

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# Project 2023-04 Webinar Modifications to CIP-003

Tony Hall, Chair, LGE & KU

Jay Cribb, Vice Chair, Southern Company

DT Members: Sean Randles, Leeward Renewable Energy, LLC., and  
Clayton Whitacre, Great River Energy

February 20, 2024

**RELIABILITY | RESILIENCE | SECURITY**



- **NERC Antitrust Guidelines**

- It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

- **Notice of Open Meeting**

- Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

# Drafting Team (DT) Members

	Name	Entity
<b>Chair</b>	Tony Hall	LGE&KU
<b>Vice Chair</b>	Jay Cribb	Southern Company
<b>Members</b>	Monica Jain	Southern California Edison
	Clayton Whitacre	Great River Energy
	Barry Jones	Western Area Power Administration
	Robert Montgomery	Duke Energy
	Peggy McDannald	Associated Electric Cooperative, Inc.
	Josef Chesney	Powder River Energy Corp
	Sean Randles	Leeward Renewable Energy, LLC
	Lemon Williams	Pine Gate Renewables
	Jeff Sykes	Utility Services
	Darrel Grumman	EPE Consulting


- Background and Overview
- Initial Draft Comments
- Modifications to CIP-003-9
- Example Diagrams from Technical Rationale
- Implementation Plan
- Q&A

**NERC**  
NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Low Impact Criteria Review Report

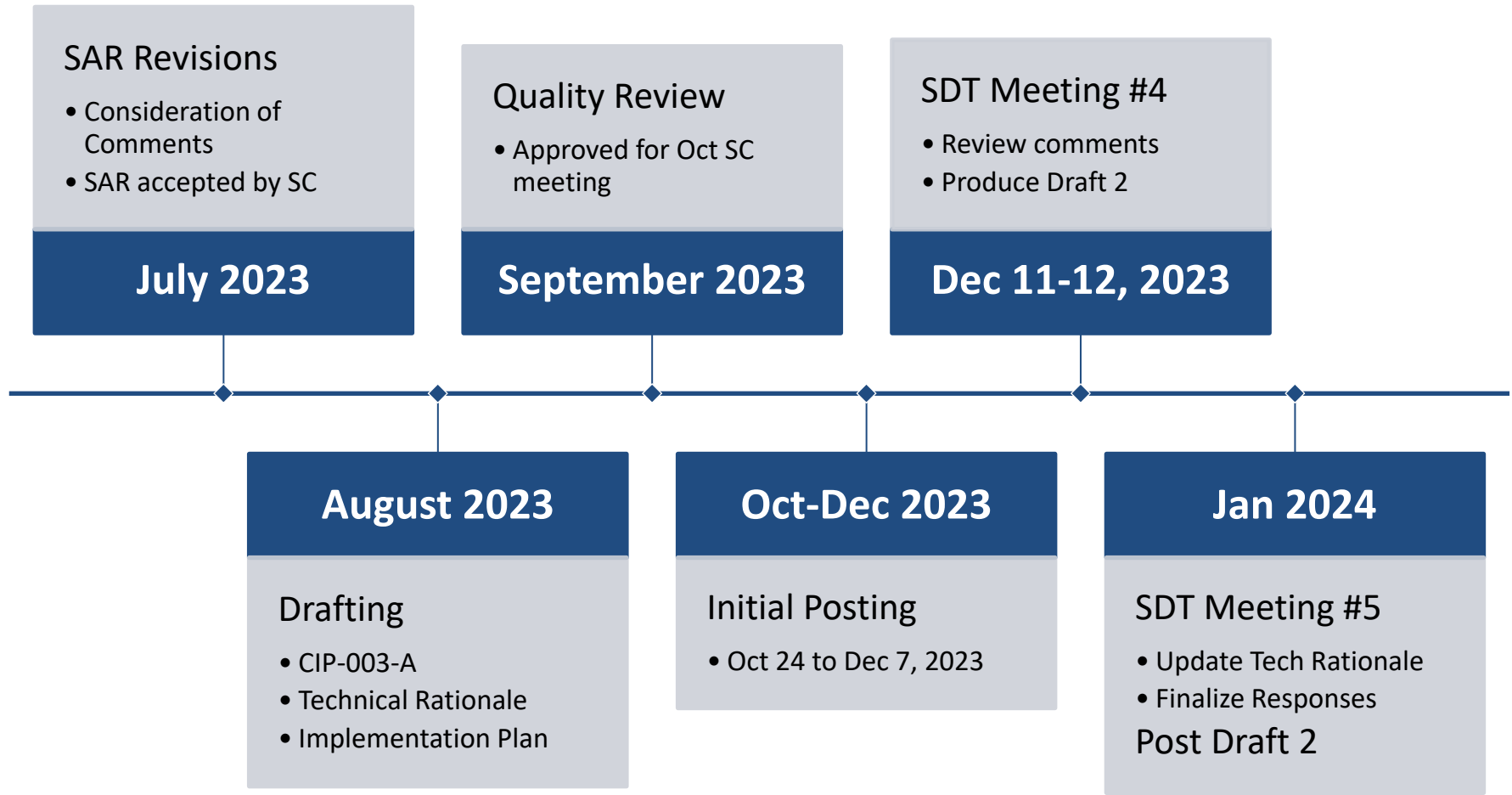
NERC Low Impact Criteria Review Team  
White Paper  
October 2022

