NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard
CIP-003-11 – Low Impact BES Cyber Security Criteria Revisions

Introduction
This document is the technical rationale and justification for Reliability Standard CIP-003-11 and includes the rationale for changes in the current proposed version, as well as previous versions of the standard.

It is intended to provide stakeholders and the ERO Enterprise with an understanding of the revisions, technology, and technical concepts of Reliability Standard CIP-003-11. This is not a Reliability Standard and should not be considered mandatory and enforceable.

Background
In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, this includes the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts, representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems (LIBCS). In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommended actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT conclusions regarding LIBCS are as follows:

- Individually, LIBCS are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the LICRT does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
- LIBCS may introduce BES reliability risks of a higher impact where distributed LIBCS are used for a coordinated attack. The LICRT recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

The LICRT report recommendations are as follows:

- Requirement(s) for authentication of remote users before granting and subsequently gaining electronic access to networks containing LIBCS at assets containing those systems that have external routable connectivity.

- Requirement(s) for protection of user authentication information in transit for remote electronic access to LIBCS at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between assets containing LIBCS with external routable connectivity.

Rationale for Attachment 1, Section 3 and Section 6

The drafting team's (DT) review of the SAR and industry comment initiated a discussion about the placement of requirements within CIP-003-11. Attachment 1, Section 3 and Attachment 1, Section 6 were identified as ideal locations to integrate the requirements due to their focus on electronic access controls and vendor electronic remote access security controls. The DT investigated two options:

Option A: Modify Sections 3 and 6, integrating the requirements, but keeping the sections separate.
Option B: Merge Sections 3 and 6.

The DT agreed to Option B: Merge Sections 3 and 6. Merging Section 3 and Section 6 would present a single section for all electronic access with sub-sections providing additional requirements based on the type of access (vendor, dial-up, local, etc.). This allows entities to look in one place for all of the electronic access control requirements needed for their assets containing low impact systems, rather than having very similar, and in some cases, overlapping requirements in multiple places within the standard.

While merging Section 3 and 6, the DT made conforming changes to the language. The DT uses the phrase "implement controls" to replace "implement a process" or "implement one or more method(s)". The DT believes a "control" can include an operation, process, procedure, or technology as described in the examples of Attachment 2. Additionally, the word "remote" was removed from the phrase "electronic remote access" as the section now covers all electronic access as described in Section 3, Part 3.1, (i), (ii), and (iii) as those define more specifically the remote nature of the in-scope access.

To clarify scope of requirements for industry and regulators alike, the DT placed the requirements in Attachment 1 Section 3.1 into a logical "if, then" order to further clarify the three identifying low impact asset characteristics or conditions (romanettes i, ii, iii) when implementing controls.

Section 3.1

The objective of the modifications within Section 3.1 is to maintain the original language used in CIP-003-10, Section 3.1, Subsections (i) - (iii). There is one revision to 3.1(iii) replacing the previous language concerning "intelligent electronic devices" with reference to the existing glossary term "Protection Systems" which is a conforming change to the change made by Project 2016-02, CIP-003-10. Figure 1 provides a graphical representation of Section 3.1, Subsections (i)-(iii).

