NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Low Impact Criteria Review Report

NERC Low Impact Criteria Review Team White Paper

_____ 2022

DRAFT

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

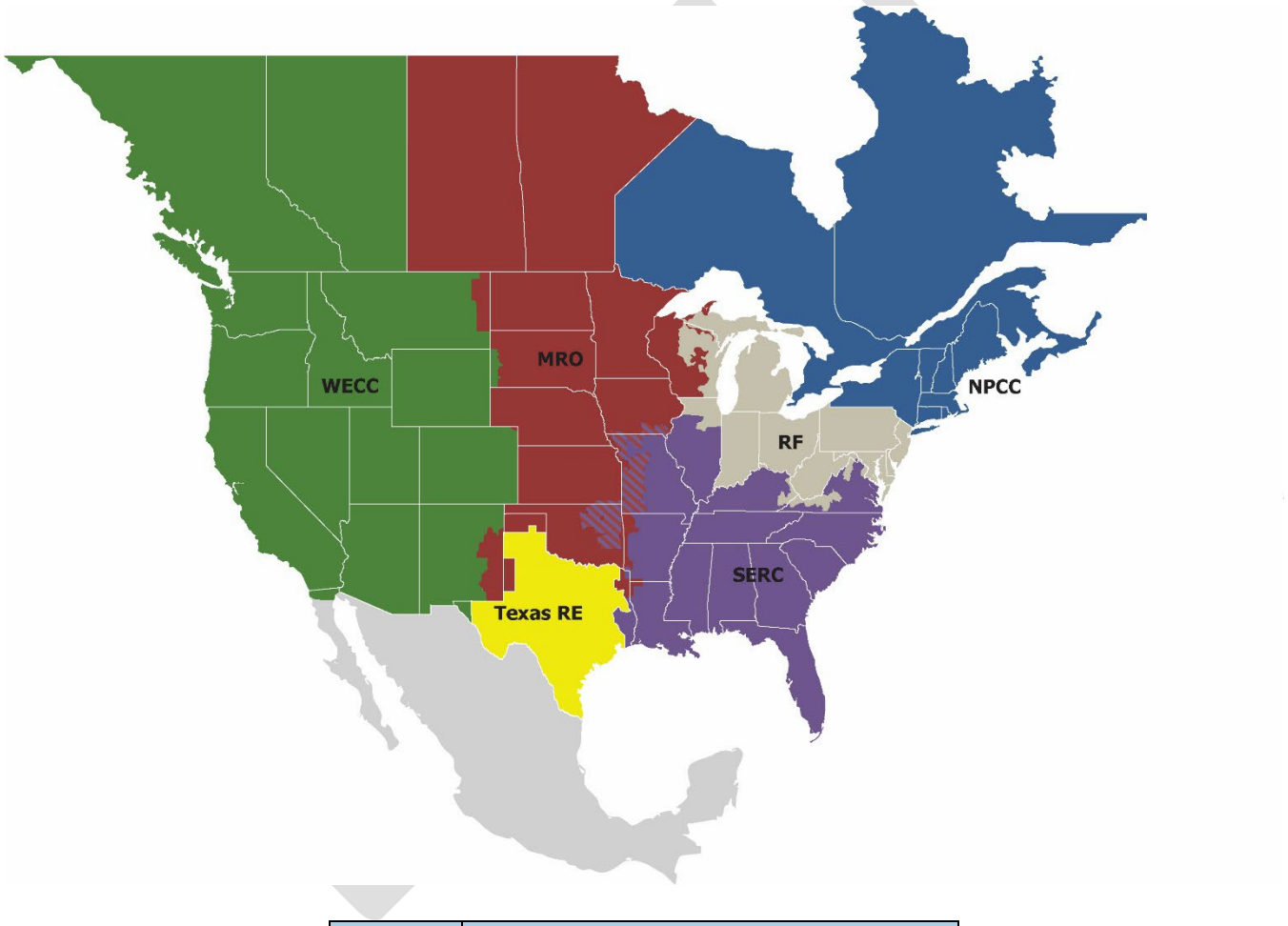
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Communications, information technology, and industrial control systems provide various opportunities for adversaries to initiate a coordinated cyberattack, thereby presenting Bulk Electric System (BES) security risk. NERC is committed to using reliability tools to support industry's efforts to mitigate these coordinated cyberattacks risks.

In 2017, NERC developed new and revised critical infrastructure protection (CIP) Reliability Standards to help mitigate cybersecurity risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards are applicable to systems that pose the greatest BES impact. To fully understand these Supply Chain risks, NERC collected registered entity data pursuant to NERC Rules of Procedure Section 1600 request for data or information.