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE  
Suite 600, North Tower  
Atlanta, GA 30326  
404-446-2560 | [www.nerc.com](http://www.nerc.com)

- LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems
- [LICRT Report](#)
- CIP Standard Revisions
  - Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
  - Requirement(s) for protection of user authentication information in transit for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
  - Requirement(s) for detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity.
- [Project 2023-04 SAR](#) includes the LICRT recommendations



- Does not allow “Intermediate System” type architectures for remote access to lows.
  - Protect the user information had a target of the “asset containing...”
- The flow of Section 3 is unclear
- “Authenticate users when permitting each instance of electronic remote access”
  - Need clarity on what “each instance” means
- For vendor access, “implement methods” became “implement controls”
  - Interpretations that all vendor access must be disabled
- “To mitigate risks associated with electronic access” in the Section 3 header is too broad



**Section 3. Electronic Access Controls:** Each Responsible Entity shall control electronic access as outlined below.

**3.1** For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, where electronic access is:

- i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
- iii. not used for time-sensitive communications of Protection Systems,

the Responsible Entity shall implement a control(s) that:

**3.1.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

**3.1.2** Detect known or suspected malicious communications for both inbound and outbound electronic access;

**3.1.3** Authenticate users when permitting each user-initiated instance of electronic access to a network(s) containing low impact BES Cyber Systems;

**3.1.4** Protect user authentication information for each user-initiated instance of electronic access while in transit between the Cyber Asset outside the asset containing low impact BES Cyber System(s) and