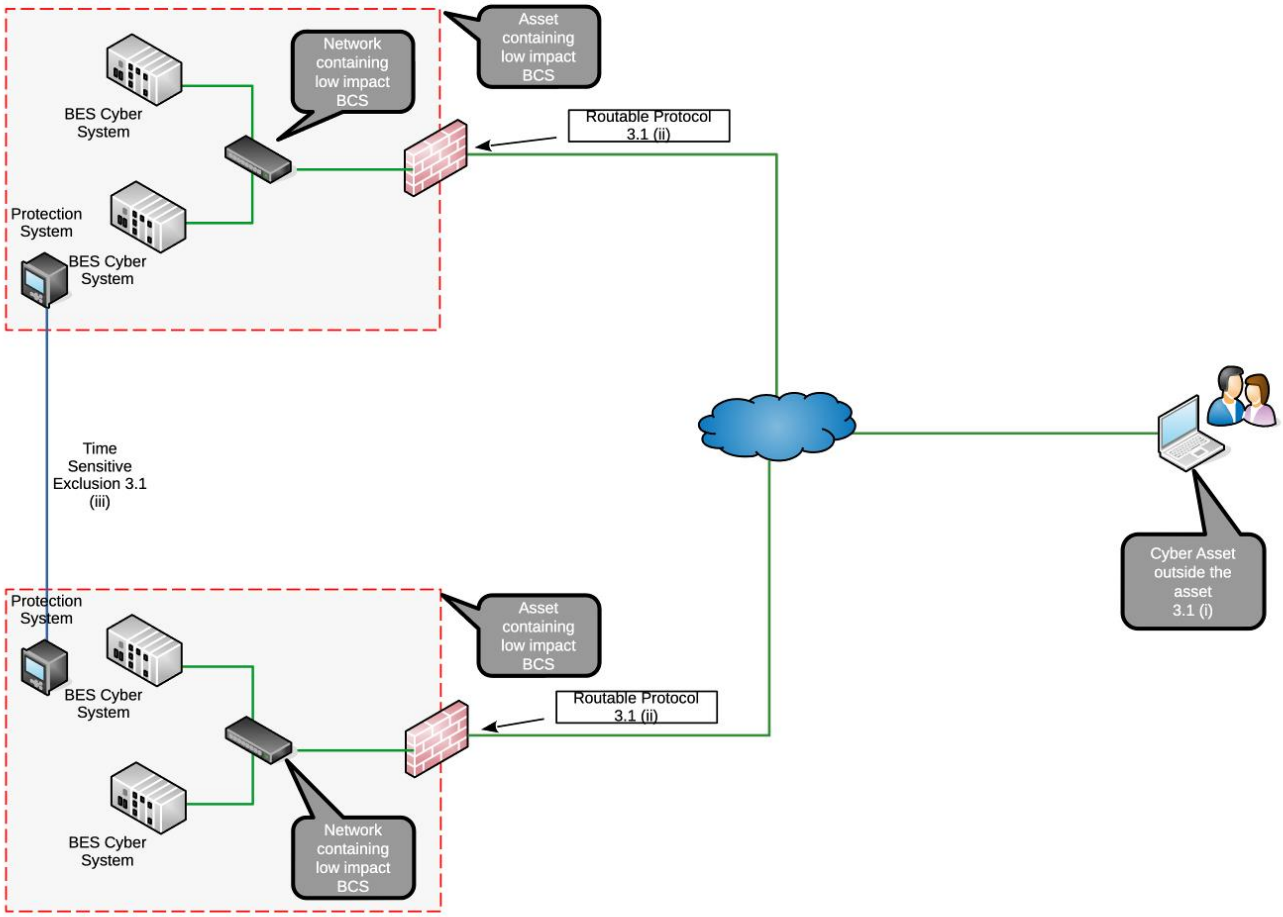

Figure 1

Section 3.1.1

The objective of Section 3.1.1 is to maintain the original language used in CIP-003-10, Section 3.1.

Section 3.1.2

This is an expanded cyber security control outlined in the SAR. The scope is expanded from CIP-003-10, Section 6.3 to include all communications rather than vendor specific communications. The objective of the modifications within Attachment 1 Section 3.1.2 is for entities to mitigate the risk posed by malicious communications to or from LIBCS. The detection of known or suspected malicious communications can be accomplished in several ways. For example, Figure 2 below depicts implementing the control (e.g., Intrusion Detection System (IDS)) in a centralized location (e.g., at a corporate hub site) rather than at every distributed "asset containing LIBCS" such as substations in this example "hub and spoke" model. The obligation in Section 3.1.2 requires that entities implement controls to detect known or suspected inbound and outbound malicious communications between a low impact BES Cyber System and a Cyber

Asset(s) outside the asset containing low impact BES Cyber System(s) thus allowing entity flexibility in where the control is implemented based on their architecture.

The DT considered entities that may use encryption to protect communications between hosts and the impact to the ability to detect known or suspected malicious communications. Because of the differences in entity programs, architectures, technologies and processes, the DT did not prescribe that encrypted communications must be decrypted for deep packet inspection when detecting known or suspected malicious communication. Requiring decryption/inspection/re-encryption may in some cases increase risk through introducing single points of failure or jeopardizing sensitive timing of communications. Entities may detect known or suspected malicious communications through other methods, such as detecting the appearance of abnormal new destination addresses or ports. The DT provided several other examples in Attachment 2. Entities may also choose to perform detection before or after the encryption tunnel occurs.

