# The Lighthouse

*By Lew Folkerth, Principal Reliability Consultant*

**Remote Access - Advanced Topics**

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.

In the March/April 2015 Newsletter I explored the basics of Electronic Security Perimeters (ESPs) and remote access (see article here). In this column, I'll discuss some advanced topics regarding remote access, including ways you can improve your compliance and security postures. Since I've seen many entities experience compliance issues in this area, my recommendations will go beyond the minimum requirements of the Standards. I do this to encourage you to improve the security of your BES Cyber Systems and to provide your entity with a more robust means of demonstrating compliance. One way of looking at remote access is that any communications traffic crossing your ESP boundary is remote access. However, the CIP Standards provide specific definitions and corresponding requirements for various types of remote access. While looking at this topic, I'll include considerations for CIP-005-6, Electronic Security Perimeter(s), which will take effect in the U.S. on July 1, 2020. Also, I will include considerations for CIP-012-1, Communications between Control Centers, even though it has not yet received regulatory approval in the U.S. In discussing electronic access control, I'll assume you are using a firewall as your access control device, but the discussion applies to other forms of access control as well, such as a router and its access control list (ACL).

**Remote Cyber Asset Capabilities**

In any remote access scenario, the capability of the remote Cyber Asset is of critical importance. At the high and medium impact levels, the remote Cyber Asset is any device outside the ESP that communicates with a device inside the ESP. At the low impact level, the remote Cyber Asset is any device outside the asset containing low impact BES Cyber Systems that communicates with a device inside the asset.

Sturgeon Point Light Station, MI - Photo by Lew Folkerth

You must ensure, and be able to demonstrate to an audit team, that any remote Cyber Asset does not meet the definition of a BES Cyber Asset. In other words, the remote Cyber Asset cannot have a 15-minute impact on the reliable operation of the BES. If the remote Cyber Asset does have this capability, then it meets the definition of a BES Cyber Asset and must be included in a BES Cyber System at the appropriate impact level. The BES Cyber System must then be accorded the protections of CIP-003-8 through CIP-013-1, as applicable to its impact rating. This applies to all remote access at all impact levels, not just Interactive Remote Access.

In support of this stance, let's refer to the FERC order that remanded an Interpretation of CIP-002-4, Critical Cyber Asset Identification, in March of 2013 (see inset). That order clearly states FERC's concern over the capabilities of remote Cyber Assets. While this order applies to CIP-002-4, which never became enforceable, the principle carries forward into CIP-002-5.1, BES Cyber System Categorization.

I'll add an example to that provided in the inset: a transmission operator's laptop computer is capable of Interactive Remote Access to the operator's normal workstation, which is a console within the Control Center. This console is a BES Cyber Asset included in a high impact BES Cyber System. Once the remote access is established, the operator can access the console as if the



Continued on page 16

*Continued from page 15*

14. For example, a laptop computer connected to an EMS network through the Internet may be used to supervise, control, optimize, and manage generation and transmission systems, all of which are essential operations. However, the proposed interpretation of "essential" may leave certain cyber assets lacking the required CIP Reliability Standards protection that could, if compromised, affect the operation of associated Critical Assets even though the unprotected cyber assets are using similar access and exerting the same control as cyber assets that are deemed under the proposed interpretation to be "necessary or inherent to the operation of the Critical Asset." The proposed interpretation, in effect, would create a window into the EMS network that could be exploited.

[Order on Interpretation of Reliability Standard, Docket RD12-5-000, March 21, 2013, at P14]

operator were sitting at the console keyboard. This will grant the operator the same operating capability as the console, which includes the ability to control various elements of the BES in real time. The operator's laptop computer can therefore have a 15-minute impact on the BES, which makes the laptop computer a BES Cyber Asset.

Another concern is the ability of the remote Cyber Asset to access or store BES Cyber System Information (BCSI). BCSI must be protected and securely handled during storage, transit and use as required by CIP-011-1 R1, Information Protection. If the remote Cyber Asset has the ability to access BCSI, then such access must conform to your information protection program required by CIP-011-1 R1. If the remote Cyber Asset has the ability to store BCSI, then it must be designated as a storage location for BCSI, and access to it must be authorized and verified in accordance with CIP-004-6 R4, Personnel & Training.