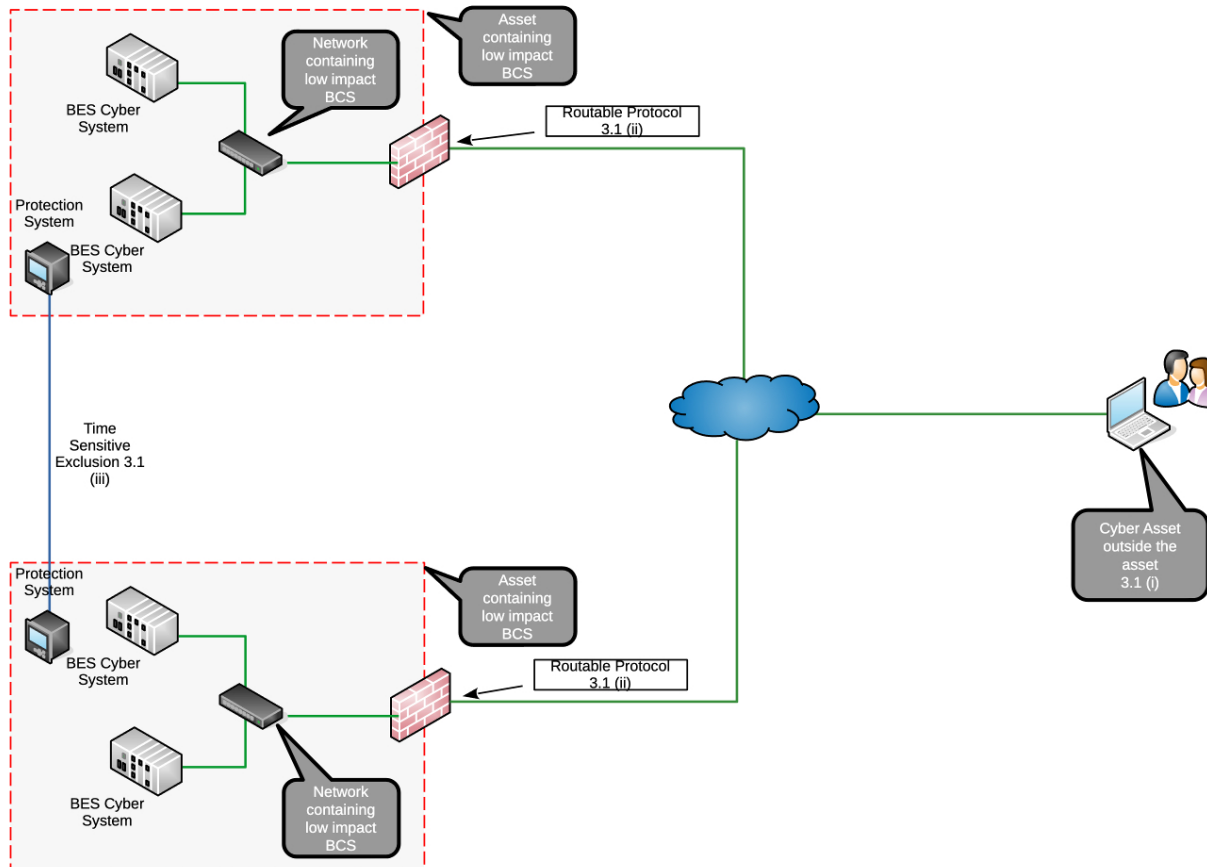
- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BES Cyber System(s);