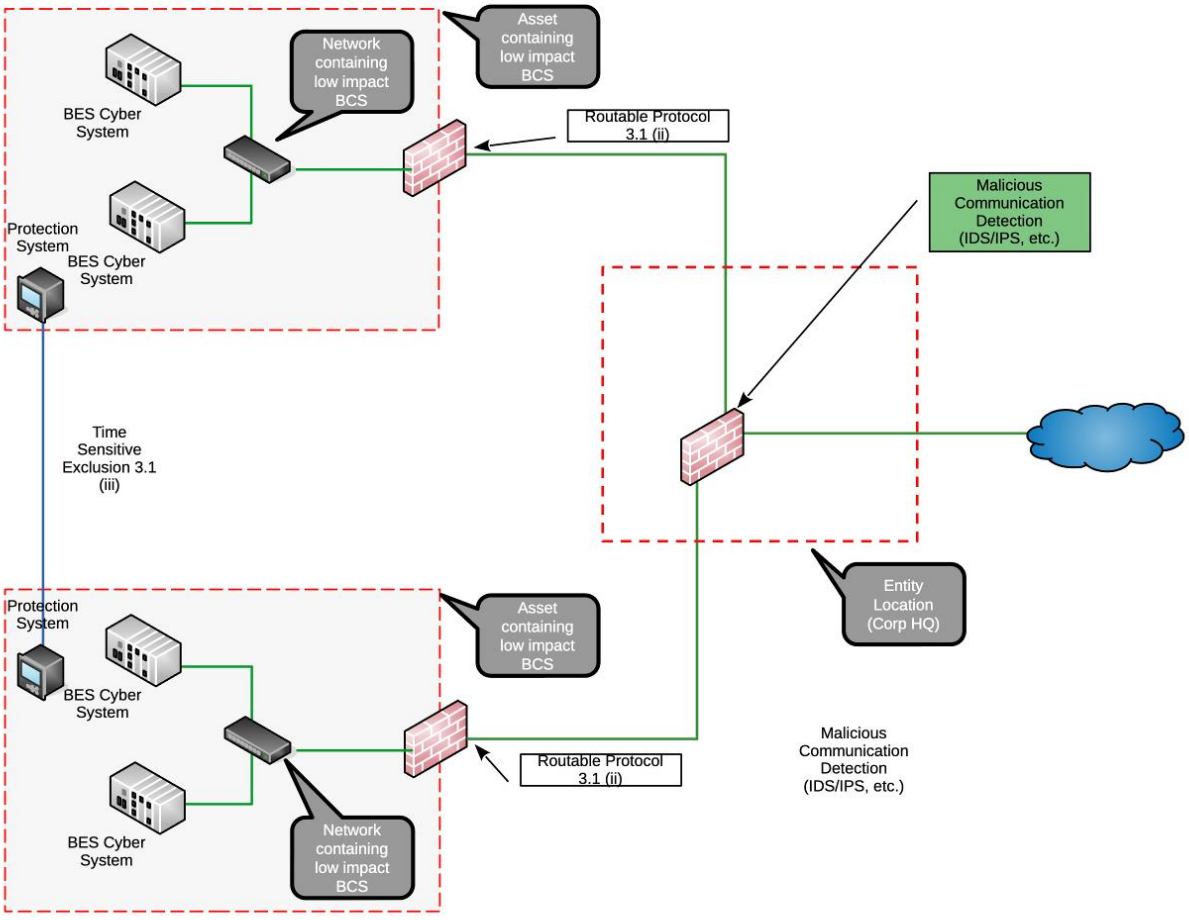

Figure 2

Section 3.1.3

This is a new cyber security control outlined in the SAR that requires entities to implement controls to authenticate users prior to permitting access to networks containing LIBCS. This control mitigates the risk of unauthenticated access to networks on which LIBCS reside. The intent is for each user to be authenticated (verifying a user) *before* they gain access to the "network containing low impact BES Cyber Systems"; thus, they have no ability to enumerate hosts on those networks, scan those networks for vulnerabilities, attempt logons to systems, or perform actions on those networks and systems before the entity has authenticated their user-initiated electronic access. It is important to note that Section 3.1.3 is not applicable to electronic access which sources (is connected) to the LIBCS network. For example, a laptop connected via an Ethernet cable to the LIBCS network would not be required to authenticate prior to accessing the LIBCS to which it is being connected. It is also important to note that the DT did not address specific account types (user or shared) used for authentication. While the intent is for entities to control each user prior to permitting electronic access, the SAR did not prescribe account types or passwords used by users to obtain (via authentication) electronic access. There are multiple methods to authenticate users for the responsible entity to choose.