NERC staff's analysis of the data shows that, while an individual compromise to any one low impact BES Cyber Asset facility would generally be a localized event, a coordinated cyberattack with control of multiple facilities may result in an interconnection wide BES event. The vast majority of transmission station and substation low impact BES Cyber Assets are at facilities that have at most only one line greater than 300 kV or two lines greater than 200 kV (but less than 300 kV). Similarly, the vast majority of generation resource low impact BES Cyber Assets are at facilities that have less than 500 MW. As such, an individual compromise to any one of these locations (transmission substations or generation resources) would generally be a localized event. However, a coordinated cyberattack with control of multiple facilities may result in an interconnection wide BES event.

On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, publicly posted details about an attack on certain software developed by SolarWinds Orion. Underscoring the severity of the event, on December 13, 2020, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, which required Federal agencies to take action based on the DHS assessment that a successful compromise from the SolarWinds attack would have "grave" consequences.

In light of these recent 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 BES Cyber Assets. Specifically, 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. In this report, the LICRT documents 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 recommends actions to address those risks.

The LICRT conclusions regarding low impact BES Cyber Systems are as follows:

- Individually, low impact BES Cyber Systems 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 team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems.
    - The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.

Those recommendations, sorted by category, are as follows:

CIP Standards 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 (e.g. combinations of usernames and passwords) 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 low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

Security Guidelines

- Develop best practice guidance documents for protection of communications to and between low impact BES Cyber Systems across publicly accessible networks.
- Develop best practice guidance documents for procurement risk evaluation for low impact BES Cyber Systems.
- Develop best practice guidance documents for entities to voluntarily submit an E-ISAC report for unauthorized physical access attempts to low impact BES Cyber Systems.

Risk Monitoring

- Continuous monitoring of E-ISAC physical access attempt reports to low impact BES Cyber Systems to determine if the risk increases over time and should be addressed.

Introduction

In 2017, NERC developed new and revised CIP Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards are applicable to the highest-risk systems that have the greatest impact to the grid. When adopting the Supply Chain Standards in August 2017, the NERC Board directed NERC to undertake further action on supply chain issues. Among other things, the Board directed NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards and develop recommendations for follow-up actions that will best address identified risks. To understand these risks better, NERC collected data from registered entities pursuant to a request for data or information under Section 1600 of the NERC Rules of Procedure.

NERC staff's analysis of the data collected[1] showed that, while an individual compromise to any one low impact BES Cyber Asset facility would generally be a localized event, a coordinated cyberattack with control of multiple facilities could result in an event that has an interconnection wide BES reliability impact. The vast majority of transmission station and substation low impact BES Cyber Assets are at locations that have at most only one line greater than 300 kV or two lines greater than 200 kV (but less than 300 kV). Similarly, the vast majority of generation resource low impact BES Cyber Assets are at facilities that have less than 500 MW. As such, an individual compromise to any one of these facilities (transmission substations or generation resources) would generally be a localized event. However, a coordinated cyberattack with control of multiple facilities could result in an event that has an interconnection wide BES reliability impact.

Based on the analysis of the data request, NERC staff recommended to the NERC Board at its February 6, 2020 meeting that Reliability Standard CIP-003-8 be modified to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary. The NERC Board approved a resolution at this meeting endorsing this action.

On May 14, 2020, the NERC Board of Trustees (Board) adopted proposed Reliability Standard CIP-002-6. The proposed Reliability Standard CIP-002-6 addressed the recommendation from the Version 5 Transition Advisory Group to clarify the phrase "used to perform the functional obligations of the Transmission Operator (TOP)" in CIP-002-5.1a, Attachment 1, Criterion 2.12.

Specifically, the proposed Reliability Standard CIP-002-6 addressed the applicability of requirements to a Control Center owned by a Transmission Owner (TO) that performs the functional obligations of a TOP. The proposed criterion established an average MVA line loading based on voltage class for BES Transmission Lines operated between 100 and 499 kV. The aggregate weighted value of the BES Transmission Lines must exceed 6,000 to meet the minimum threshold established in Criterion 2.12. In meeting that threshold, associated BES Cyber Systems would be categorized as medium; those Control Centers that did not meet the threshold would have low impact BES Cyber Systems (if not already identified as high).

On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, publicly posted details about an attack on certain software developed by SolarWinds Orion. For victims, this attack was particularly damaging because in order to function SolarWinds must have broad and privileged access to the networks it manages, including both the corporate and operational networks of an entity. The breach provided the opportunity for an adversary to monitor network traffic and compromise systems, which could result in disruption of their operations.

