# The Lighthouse

*By: Lew Folkerth, Principal Reliability Consultant*

## "Achieve the Objective…"

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

**Q: How do I show an audit team that I have "achieved the objective" of a CIP Requirement?**

**A: Objective-based Standards**

The ERO Enterprise (NERC and the Regions) has been trending toward objective-based Reliability Standards for many years. This trend appears to be gaining momentum, especially with the CIP Standards.

Some Requirements, such as CIP-010-3 R4, Transient Cyber Assets and Removable Media, explicitly use the phrase "achieve the objective" within the language of the Requirement. FERC stated recently, "We expect responsible entities to be able to provide a technically sound explanation as to how their electronic access controls meet the security objective." [Order 843 at P28, referring to electronic access controls for low impact BES Cyber Systems]

I recommend that you treat all of the CIP Standards as objective-based, and that you write your policies, plans, processes, and procedures from this perspective.

The shift toward objective-based Standards is good for security and also makes good business sense. Why spend money on compliance and security programs that do not result in a robust security posture? Why not maximize the benefit of compliance expenses by implementing good security practices that achieve the intended objective, and use compliance as the governing layer to ensure those security practices are followed rigorously? Compliance should be a by-product of a robust security program, not an end in itself.

As an example, an entity implemented a network backup system for its primary Control Center. The backup system uses a network-attached storage system, which stores the backed-up files for the entire Control Center. This arrangement meets the language of CIP-009-6, Recovery Plans for BES Cyber Systems, by providing for the backup and storage of information required for

Sand Hills Lighthouse, Ahmeek, MI – Photo: L Folkerth

recovery. However, online storage is subject to the threat posed by ransomware, which encrypts a victim's data and demands a ransom to provide decryption. If the Control Center's systems fall victim to this threat, the online backups that might be used to recover those systems could be encrypted as well. This would leave no way to recover the Control Center's systems without rebuilding those systems from scratch, a lengthy process which may result in a very different operating environment for the entity. If the entity had reviewed this approach against the objective of CIP-009-6, which might be stated as: "Be able to recover Control Center operability from any foreseeable event within a reasonable time," the entity would probably have seen the need for offline backups on its own.

**Security Plan**

In order to be able to demonstrate meeting objectives, your organization needs to have a documented plan in place. That plan needs to address all objective-based Requirements, but I recommend that you write your plan to address the objectives of all the Requirements that are applicable to you.

If you're subject to the CIP Standards, you already have a security plan that consists of a set of security processes tied together by a security policy. Let's build on this foundation to create a comprehensive security plan for your CIP assets.

**Overall Security Objective**

Your organization's security plan should include an objective for the plan as a whole. This overall objective will be the target all Requirement-based objectives


Continued on page 13

*Continued from page 12*

should support. For example, the overall objective for a Generator Operator might say, "Maintain the safety, operability, and integrity of ABC Generating Plant by rigorously implementing security practices that address the risk of compromise by a malicious actor or by inadvertent action."

I'll take this objective apart and explain what it means to me. I suggest that you perform this exercise for each of your objectives and keep the analysis in your documentation.

- "Maintain" implies a continuing process. Security is not something that you perform once and you're done. Security is an ongoing set of actions that adapt to changing conditions.
- "Safety" is always the first priority. I included safety here because safety instrumented systems have been successfully compromised by malicious actors.
- "Operability" of an asset is the ability to have control over the operation of that asset. If you lose operability, the consequences could be extreme. For example, a set of relays at multiple substations could be operated in a way to cause extended overload of a transformer or transmission line, perhaps resulting in destruction of that equipment.
- "Integrity" is the health of the asset as a whole. If integrity is compromised, the asset could be damaged, you may lose the benefit of the asset for an extended time, and you may incur substantial costs to repair the asset.
- "Rigorously implementing" means that security that is partially implemented, or implemented on an irregular schedule, may not be effective in preventing the asset from being compromised. For example, the Equifax breach was reportedly possible because one security patch was not applied to a server in a timely manner.
- "Security practices" are the actions specified in this security plan.
- "Address the risk" means to look at or pay attention to risk. It is impossible to eliminate all risk, so we prioritize where we spend our resources based on our evaluation of the risk involved.
- "Compromise" can be any condition that affects the function of the asset. This could involve denial of service, installation of malicious code, damage or destruction of physical equipment, and so on.
- "Malicious actor" can be an employee, contractor, vendor, activist, criminal, nation-state, and many others. Your security plan should evaluate the risk of each type of actor and implement protections based on the assessed risks.
- "Inadvertent action" means any action taken that has unintended adverse consequences. For example, NERC Lesson Learned LL20181001 (available here) discusses the loss of a SCADA system for several hours after a seemingly simple patch cable change.