Figure 3, below, depicts a situation where the authentication of the remote user is not occurring "prior to" but after the user already has access to the "network containing LIBCS" — as the authentication servers are on the same network with the LIBCS. The firewall in this scenario allows the user through to the network on which the LIBCS reside before the user is authenticated, and this does not meet the intent of the requirement.

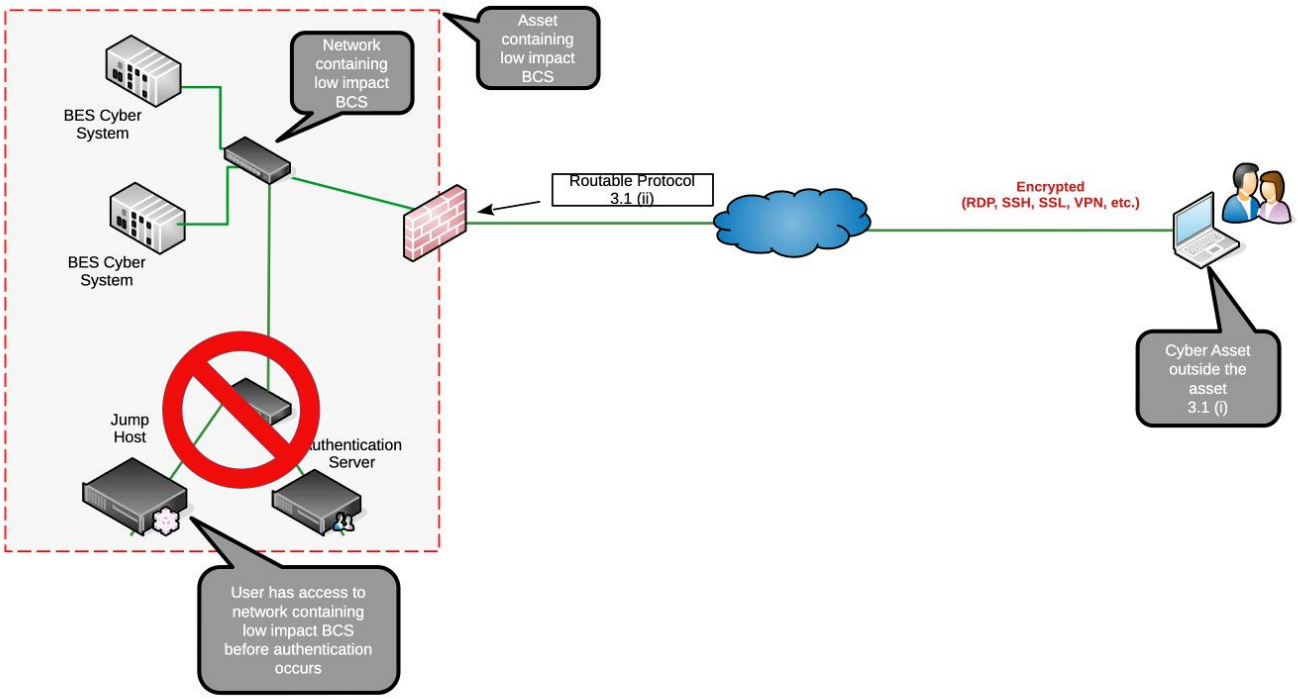

Figure 3

The intention of the phrase "each user prior to permitting access to a network(s)…" is meant to include the initial authentication and not all subsequent access to other downstream networks. If there is a collection of sub-networks or Cyber Assets within the network containing LIBCS, then multiple re-authentications at those levels would not be required by this specific requirement. Regardless of how many subsequent networks or BES Cyber Systems a user may access, as long as the entity's implemented control(s) have authenticated the user prior to their access to those subsequent networks, that meets the intent. This may include, but is not limited to, configurations where authentication is local device specific authentication or configurations consisting of centralized authentication using technologies such as an access, terminal, or proxy server ("Intermediate System") which processes authentication to the low impact asset networks through a centralized gateway.