[1] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply%20Chain%20Risk%20Assesment%20Report.pdf

Underscoring the severity of the event, on December 13, 2020, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, which required Federal agencies to take action based on the DHS assessment that a successful compromise from the SolarWinds attack would have "grave" consequences. On December 15, 2020, the White House National Security Council (NSC) established a Cyber Unified Coordination Group (UCG) composed of multiple Federal agencies to coordinate the investigation and remediation of the "significant" cyber incident. On December 17, 2020, CISA issued Alert AA20-352A, directed toward the private sector, which described the attack for industry, the affected products, and the mitigation recommendations.

In response, the Federal Energy Regulatory Commission (FERC) staff and the NERC Electricity Information and Analysis Sharing Center (EISAC) jointly prepared a white paper[2], emphasizing the need for continued vigilance by the electricity industry related to supply chain compromises and incidents and recommends specific cybersecurity mitigation actions to better ensure the security of the bulk-power system (BPS). While focusing primarily on the ongoing cyber event related to the SolarWinds Orion platform and related Microsoft's 365/Azure Cloud compromise, it also addresses related compromises in products such as Pulse Connect Secure. Two additional examples of compromises, Microsoft's on-premise Exchange servers, and F5's BIG-IP are discussed to illustrate continued adversary interest and exploitation of ubiquitous software systems.

Because of SolarWinds' wide use and the adversarial tactics used, even entities that did not install SolarWinds on their networks could still be impacted. For example, the indicators of compromise (IOCs) have been found on networks without SolarWinds. In addition, although SolarWinds may not have been used by entities, their key suppliers may use the product. Should the suppliers be compromised, the supplier in turn could compromise their customers, including those without SolarWinds. In fact, there is evidence technology firms were targeted for this reason.

In light of these recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to withdraw CIP-002-6. In doing so, they approved a resolution to withdraw CIP-002-6 and directed NERC Staff, working with stakeholders, recognizing the complexity of the undertaking, to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and report on whether those criteria should be modified.

[2] https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds and Related Supply Chain Compromise White Paper.pdf

Chapter 1: BES Cyber Systems and Impact Ratings

This chapter provides an overview of the identification and categorization of relevant cyber systems within the North American Bulk Electric System. It describes the history and the current state of this process within the NERC CIP standards and the rationale for the current state, including specific discussion on the low impact category within the NERC CIP standards and the protections required today for the low impact BES Cyber Systems.

BES Cyber System Identification & Impact Categorization

In the NERC CIP standards (specifically CIP-002) from Version 1 to Version 3, entities were required to have their own risk assessment methodology that identified Critical Assets and their supporting Critical Cyber Assets. As is the term 'critical', this categorization was binary in nature; cyber assets were either critical and fully in-scope or non-critical and thus fully out of scope of the standards and their cyber security requirements. Subsequent to FERC Order 706, the CIP standards underwent a large transition leading up to Version 5 that consisted of two foundational changes:

- A transition to a single set of risk-based criteria for all entities to use to identify and categorize their cyber systems that could impact the Bulk Electric System (defined as BES Cyber Systems that consist of BES Cyber Assets , a subset of Cyber Assets)
- The concept that **every** BES Cyber System requires a base level of cyber security protection.

With this transition, the scope of cyber assets under the NERC CIP standards exploded from a smaller number of Critical Cyber Assets to literally millions of BES Cyber Assets across all entities in the North American BES. With a core defining characteristic of "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment…", the scope of cyber assets covered by the CIP standards increased exponentially.

With this large increase in scope for Version 5, the CIP-002 standard borrowed a concept from the NIST Risk Management Framework and transitioned to a graduated and risk-based approach with the introduction of graduated impact categories: High, Medium, and Low impact. These categories were created in recognition of the fact that every BES Cyber System does not present the same level of risk to the BES. Within the Version 5 CIP-002 standard, Attachment 1 was created that presented a set of defined criteria by which all BES Cyber Systems are categorized into the high, medium, or low impact categories (Appendix C contains the complete impact rating criteria from CIP-002-5.1a). At a very high level, these risk-based impact categories consist of:

- **High impact** – BES Cyber Systems associated with Control Centers that have a large span of control of BES assets
- **Medium impact** – BES Cyber Systems associated with:
  - Larger field assets, such as the more impactful generation resources and Transmission substations that contain 500kV or above 'backbone' Transmission lines or larger 'hub' sites for many Transmission lines
  - Control Centers with a smaller span of control of BES assets
- **Low impact** – Every other BES Cyber System in the Bulk Electric System associated with all other BES Control Centers, transmission resources, and generation resources.