This is a simplified example. You should adopt the overall security objective that works best for your organization.

**Requirement-based Security Objectives**

In order to achieve the overall security objective, specialized security objectives should be created to address particular areas of security. You can combine multiple CIP Requirements into a program group, such as ports and services, with a common objective. Or you can address the CIP Requirements individually.

For the discussion below, I'll assume we're looking at the Requirements individually. Make sure your security plan can answer the following questions for each Requirement:

1. **What is the security objective of this Requirement?**
   Try to state the security objective, as you believe it applies to you, clearly and succinctly. For example, I might state the security objective of CIP-002-5.1 R1, BES Cyber System Categorization, as, "Identify and categorize each device that could be susceptible to cyber compromise and that could have a reliability impact before manual intervention can override the compromised device."
2. **How will the security objective be met?**
   Your security plan must clearly show the steps you take to meet the security objective. You get to determine how you will achieve the objective, subject to review and assessment from an audit team. These steps will be what your performance is measured against, rather than a prescriptive requirement. For example, if your security plan calls for you to use application whitelisting to prevent malicious code, your audit will assess your effectiveness in the implementation of this approach.
3. **How will the security plan adapt to changing threats?**
   The threat environment changes far more quickly than Standards can be modified. Unless the standards development process changes, the CIP Standards will always lag far behind emerging threats. Therefore, it is important that your security plan is designed to recognize and deal



Continued on page 14

*Continued from page 13*

**Internal Controls**

If you want to learn more about internal controls, there are many sources of information. *Standards for Internal Control in the Federal Government* (the GAO "Green Book") is available here.

NERC's *ERO Enterprise Guide for Internal Controls* is available here.

If you are interested in a discussion of internal controls with RF staff, please request an Assist Visit. Details are at the end of this article.

with evolving threats. For example, your security plan might establish a threat analysis team that meets periodically to analyze changes to the threat environment and to plan responses to emerging or changing threats. In the CIP-009-6 R1 example I presented earlier, the entity designed the online backup scheme before the threat of ransomware became significant. A threat analysis team could have identified that threat as it became known and responded by ensuring an offline backup system was implemented to supplement the online backups.

4. **How will you measure performance of the plan?**
   Your security plan should include measures to provide reasonable assurance that the objectives of the plan will be achieved. This is one of the functions of internal controls. Your internal controls should be designed to identify potential problems before they become actual security or compliance issues. [See sidebar]

5. **How will you correct any shortcomings in the plan?**
   Especially in cyber security, plans can age and need updating. You should review your security plan and your performance measures periodically to ensure the plan is not beginning to weaken in any area. You will need to determine what the frequency of this review should be. This will depend on many factors, such as the emergence of new threats, changes in existing threats, the position of your entity within the BES, etc.

6. **Does the plan meet compliance requirements?**
   Whenever the plan changes, make sure you are still meeting the letter of each Requirement, in addition to your security objective. For example, an entity implemented application whitelisting to achieve the objective of preventing the introduction of unauthorized code into its systems. Since the entity achieved its objective in this way, the entity wanted to know if it could perform patch management on a quarterly cycle, rather than monthly. The audit teams have great flexibility, but the language of CIP-007-6 R2 is clear. The entity was advised to retain the monthly patch cycle until audit practices become sufficiently flexible to be able to permit alternate ways of achieving compliance.

7. **Will the plan produce sufficient, appropriate evidence of compliance?**
   For the prescriptive CIP Requirements, such as CIP-007-6 R2, Patch Management, make sure your security plan produces good quality evidence of compliance. As a guide to what evidence will be requested during an audit, Version 2 of the Evidence Request Tool is now available on the NERC web site. For objective-based CIP Requirements, such as CIP-007-6 R3, Malicious Code Prevention, produce documentation of the above six steps, with emphasis on steps 2 and 4. You can look at step 2 as providing the (self-imposed) prescriptive requirements that the objective-based Requirement lacks. Step 4 provides evidence that you are rigorously following the requirements you specified in step 2. Refer to the Evidence Request Tool for examples of the type of evidence needed to satisfy a prescriptive Requirement, and adapt these examples for your own use.

If you would like help in setting up a risk-based compliance program that addresses objective-based Standards and Requirements, or if you just want a different set of eyes to look at your work, you may request an Assist Visit via the web link below.

**Requests for Assistance**

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

## Feedback

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

I may be reached here.