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those entities who have established or implemented such infrastructure or technologies may use them for authenticating access

to the assets containing low impact BES Cyber Systems to satisfy these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would further clarify CIP-003's requirements, the DT has chosen not to prescribe such requirements due to the impact to a broad and diverse range of entities and their specific technologies and processes used to meet low impact BES Cyber Systems authentication requirements. For example, it would be excessive to require an entity with a single CIP-003 applicable renewable generation site to implement architectures and technologies (Intermediate Systems) to meet the CIP-005 Requirement R2 Interactive Remote Access requirements. Such an entity may only need a Secure Sockets Layer (SSL) Virtual Private Network (VPN) to an access control device (e.g., firewall) at the one site that authenticates the user prior to allowing access to the network containing low impact BES Cyber Systems on its inside interface. The entity may also choose to authenticate a local non-low impact BES Cyber Systems network first, then control access to the LIBCS from that access point. Conversely, an entity with many assets distributed over a large geographic area, with a variety of impact categorizations and supporting BES Cyber Systems, may want to use their existing CIP-005 Requirement R2 remote access solutions for all of their sites (centralized access controls). The DT's intent in the CIP-003 language is to allow flexibility for both cases.

The phrase, "through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted" is included in Section 3.1.3 to clarify scoping. As Section 3.1.3 is written at a different granularity of "network(s) containing", which is not mentioned in the romanettes, this phrasing simply clarifies that the intended scope remains those networks through which the specific access described in the Section 3.1 romanettes is subsequently permitted. The romanettes (i), (ii), and (iii) in Section 3.1 define the ultimate access that is in scope, which is from a remote client outside the asset containing the LIBCS and destined for a LIBCS within the asset.

Section 3.1.4

This is a new cyber security control outlined in the SAR. The objective of Attachment 1, Section 3.1.4 is for entities to protect the user authentication information (e.g., username, password, multi-factor authentication (MFA) information, session token, etc.) while in transit between the remote user's Cyber Asset and either the asset containing the low impact BES Cyber Systems or the entity's authentication system used to meet Section 3.1.3. This mitigates the risk of user authentication information being captured, especially as some BES equipment may still require protocols that transmit such information in clear text. The intent is not to specify authentication directly to a particular device but to allow entities that desire to use an existing compliant CIP-005 Requirement R2 Intermediate System, or similar architecture, access to networks containing LIBCS (Figure 4). For example, Figure 4 below depicts protection of the user authentication information to the asset containing a LIBCS.

Figure 5 depicts an alternative example of protecting the user authentication information to/from a central system (i.e. jump host) *before* accessing a network containing a LIBCS. This protection mitigates the unintended disclosure of authentication information for electronic access to low impact cyber systems.

Note that both Figure 4 and Figure 5 have a significant difference from Figure 3 above in that, although the authentication services are also within the asset containing the LIBCS, they are located on a separate network from those containing BES Cyber Systems. In this example, assuming the firewall is configured to only allow authenticated user sessions on the jump host through to the network containing the LIBCS, this would meet the intent of the Section 3.1.3.