The CIP-002 standard also assigns these impact ratings not to the BES assets themselves (Control Centers, transmission resources, generation resources, etc.) but only to BES Cyber Systems. This recognizes that not every BES Cyber System in an asset is of the same risk or potential impact and a BES Cyber System should be protected at a level commensurate with the risk presented by that cyber system, not simply inherited from the asset it supports. For example, a Transmission substation may have many digital relays within its boundary. Some may be protecting and controlling 500kV major backbone Transmission lines and be of medium impact to the BES, others may be

protecting and controlling a single 100kV line and are of low impact to the BES. The lower impact relay does not inherit a higher impact rating simply due to its proximity to a higher impact BES Cyber System . Within a generation resource, a BES Cyber System that can trip 1500MW or more of generation is a medium impact system, but a system controlling an individual 20MW generator, although it may be located at the same plant site, would be low impact. Therefore, the CIP-002 standard requires the identification of all BES Cyber Systems but then categorizes each one according to that cyber system's potential impact to the BES. Those that do not fall into the high or medium impact categories default to the low impact category, with the result being that every BES Cyber System receives cyber security protections in a risk-based manner.

This generation example shows how the CIP-002 impact rating criteria alone can incentivize beneficial security changes in the Bulk Electric System. A primary example is Criterion 2.1 from CIP-002 Attachment 1 that requires any "shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection" to be categorized as medium impact. This criterion was established to recognize the elevated risk of a BES Cyber System at a generation resource that could impact enough generation to challenge the average Contingency Reserve that Balancing Authorities are required to maintain per the NERC BAL-002 Disturbance Control standard. This criterion caused entities to evaluate the architectures of their BES Cyber Systems and networks within their generating plants to determine their potential impact. For example, a generating plant with two 800MW units with control system(s) on a single, flat control network or that controlled critical processes on both units could mean that an issue on that BES Cyber System may impact both units, turning a potential 800MW impact into a 1600MW impact. The sudden loss of 1600MW would be greater than the 1500MW threshold representing an average Balancing Authority's Contingency Reserve and rise to a medium impact to the BES. Therefore, due to this criterion in CIP-002, entities across the BES analyzed their architectures and many, upon discovering any such systems, decided to not simply accept that higher level of risk and impact, but to implement projects to rearchitect and segment systems and networks to reduce the potential impact and risk. This criterion resulted in entities taking action to reduce the attack surface and limit the scope of impact of BES Cyber Systems through cyber security practices of good network and system segmentation as the CIP-002 analysis highlighted a higher than necessary risk in their environment.

Low Impact BES Cyber Systems

In recognition of the vast scope of BES Cyber Systems across the North American Bulk Electric System, the CIP standards treat the impact categories differently and in particular the individual cyber assets that make up the low impact BES Cyber Systems. Those BES Cyber Systems with a high or medium impact are treated individually and for some requirements (e.g., security patching) at an individual BES Cyber Asset level. However, identifying and protecting every individual low impact BES Cyber Asset at every BES asset would, due to its scale, dilute focus, and resources away from the higher impact systems. The reason the CIP standards have an "all-in" nature is so that every BES Cyber Asset receives a base level of protection, but we identify and protect at a much higher level those BES Cyber Systems that present a much greater level of risk due to their span of control or impact to the BES.

Therefore, the CIP standards treat the low impact BES Cyber Systems at the level of an "asset containing low impact BES Cyber Systems." This allows for all the low impact BES Cyber Systems to have cyber security requirements applied to them, but at a manageable level grouped by the asset or site. For example, cyber security protections for electronic access to any BES Cyber System can be applied at a site level and thus inherited for all the individual BES Cyber Systems within the site. This is a manageable way to provide base level protections against every BES Cyber System in the Bulk Electric System while focusing efforts on the higher risk, higher level targets of those systems with larger span of control and a much higher level of impact if compromised. As the saying goes, "a focus on everything is a focus on nothing," and CIP-002 incorporates that philosophy.

Low Impact BES Cyber System Cyber Security Requirements

With the philosophy of protecting the myriad individual and lower-risk BES Cyber Systems at a site or asset level, the CIP standards (in this case CIP-003 for low impact BES Cyber Systems) requires both cyber security policies and detailed cyber security plans that cover every low impact BES Cyber System at a BES asset level.

With the incredible scale and diversity of low impact BES Cyber Assets across Control Centers, substations, and generation resources of all types, the idea of having a base cyber security plan with required sections to mitigate high level risk areas rather than prescriptive device-level requirements is a manageable way for all entities to document how they meet the cyber security objectives for the assets containing low impact BES Cyber Systems.

