BCSI that is not in scope for CIP-004-7, such as BCSI pertaining to medium impact BES Cyber Systems, EACMS and PACS without External Routable Connectivity.
    b. Authorized system (not individual) access to BCSI, if any.

Early Adoption

If you wish to take advantage of the increased flexibility afforded by CIP-004-7 and CIP-011-3, you may elect to adopt these Standards before their official (in the U.S.) effective date of January 1, 2024. If you choose to adopt them early these considerations will apply:

- Required:
    - You must notify all Regional Entities with which you are registered of the date you will begin compliance with CIP-004-7 and CIP-011-3.
    - You must continue to comply with CIP-004-6 and CIP-011-2 until that date.
    - Your new BCSI access management program should become effective on or before the date you begin compliance with CIP-004-7.
    - Your IPP should be reviewed for applicability with the new Standards, and any changes should become effective before the date you begin compliance with CIP-011-3.

- Recommended:
    - You are requested to notify your Regional Entities at least 90 days prior to the date you will adopt CIP-004-7 and CIP-011-3.
    - You are requested to adopt CIP-004-7 and CIP-011-3 on the first day of a calendar quarter.

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.

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.