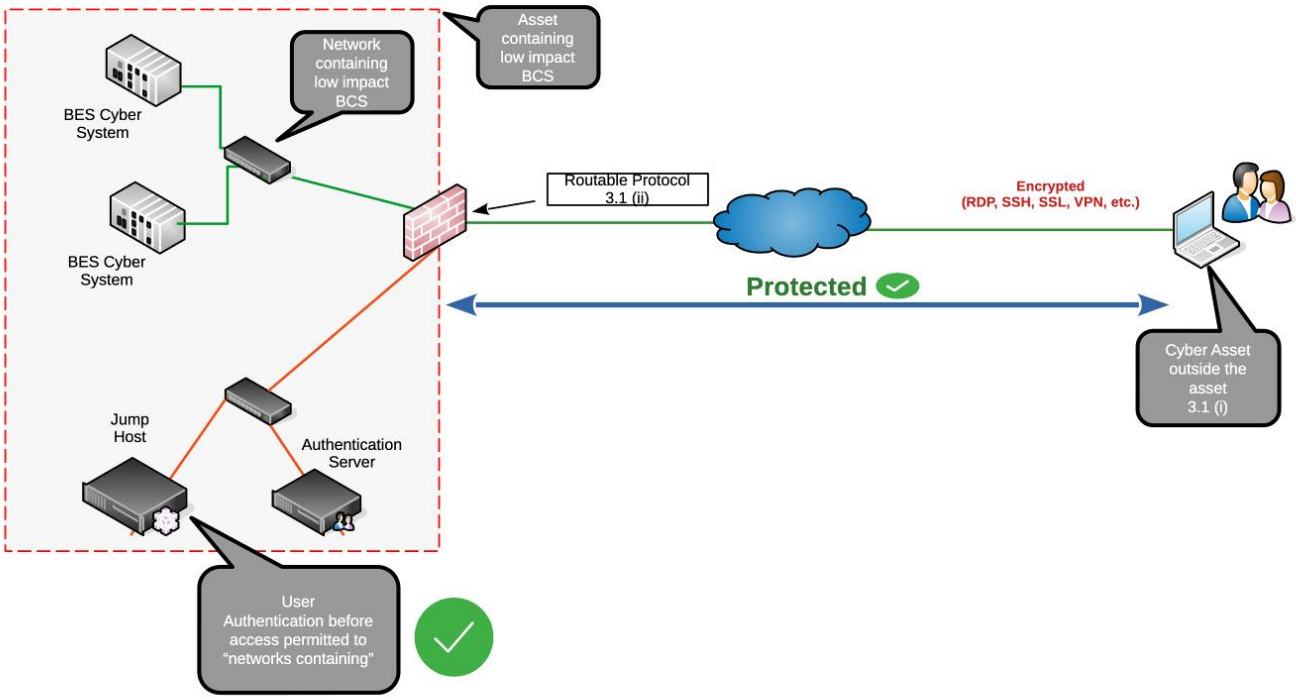

Figure 4

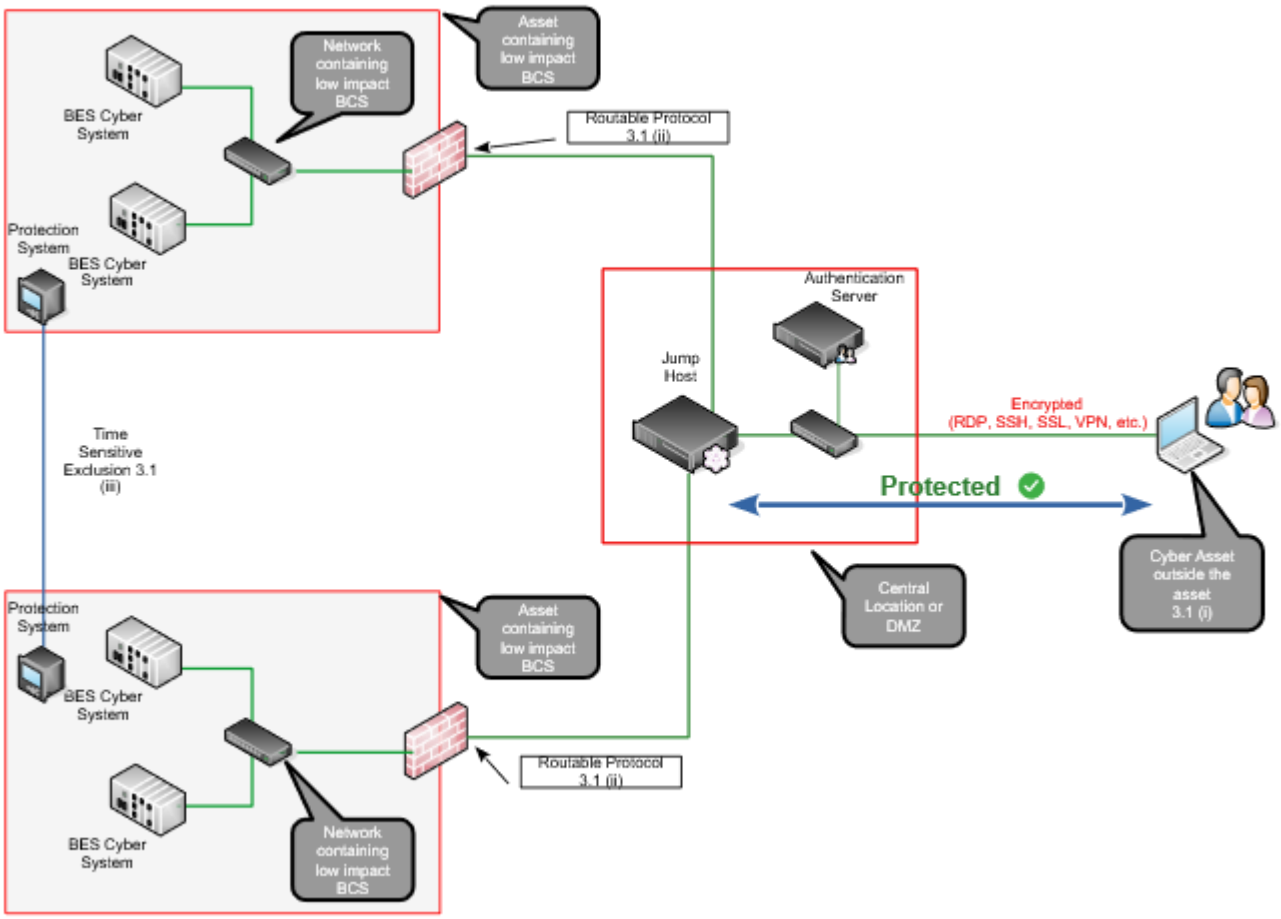

Figure 5

The DT has not required the use of an "Intermediate System" as is prescribed in CIP-005 Requirement R2 for high and medium impact BES Cyber Systems. However, the DT's intent is that those who have such infrastructures in place can, if they choose, use them for access to the assets containing low impact BES Cyber Systems to satisfy the intent of these requirements. While prescribing such an architecture as in CIP-005 Requirement R2 would make the target of CIP-003's requirements clearer to describe, the DT has chosen not to be this prescriptive due to the wide diversity of entities that may have only LIBCS. For example, an entity may have one small renewable generation site that falls under CIP-003 and implementing a full CIP-005 Requirement R2 "Interactive Remote Access with Intermediate System" architecture for access to one site may be excessive. That entity may only need an SSL VPN to an access control device (e.g., firewall) at the one site that authenticates the user and then allows access to the network containing LIBCS on its inside interface. However, an entity with 100 assets with BES Cyber Systems of varying impact categorization over a large geographic area may want to use their CIP-005 Requirement R2 remote access solution for all of their sites. The DT's intent in the CIP-003 language is to allow flexibility for both.

Section 3.1.5

The objective of Section 3.1.5 is to maintain the original language used in CIP-003-10, Section 6.1. One or more method(s) can be identified as part of this electronic access control. Entities must determine vendor electronic remote access, where permitted, to their LIBCS. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access.

Section 3.1.6

The objective of Section 3.1.6 is to maintain the original language used in CIP-003-10, Section 6.2. One or more method(s) can be identified as part of this electronic access control. Entities must have the ability to disable vendor electronic remote access, where permitted, for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing LIBCS.