The required cyber security plans that provide a base level of protection for every BES Cyber System must include (as of the date of this paper) sections concerning five areas of risk that cover the main areas of people, process, and technology. These five areas and the rationale behind each are:

- **Cyber Security Awareness** – A core part of cyber security is the people aspect; those who use or maintain such systems and their actions. The cyber security plans, therefore, require a cyber security awareness program that reinforces good security practices.
- **Physical Security Controls** – Another core part of cyber security is protecting physical access to the cyber systems. As has been said, physical access control to a cyber system is vital as many electronic security controls can be overridden if an attacker gains physical access to the system. Therefore, the CIP standards have required that physical access be controlled based on need either (or both) at an asset level or to locations of low impact BES Cyber Systems within the asset, as well as specifically to any cyber assets that control electronic access to the asset (e.g., firewalls protecting external access to the BES Cyber Systems).
- **Electronic Access Control**s – One of the primary risks facing low impact BES Cyber Systems (or any BES Cyber System) is electronic remote access from outside of the asset containing the systems. With the rise of Internet search engines devoted to finding publicly-accessible industrial equipment and control systems, the CIP standards incorporated this section to require the implementation of electronic access controls that permit only needed inbound and outbound routable protocol electronic access to the asset containing lows (and thus all individual low impact systems) from anything outside of the asset; in other words, all remote access must be controlled and limited to only what is necessary. In like manner, any dial-up connectivity must also authenticate the remote client and not provide unauthenticated access to anyone with the correct phone number. With this covering every BES Cyber System in the North American BES, this requirement for electronic access controls has reduced an enormous amount of risk.
- **Cyber Security Incident Response** – While other sections of the entity's cyber security plan have been in the realm of prevent, this section of the plan deals with the "detect, respond, and recover" aspects of cyber security. This requires that every entity with a low impact BES Cyber System have an incident response plan that covers six areas of incident response, including identification, response, reporting, roles and responsibilities, handling, testing, and updating of those plans.
- **Transient Cyber Assets and Removable Media** – One final 'front door' through which malware or other exploits can enter an asset and impact BES Cyber Systems is through the devices that authorized users bring in and directly connect that thus bypass the electronic remote access controls. This required fifth section of the cyber security plan revolves around mitigating the risk of malicious code on devices that 'walk in' and directly connect and covers Transient Cyber Assets such as laptops used for configuration, troubleshooting, maintenance, etc., as well as removable media such as USB thumb drives. This section has the stated security objective of mitigating the risk of the introduction of malicious code from such devices and requires various methods of detecting and mitigating the malicious code threat before connecting to any low impact BES Cyber System.

The NERC CIP standard then covers every low impact BES Cyber System in the North American BES with these requirements that cover people, processes, and technology and require controls at the 'front doors' through which most threats exploit vulnerabilities – electronic remote access to the site, unauthorized physical access to the site, or through devices carried into the site by authorized users.

In addition to having cyber security plans, each entity must also have corresponding cyber security policies that incorporate these areas.

One further area where the CIP standards apply to low impact BES Cyber Systems is for those that reside in a Control Center. In such cases, the CIP-012 standard applies protections to the real time monitoring and assessment data as it is being transmitted between that Control Center and all other Control Centers.

Chapter 2: Current Risk to Low Impact Systems

Risks to BES Cyber Systems are not static because the threats are not static. One of the unique aspects of cyber security risks to BES equipment over others such as weather, environmental, mechanical, or electrical is it is a risk from motivated, intelligent, and adaptable human adversaries. Over time cyber threats have gone from defacing Internet-accessible websites, to exploiting firewall rules, to 'hacking the humans' through phishing, to ransomware, to sophisticated supply chain attacks. As the defenses have adapted to the attacks, the attacker's techniques change as well. Unlike many other risks, cyber security risks are subject to constant adaptation by the adversary.

Risk of Coordinated Attacks

The CIP-002 standards categorize most individual BES Cyber Systems within the BES as low impact. This is reasonable on what has been called the 'largest machine in the world' that stretches across the North American continent and is designed, built, and operated to withstand the loss of portions of itself including any single asset. For example, weather events often cause unavailability of individual substations, lines, and generating units yet the BES remains stable. Having the majority of the individual BES cyber systems categorized as low impact is therefore reasonable, given that the assets they support are also of low impact individually. If a line can trip from a lightning strike or a generating resource trip due to a bearing failure, then a trip from a cyber system cause on that same asset is of the same low impact to the BES.

However, the primary risk presented by low impact BES Cyber Systems is not from each individually, but through using cyber means (network connectivity, remote access, etc.) to aggregate the impact across many individual low impact BES Cyber Systems affecting multiple BES assets. This is the risk of a 'coordinated attack', defined for the purposes of this report as:

> *"An orchestrated attack against multiple low impact BES Cyber Systems, independent of Responsible Entity ownership, which has the goal of causing an Adverse Reliability Impact to the BES."*

The ability to simultaneously communicate with many low impact systems across multiple BES assets can allow coordinated attacks whose impact can aggregate to an equivalent medium or high impact to the BES. This aligns with the categorization of high impact BES Cyber Systems that are within larger Control Centers – a centralized system that is a single point with a large 'span of control' from which to perform a coordinated attack across many lows or mediums.