**Procedural vs. Technical Controls**

CIP-005-6 requires technical controls for each Requirement and Part. It's a good idea to layer procedural controls on top of the technical controls. This will reinforce the concept that remote access to protected systems must obey strict rules. But you must not rely on the procedural controls alone. Your firewall rules must protect your networks from inadvertent and malicious use of remote access.

**Remote Access Protocols**

Let's take a closer look at what constitutes a remote access client. The language of the Interactive Remote Access definition says that Interactive Remote Access uses a remote access client but doesn't further define what a remote access client is. This isn't really a problem because there is no way to determine what software is being used to initiate the access from a remote Cyber Asset. The only indication we have is the communication protocol being used to access the system within the ESP.

Your audit team will look at your firewall ruleset to see if any communication protocols capable of interactive access are permitted from a location other than an Intermediate System.

Here are some common remote access clients and the protocols they use:

| Remote Access Client | Protocol | Well-known Port(s) |
|---|---|---|
| Remote Desktop | Remote Desktop Protocol (RDP) | TCP/3389 |
| Terminal Emulator | Telnet | TCP/23 |
| Many free and commercial programs | Secure Shell (SSH) | TCP/22 |
| Web browser | HTTP, HTTPS | TCP/80, TCP/443 |
| FTP Client | File Transfer Protocol (FTP) | TCP/20, TCP/21 |
| File explorer, etc. | SMB | TCP/445 |
| File explorer, etc. | NFS | TCP/2049, UDP/2049 |
| MIB Browser | SNMP | TCP/161, UDP/161 |
| Unix r-commands | rlogin, rcp, rsh, etc. | TCP/513 |

CIP-005-6 R2 Part 2.1 requires all Interactive Remote Access to utilize an Intermediate System. In order to enforce this Requirement you will need technical controls that do one of the following:

- Ensure that all communication protocols that permit interactive access into the ESP originate only at an Intermediate System. The firewall ruleset (or router ACL) will provide your auditors with the evidence they need to determine compliance.
- If you permit a remote access communication protocol from a Cyber



Continued on page 17

*Continued from page 16*

Asset other than an Intermediate System, you must provide additional technical controls to ensure that interactive access is not permitted.

One of the protocols listed in the table above is Secure Shell (SSH). SSH has many capabilities and can present problems in demonstrating that your Intermediate Systems are not being bypassed. The SSH client, which communicates with the SSH protocol, is designed for interactive access. But the SSH protocol is also commonly used for system-to-system access.

Interactive and system-to-system access both use the same protocol, so your firewall can't tell the difference. Neither can your auditors. It is up to you to be able to demonstrate that a remote connection using the SSH protocol from a Cyber Asset other than an Intermediate System cannot be used for interactive access. I plan to discuss methods of doing this in a future article.

**Demonstrating Compliance**

CIP-005-6 R2 Parts 2.1-2.3 do not require you to implement Interactive Remote Access. If you choose not to permit Interactive Remote Access into your ESPs, then you do not need Intermediate Systems, multi-factor authentication, etc. But you must still be able to demonstrate that your technical controls do not permit interactive access. And, as discussed above, if you do implement Interactive Remote Access you must still show that your Intermediate Systems cannot be bypassed with an interactive-capable protocol. Since this topic is inextricably entwined with firewall rule management as a whole, I'll base my discussion on CIP-005-6 R1 Part 1.3.

Demonstrating compliance with CIP-005-6 R1 Part 1.3 begins with your change management program for firewall rules. Before a new rule is put into production, it should receive a rigorous review. To avoid common problems with the documentation of access control rules, and to ensure your security is as effective as possible, I strongly recommend going beyond the minimal requirements of the Standard.