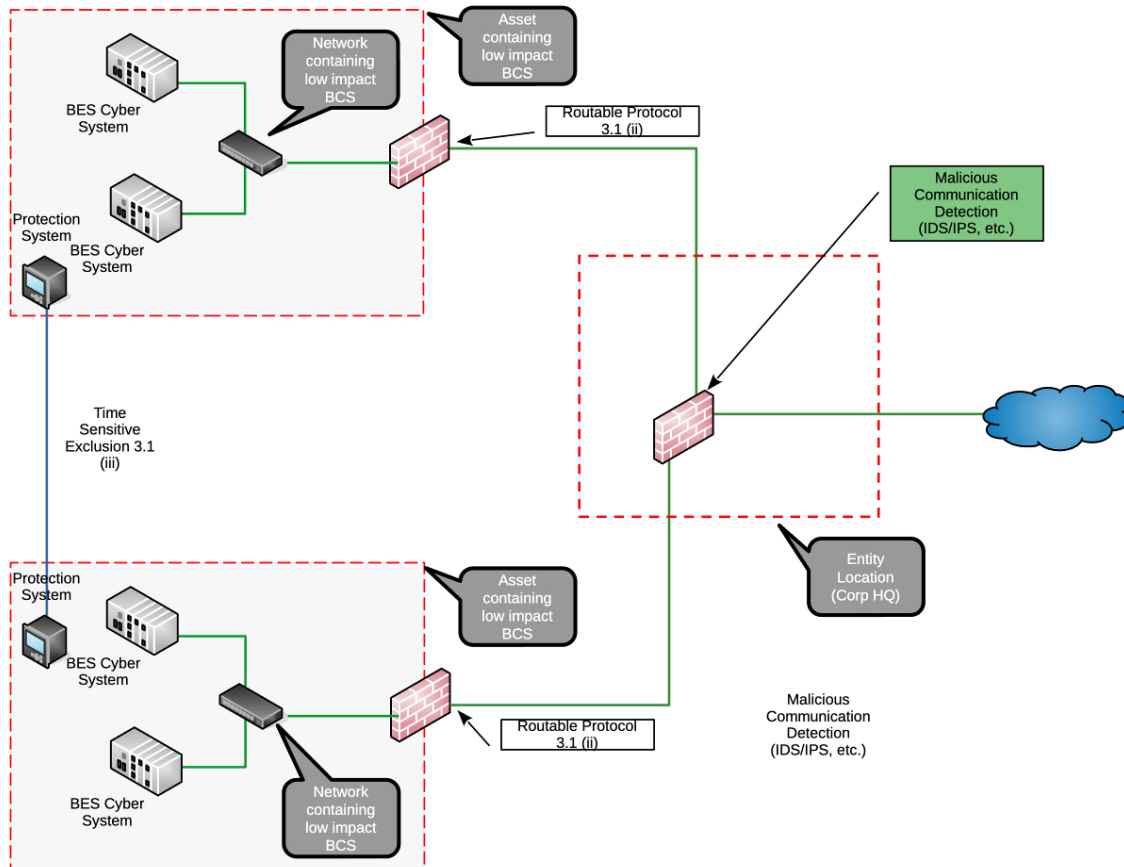
**3.1.5** Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

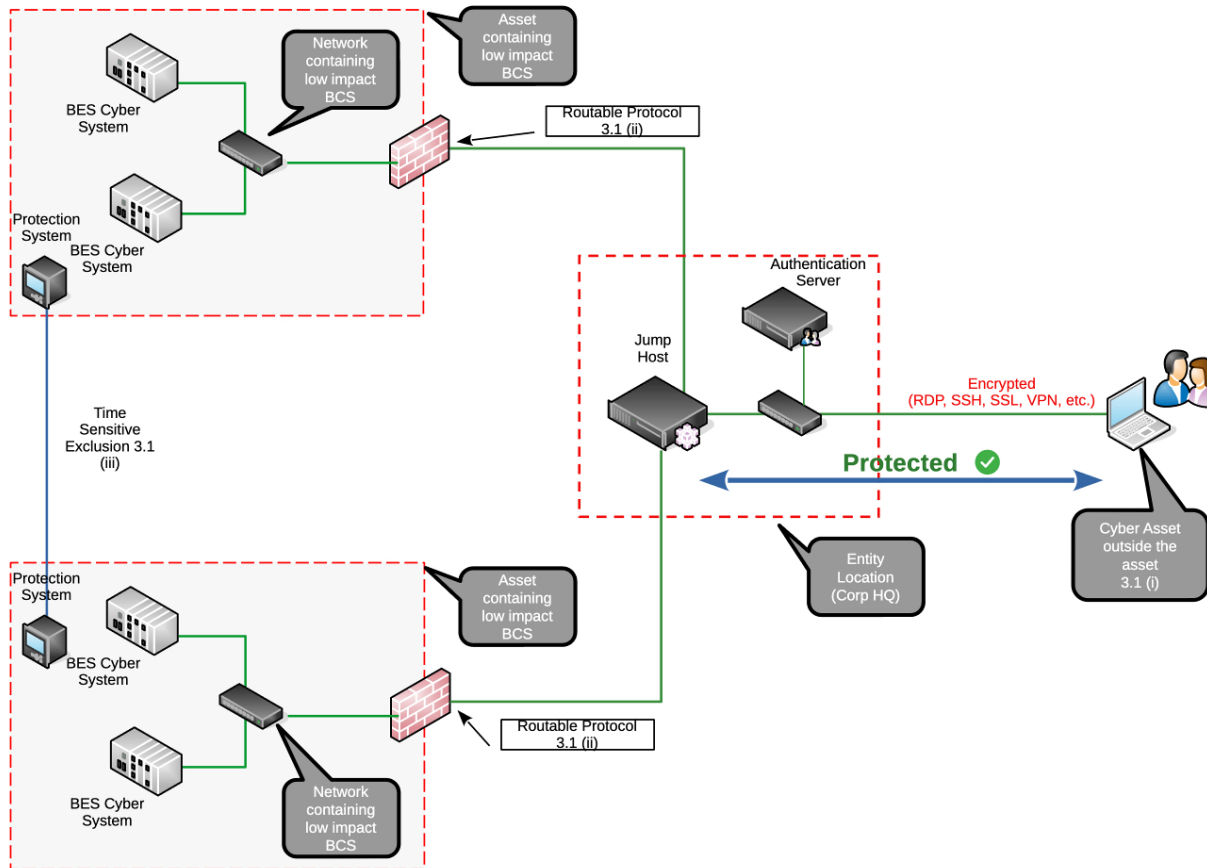
**3.1.6** Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