An effective evaluation of risk associated with a distributed and coordinated attack event requires an understanding of the requirements for an attacker to initiate a successful attack. Every successful cyber-attack requires motive, method, and opportunity.

- Motive represents the 'what' or the goal an attacker is trying to accomplish. Motive is not always clear, although it is a potential indicator of the most probable risk(s) an organization is likely to face from a cyber-attacker. For example, an organization with a strong financial position is more likely to attract attackers with a financial motive. Organizations that understand probable attacker motives are able to effectively prioritize those cybersecurity controls that defend against related attack methods.
- Method represents 'how' the attacker accomplishes their motive and is representative of the ability, complexity, and effectiveness of an attacker.
- Opportunity represents the potential weaknesses in an organization's cybersecurity that an attacker may leverage to achieve their goal, allowing their method to achieve their motive.

With these in mind, the LICRT identified several different attack methods that could be used individually or in combination to initiate a coordinated attack against low impact BES Cyber Systems at multiple locations. These attack methods were then ranked based on a compilation of:

- Ease of execution,
- Potential impact to operations, and
- Probability.

The highest ranked category of coordinated attack methods consists of:

- **Unauthorized Remote Access** – Management access by an unauthorized party for malicious intent initiated from an external system, using any communication means available, including compromise of known or unknown access methods, insecure configurations, or system vulnerabilities. This method could be used by an attacker using compromised credentials or a compromised cyber system to access and modify many low impact BES Cyber Systems across several BES assets to implement a coordinated attack.
- **Malicious Software** – Software that enables unauthorized malicious behavior on a target system, such as spyware, ransomware, logic bombs, worms, trojans, keyloggers, etc. Malicious software on one low impact BES Cyber System does not constitute a coordinated attack, however malicious software that can use connectivity to spread to cyber systems in other BES assets and cause wider impact (e.g., ransomware) is the concern from a coordinated attack perspective.

The medium category methods are:

- **Supply Chain Common Service Attack** – Compromise of a service organization that has business relationships with multiple partner organizations to enable the malicious actor to gather sensitive data, initiate unauthorized remote access, deliver malicious code, or initiate any other attack against partner organizations. Examples include, but are not limited to, vendors, Managed (Security) Service Providers (MSP, MSSP), ISO/RTO type communications (ICCP), etc. This method could be used for a coordinated attack if the attacker was able to infiltrate an outside service that has connectivity or control of multiple low impact BES Cyber Systems, especially not only across multiple BES assets, but multiple entities.
- **Supply Chain Product Compromise** – An attack against one or more suppliers that provide products and/or services in order to initiate a malicious campaign against one or more target organizations. This differs from a common service attack method (that originates externally from a provider) as this is a common product or service installed internally within multiple BES assets or entities. This method could be used for a coordinated attack if the attacker compromised the software/firmware processes of a vendor and embedded malicious code that is then installed in low impact BES Cyber Systems across multiple BES assets or multiple entities.
- **Unauthorized Internal Access by a Single Actor** - Physical access by an unauthorized party or by a party abusing their existing access for malicious intent initiated from an internal system, thus bypassing any network perimeter remote access controls. The attacker then uses any communication means available to launch a coordinated attack by compromising or operating other systems at multiple locations.

The lower category methods are:

- **Denial of Service** – A remote attack that interrupts normal operation, typically by saturating communications (shared or otherwise), interrupting system process capabilities, or initiating a system failure. This could be used as a method of coordinated attack mostly for BES assets that are dependent upon Internet connectivity, typically using Virtual Private Networks (VPN) over a connection to the public Internet. If multiple assets containing low impact BES Cyber Systems are connected to the public Internet, an attacker could direct a large network of compromised machines (i.e., a 'botnet') to flood many assets with traffic simultaneously.

- **Data Manipulation** – Malicious modification of data, typically at the application protocol level, to hide, mislead, or initiate unauthorized changes to target systems. This could be used as a method of coordinated attack if the attacker has access to the network connecting many BES assets containing low impact BES Cyber Systems and operational traffic is not encrypted or otherwise protected from tampering. Spoofing network addresses of valid systems and issuing commands or intercepting and changing data within unencrypted sessions could be used to aggregate impact across multiple sites.

- **Unauthorized Internal Access by Multiple Actors** - Simultaneous physical access at multiple sites by unauthorized parties or by multiple parties abusing their existing access for malicious intent. This attack method requires multiple individuals at multiple locations working in a coordinated fashion towards a single purpose.