Section 3.2

The DT made conforming changes to Section 3.2 with the objective to maintain the original intent of CIP-003-10, Section 3.2.

Special Scenarios

One low impact BES Cyber System across more than one asset containing that system.
In this scenario, a low impact BES Cyber System is not entirely located within one asset. For example, a generation resource has the majority of its BES Cyber System components within the site, but its network is extended full-time (e.g., over a dedicated circuit or dedicated VPN) to an operator console located at another site, and the console is part of the single BES Cyber System.

Since the components of the BES Cyber System are all located in "assets containing low impact BES Cyber System", just not a single asset, then this scenario is not in scope as it does not meet the condition of Section 3.1(i) of "between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber System(s)." The intent of Section 3.1.3 is authentication of users who are not located within any other "assets containing low impact BES Cyber System." This keeps CIP-003 analogous to the same concept in CIP-005 and the Interactive Remote Access definition that excludes from Interactive Remote Access user access that originates in another of the entity's Electronic Security Perimeters, such that operators in Control Centers are not required to implement CIP-005 Requirement R2 controls such as Intermediate Systems to operate field assets. It also avoids CIP-003 becoming circular when a local user at the BES Cyber System console would need to authenticate prior to permitting access to the extended network they are already on while seated at the console.

Rationale for Attachment 2

The DT made conforming changes to Attachment 2 merging Sections 3 and 6 and provided examples of compliance related activities.

Previous CIP-003 Versions Technical Rationale

Project 2020-03 Supply Chain Low Impact Revisions (CIP-003-9) Technical Rationale
Project 2016-02 Modifications to CIP Standards (CIP-003-10) Technical Rationale