**3.2** For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement a control(s) that authenticates all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

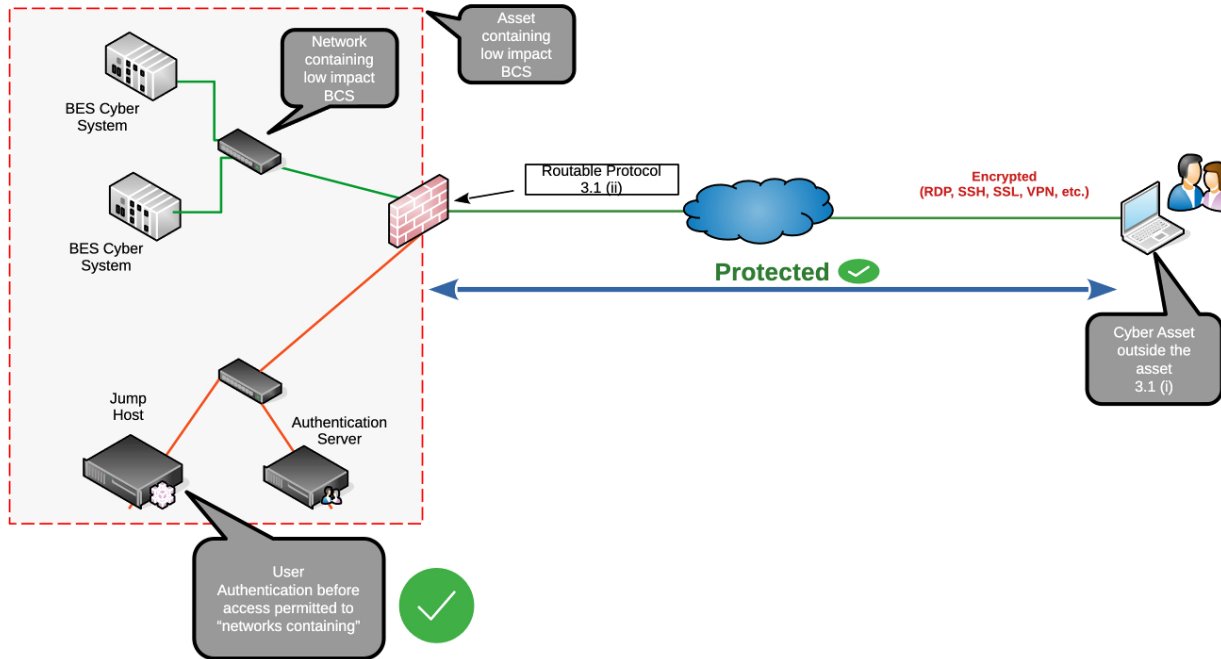
# 3.1 Electronic Access ("erc")