Chapter 3: Existing CIP Standards Gap Evaluation

Several risks associated with Low Impact BES Cyber Systems are addressed by the existing CIP standards as described in Chapter 1 titled "Low Impact BES Cyber System Cyber Security Requirements". In Chapter 2 the LICRT analyzed and documented the main coordinated attack methods that could be used by an attacker. This chapter evaluates each of those coordinated attack methods against the existing CIP-003 and CIP-012 standard requirements for assets containing low impact BES Cyber Systems and considers any in-process NERC standards efforts. It then analyzes any remaining gaps that may present opportunities for an attacker to use that method to perform a coordinated attack.

Unauthorized Remote Access

Unauthorized remote access is one of the highest risk coordinated attack methods. As increasing numbers of low impact BES Cyber Systems gain increased remote access capabilities, the threat of unauthorized use of this access grows.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems, reducing the available remote attack surface.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - By identifying, monitoring, and controlling vendor remote access sessions, the risk of unauthorized remote access is reduced. Also, by detecting malicious communications, insecure configurations and system vulnerabilities are likely to be identified.

Gap Analysis

- No requirement to authenticate users before they are granted access to networks containing low impact BES Cyber Systems, enabling lateral movement to occur to many lows. No authentication is required for remote access using routable protocols, which could result in a compromise that allows easy connection to multiple locations. Without authentication, entities cannot ensure that the sessions within the permitted communication paths are authorized.
- No requirements for strong (multi-factor) authentication of remote access users, allowing use of weak or single factor credentials. Compromised single-factor (ID/Password) credentials could be used by attackers to access multiple lows.
- Suspected suspicious or malicious communications may not be detected and monitored for necessary electronic communications through an otherwise permitted path (see CIP-003 Attachment 1 Section 3). Project 2020-03 will require this only for vendor communications, which will exclude all other non-vendor communications.

Malicious Software

Malicious software that may find an entry point on one low impact BES Cyber System may be able to spread and impact many like systems across multiple BES assets and be used to conduct a coordinated attack. This is another high-risk area due to the increased network connectivity.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems which prevent any unnecessary traffic between BES asset sites.
- CIP-003 Transient Cyber Asset and Removable Media requirements that require mitigating the risks of introduction of malicious software to low impact BES Cyber Systems from physically present Cyber Assets and media that connect to low impact BES Cyber Systems.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - Addition of detecting malicious vendor remote access communications by which malware, spyware, ransomware, etc. would be more likely to be identified as it attempts to spread to other BES assets.

Gap Analysis

- Suspected suspicious or malicious communications may not be detected and monitored for necessary electronic communications through an otherwise permitted path (see CIP-003 Attachment 1 Section 3). No active monitoring for malware is required for assets that allow remote connections. Project 2020-03 will require this only for vendor communications, which will exclude all other communications.

Supply Chain Common Service Attack

Common external services with access to low impact BES Cyber Systems at multiple assets within an entity, or especially across multiple entities, are an avenue of coordinated attack.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems. This reduces the attack surface available to the external service to only what is necessary.
- CIP-012-1 - Cyber Security – Communications between Control Centers (effective 7/1/2022) requires implementing methods to protect confidentiality and integrity of Real-Time Assessment and Real-Time monitoring data while being transmitted between Control Centers. This mitigates the risk of any unauthorized entity or threat actor with access to these external networks to intercept or manipulate this data.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - By identifying, monitoring, and controlling vendor remote access sessions, the risk of unauthorized remote access is greatly reduced. Also, by detecting malicious communications, insecure configurations and system vulnerabilities are likely to be identified.

Gap Analysis

- No requirement to authenticate remote users before they are granted access to networks containing low impact BES Cyber Systems, enabling lateral movement to occur to many lows.
- No requirements for strong (multi-factor) authentication of remote access users, allowing use of weak or single factor credentials. Compromised single-factor (ID/Password) credentials could be used by attackers to access multiple lows.

- Protection of communications across publicly accessible networks only required if between Control Centers.
- Detection of suspicious or malicious electronic communications not required. Project 2020-03 will require this only for vendor communications, which will exclude all other communications.
- Communications to and from an asset containing low impact BES Cyber Systems are not restricted from using publicly accessible networks (e.g., the Internet). Remote systems that are allowed through current electronic access controls could be spoofed if not protected on publicly accessible networks.

Supply Chain Product Compromise

A common product or service that is installed internally within a BES asset or across multiple assets or entities could be used for a coordinated attack if the attacker compromised the software/firmware processes of a vendor and embedded malicious code that begins to compromise other systems across multiple BES assets.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems which prevent any unnecessary traffic between BES asset sites.
- CIP-012-1 - Cyber Security – Communications between Control Centers (effective 7/1/2022) requires implementing methods to protect confidentiality and integrity of Real-Time Assessment and Real-Time monitoring data while being transmitted between Control Centers. This mitigates the risk of any unauthorized entity or threat actor with access to these external networks to intercept or manipulate this data.