Here are the items I recommend you consider and document for each rule:

- Nature of the remote device: What type of device is at the far end of this connection? Who owns it? How is its security managed?
- What port or port range will need to be permitted? Is the traffic inbound or outbound?
- What protocol will be used on this connection?
- What is the operational purpose of this traffic? What does it contribute to the reliable operation of the BES?
- What type of access does this rule permit?
    - Interactive Remote Access
    - ESP-to-ESP
    - System-to-system
    - Vendor remote access
        - If so, you must have a method to disable the access per CIP-005-6 R2 Part 2.5
    - Control Center to Control Center
        - Prepare for CIP-012-1 protections (e.g., encryption)
    - Other?
        - If so, what?
- When this rule is implemented, what capability will the remote device have?
    - Could it have a 15-minute impact on the BES?
        - If so, it must be identified as a BES Cyber Asset, included in a BES Cyber System, and protected.
    - Could it have access to BCSI?
        - If so, your information protection program must be applied.
        - If it will be able to store BCSI, it must be identified as a BCSI storage location and access controlled per CIP-004-6 R4.
- What changes to remote systems, companies, etc. might cause this rule to be modified or removed? You should have a method of monitoring for events that should trigger a re-evaluation of a rule.

When you have the information listed above, I recommend that you perform a risk assessment of the rule in the context of the operational purpose of the rule. Your risk assessment should answer these questions:

- Does the capability provided by this rule justify the risk this rule adds?
- Can this traffic be intercepted?
- Can this traffic be compromised?
- Is this traffic considered Interactive Remote Access? If so, is it through an Intermediate System?

And, once you have assessed the risk of a rule, what mitigations should you apply to minimize the risk the rule presents?

- Can the scope of the rule (e.g., port ranges, address ranges) be



Continued on page 18

*Continued from page 17*

reduced?
- Should this traffic be monitored? If so, how?
- Should this traffic cause an alert? If so, under what circumstances?
- Does this traffic need additional protections? If so, what is needed?

In order to keep this information up to date, I recommend that you periodically review the information and assessments listed above. This is not explicitly required by CIP-005-6 but is a good practice to minimize both your security risk and compliance risk by catching changes that might slip through your normal processes.

I also recommend that you monitor traffic crossing your ESP boundary to look for patterns of traffic that are new, unexpected, or vary from your normal patterns. There are several commercial and open source tools to help you do this.

On the topic of monitoring, I also recommend monitoring the content of Interactive Remote Access sessions. Monitoring remote sessions can provide assurance that the remote access is being used in accordance with the need for which it was granted. This may need to be implemented on the Intermediate System, since encryption is required up to the Intermediate System.

**Remote Cyber Asset Security**

Many of the Cyber Assets that remotely access devices within the ESP are not within the scope of the CIP Standards. Even though they are not in scope, I recommend that you consider implementing controls to reduce the security risk these Cyber Assets present. For example, a device engaged in Interactive Remote Access over a Virtual Private Network (VPN) should not permit other network traffic at the same time as VPN traffic. This is known as split tunneling and is a serious risk to the protected Cyber Asset being accessed.

Protections on the remote Cyber Asset should include:

- Prohibiting split tunneling;
- Ensuring no personal devices can be used for remote access;
- Managing access permissions on the device – ensuring administrative access is strictly controlled;
- Managing security patches for all software on the device;
- Hardening the device to reduce its attack surface;
- Ensuring no unauthorized software can be installed on the device;
- Storing the device in a secure location when not in use;
- Keeping anti-malware software and signatures up to date; and
- Enabling a host-level firewall on the device.

This is not an exhaustive list, but it might serve as a starting point in your consideration of this issue.

**General Recommendations**

In summary, CIP-005-6 requires that you tightly control all traffic crossing the ESP border. You should document all traffic so there is no question of what the traffic is for and why it is needed. Meeting minimum compliance Requirements in this area may not be enough. You may find it useful to go beyond minimum compliance to ensure you have the documentation to provide an audit team with reasonable assurance that you are meeting compliance for each Requirement.

**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.

## 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.