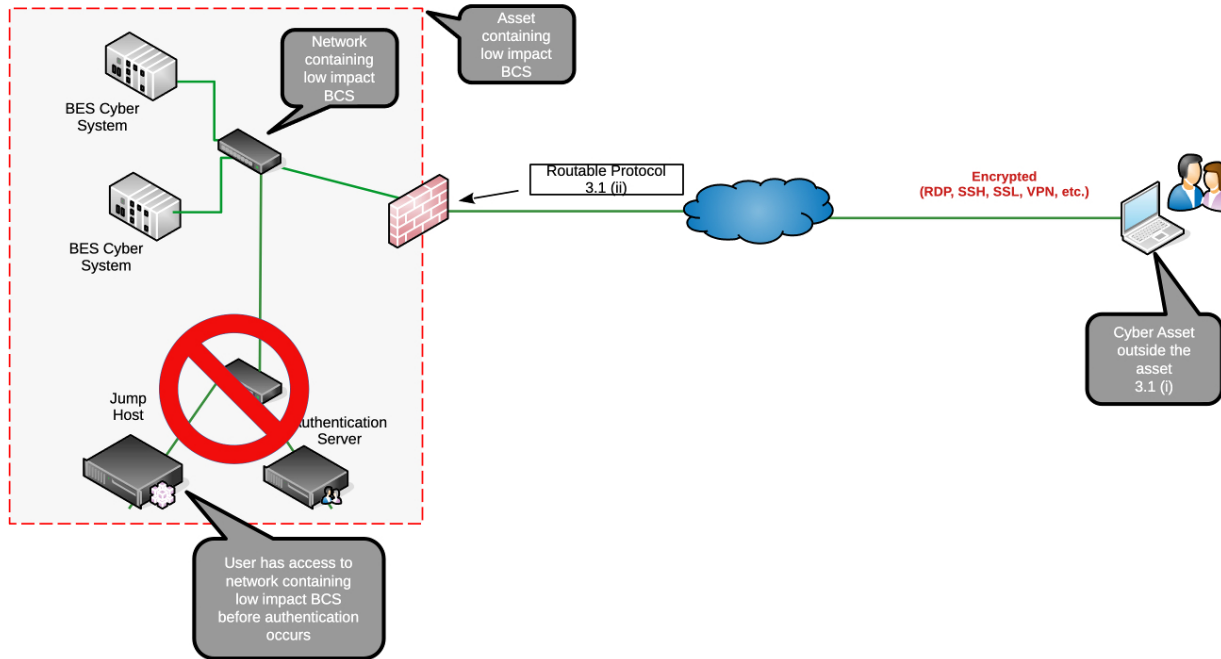




# 3.1.3/4 Auth in DMZ at Asset



# Auth NOT before access to network



- [Implementation Plan](#)
- Three (3) years from regulatory approval to be compliant with CIP-003-A
- Revise cyber security policy, plan, and procedures.
- Hire and train new staff to implement the new cyber security controls.
- Reconfigure system, network, or security architectures.
- Purchase and procurement of new technology(s).
- ~~Install new technology(s) at all assets containing low impact BES Cyber Systems.~~
- The effective date of CIP-003-9 is April 1, 2026. CIP-003-A builds upon the implementation of CIP-003-9 for vendor remote access.

- Ballot pools formed through March 14, 8:00 p.m.
- Additional ballot for CIP-003-A and implementation plan, March 5-14, 8:00 p.m. Comment period opened Jan 30.
- CIP-003-10 revisions (2016-02) will eventually be merged with CIP-003-A based on the timing and results of respective ballots. Final ballot of CIP-003-A will likely include CIP-003-10 revisions (acronyms and Section 3.1 revisions).





# Questions and Answers

