Managing Interactive Remote Access

2015 CIP Compliance Workshop

June 2, 2015

Shon Austin
Lead Compliance Specialist
Objectives

• What is Interactive Remote Access?
• Which requirements are associated with Interactive Remote Access?
• Migrating from V3 to V5 (example implementation solutions)
• Avoid the most common sticking points/potential issues
• Questions and Summary
What is Interactive Remote Access

Interactive Remote Access - Effective 4/1/16 - Interactive Remote Access is defined as:

“User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from:

1) Cyber Assets used or owned by the Responsible Entity,
2) Cyber Assets used or owned by employees, and
3) Cyber Assets used or owned by vendors, contractors, or consultants.

Interactive remote access does not include system-to-system process communications.”
What is Interactive Remote access

Intermediate System is defined in the NERC Glossary of Terms as:

“a Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter. (ESP)”

The Intermediate System acts as proxy between the Cyber Asset initiating the external communication and the cyber assets within the ESP.
What is Interactive Remote access

• Intermediate system can be broken into a collection of systems
  – Number of functions (e.g., protocol break or proxy, encryption termination, and multi-factor authentication)
  – Mix and Match
Applicable Systems

• High Impact BES Cyber Systems and their associated PCA

• Medium Impact BES Cyber Systems with External Routable Connectivity* (ERC*) and their associated PCA

*This is addressed in SPP RE External Routable Connectivity presentation.
Requirement

- Part 2.1 - Use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset
- Part 2.2 - Use encryption that terminates at an Intermediate System for all Interactive Remote Access
- Part 2.3 - Use multi-factor (i.e., at least two) authentication to manage all Interactive Remote Access sessions
Implementing Part 2.1

- Part 2.1 - Use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset
  - Identify your entity’s requirements for allowing Interactive Remote Access
  - To increase overall security posture, place the Intermediate System(s) into a demilitarized zone (DMZ)
    - a defined, protected network with both ingress and egress filtering rules in place
  - The Intermediate System can be used to access Cyber Assets in mixed environments
    - These system can have different impact ratings inside the ESP as well as be outside the ESP
Implementing Part 2.1

• Establish a criteria for determining which applications should reside on the Intermediate System
  – Need to know

• Ensure Interactive Remote Access must be managed by the Intermediate System
  – Cyber Asset initiating the external communication does not have direct external access
    ▪ Cannot RDP directly to SCADA system within an ESP from outside the ESP
  – Not a pass through
    ▪ RDP from the intermediate System must be a new session from the Intermediate System
Implementing Part 2.1

• Interactive Remote Access is **NOT**
  – System-to system communications
    ▪ Despite the fact that the protocol can be used for Interactive Remote Access
Implementing Part 2.2

• Part 2.2 - Use encryption that terminates at an Intermediate System for all Interactive Remote Access
  – Encryption between the Cyber Asset initiating communication and the Intermediate System(s)
  – Where is encryption required to terminate?
    ▪ There is confusion regarding where encryption must terminate
    ▪ Encryption only required on the “non-secure” side of the Intermediate System
How to implement Part 2.3

- Part 2.3 - Use multi-factor (i.e., at least two) authentication to manage all Interactive Remote Access sessions
  - Implement multi-factor authentication use authentication factors from at least two of three generally accepted categories:
    - Something you know (the knowledge factor)
      - (e.g., a password or personal identification number or PIN)
    - Something you have (the possession factor)
      - (e.g., a one-time password token or a smart-card)
    - Something you are (the inherence factor)
      - (e.g., fingerprint or iris pattern)
How to implement Part 2.3

• An additional authentication factors outside of the classical paradigm
  – When implemented reduces the shortcomings associated with traditional (static) password
    ▪ Location factors - the authenticator's current location
      – GPS device (Smartphone)
How to implement Part 2.3

• Where does multi-factor authentication have to be performed?
  – Before gaining access to a system inside the ESP

• Can a Intermediate System be accessed directly for Interactive Remote Access without performing multi-factor authentication?
  – No. Must ensure multi-factor authentication cannot be by bypassed when attempting Interactive Remote Access to assets within the ESP
How Interactive Remote Access’s vulnerabilities are reduced in V5 (from V3)
Entity’s EMS SysAdmin via Remote PC
- Remote PC is an Entity owned asset
- Remote PC is assessed by Entity’s NAC solution
- Remote PC has no EMS applications installed
- When connected via VPN, Remote PC is assigned an IP from a dedicated DHCP scope

Connection Methodology:
- EMS SysAdmin connects to Entity’s network via VPN using multi-factor authentication
- For EMS system access, Remote PC is permitted to connect via RDP to the EMS Jump Host
- For Corporate resource access, Remote PC is permitted to connect via RDP to their Corporate PC
Entity's EMS SysAdmin via Corporate PC
- Corporate PC is an Entity owned asset
- Corporate PC is assessed by Entity's NAC solution
- Corporate PC has no EMS applications installed
- Corporate PC is on a dedicated Corporate subnet

Connection Methodology:
- For EMS system access, Corporate PC is permitted to connect via RDP to the EMS Jump Host. EMS SysAdmin connects to EMS Jump Host via RDP
- For Corporate resource access, EMS SysAdmin utilizes this PC
EMS Supporting Services
Firewall
Permits RDP from EMS SysAdmin Corporate PCs and from EMS SysAdmin VPN address pool to EMS Jump Host(s)

EMS Jump Host Domain Controller (DC)
- EMS Jump Host authenticates users against the EMS Jump Host DC
- EMS Jump Host DC resides in the same subnet as the EMS Jump Host(s)

EMS Jump Host (Intermediate Device)
- EMS Jump Host is an Entity owned asset and is assessed by Entity’s NAC solution
- EMS Jump Host is on a dedicated firewalled subnet
- RDP access only, no local access allowed
- No Internet or Email Access
- EMS SysAdmin logs into the EMS Jump Host with EMS Active Directory (AD) credentials and thumb print reader for multi-factor authentication
- Connects to EMS CIP servers using the appropriate applications
EMS CIP ESP Firewall
Permits only the necessary ports from the Jump Host(s) to the EMS CIP Servers

EMS CIP Servers
- All EMS administrative applications reside on the EMS CIP Servers
- From the EMS Jump Host, EMS SysAdmin logs into the EMS CIP Servers with EMS credentials stored in the EMS
Suggested Evidence

• Network diagrams
• Evidence of multi-factor authentication
• Evidence of end-to-end encryption
• Evidence that Intermediate System is subjected to applicable CIP requirements for EACMS (Electronic Access Control or Monitoring System)
References

• DRAFT Lesson Learned CIP Version 5 Transition Program, CIP-005-5 R2: Interactive Remote Access, Version: January 9, 2015

• NERC Guidance for Secure Interactive Remote Access, July 2011

• National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-63-2 (2013)
Summary

- Interactive Remote Access must be managed by an Intermediate System(s)
- Interactive Remote Access does not originate on an Intermediate System or inside of an ESP
- Requires encryption to Intermediate System
- Requires multi-factor authentication
- Programmatic interfaces can run on Intermediate System, eliminating Interactive Remote Access
SPP RE CIP Team

- **Kevin Perry**, Director of Critical Infrastructure Protection  
  (501) 614-3251
- **Shon Austin**, Lead Compliance Specialist-CIP  
  (501) 614-3273
- **Steven Keller**, Lead Compliance Specialist-CIP  
  (501) 688-1633
- **Jeremy Withers**, Senior Compliance Specialist-CIP  
  (501) 688-1676
- **Robert Vaughn**, Compliance Specialist II-CIP  
  (501) 482-2301