Current NERC Efforts

- Project 2020-03 – Supply Chain Low Impact Revisions (Modifications to CIP-003-8)
  - Known malicious traffic associated with a supply chain compromise should be identified by implementation of the CIP-003-8 controls. Vendor remote access detections may also inhibit exploitation of supply chain compromise.

Gap Analysis

- No evaluation and mitigation of risks for procurement (i.e., CIP-013 and CIP-010). Not having an evaluation and mitigation of risks for procurement places dependency on controls that rely on detection after a compromise. For example, a product (or multiple products) that has a common dependency (e.g., shared DLL, shared common code) installed in multiple locations.

Unauthorized Internal Access by a Single Actor

Physical access by an unauthorized party or by a party abusing their existing access for malicious intent could initiate a coordinated attack by compromising or operating other systems at multiple locations from their internal location.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems which prevent any unnecessary traffic between BES asset sites. The attacker would need to work within what is allowed outbound at their location and inbound at other locations.
- CIP-003 Physical Access Controls that require physical access be controlled based on need either (or both) at an asset level or to locations of low impact BES Cyber Systems within the asset, as well as specifically to any

cyber assets that control electronic access to the asset (e.g., firewalls protecting external access to the BES Cyber Systems).

Current NERC Efforts

- None

Gap Analysis

- Detection and prevention of unauthorized physical access of an individual to initiate an attack against BES Cyber Asset(s) at multiple locations simultaneously from an internal system. By not addressing local physical access, unauthorized use of trusted electronic communication to BES Cyber Asset(s) at multiple locations may not be detected, logged, monitored, or controlled.

Denial of Service Attack

Common network connectivity on a publicly accessible network such as the Internet could be used by an attacker to conduct (Distributed) Denial of Service (DDoS/DoS) coordinated attacks against multiple BES assets containing low impact BES Cyber Systems, either causing boundary devices such as FWs to temporarily fail or cause time-sensitive communications to fail.

Current CIP Standards Low Impact Requirements

- None

Current NERC Efforts

- Project 2020-04 Modifications to CIP-012
  - By implementing protections to ensure the availability of real-time data between Control Centers (all impact levels), such as alternate communication paths, the risk of a denial-of-service attack preventing transmission of real-time data between Control Centers is mitigated or eliminated.

Gap Analysis

- CIP-012 and its protections only apply to Control Centers of all impact levels. It is not known how many other types of BES assets such as substations or generation resources are exposed directly to public networks and thus subject to a DDoS attack from large numbers of compromised Internet devices that could affect enough lows simultaneously to cause an Adverse Reliability Impact.

Data Manipulation

An attacker with access to common network connectivity, particularly on a publicly accessible network such as the Internet, could modify data or issue commands in a coordinated attack against multiple BES assets containing low impact BES Cyber Systems.

Current CIP Standards Low Impact Requirements

- CIP-003 Electronic Access Controls that permit only necessary inbound and outbound communications to an asset containing low impact BES Cyber Systems.
- CIP-012-1 - Cyber Security – Communications between Control Centers (effective 7/1/2022) requires implementing methods to protect confidentiality and integrity of Real-Time Assessment and Real-Time monitoring data while being transmitted between Control Centers. This mitigates the risk of any unauthorized entity or threat actor with access to these external networks to intercept or manipulate this

data. By encrypting communications or deploying non-repudiation-based technologies of data between Control Centers, the risk of unauthorized data manipulation is mitigated or eliminated.

Current NERC Efforts

- None

Gap Analysis

- No protection of data in motion, other than that covered by CIP-012-1 between Control Centers.
- Modification of data or commands between BES Cyber Assets at multiple locations could initiate unauthorized control, could compromise situational awareness, and could lead to inadvertent system operator actions.
- Data between Control Centers and substations or generation resources on publicly accessible networks does not require protection of its confidentiality or integrity (i.e., encryption, VPN).
- The electronic access controls in CIP-003 are typically a source/destination address pair that could be spoofed if the communications are not within a defined Virtual Private Network (VPN) required between the source and destination points.

Unauthorized Internal Access by multiple actors

Simultaneous physical access by multiple unauthorized parties at multiple locations could initiate a coordinated attack by compromising or operating systems at multiple locations from their internal locations.

Current CIP Standards Low Impact Requirements

- CIP-003 Physical Access Controls that require physical access be controlled based on need either (or both) at an asset level or to locations of low impact BES Cyber Systems within the asset, as well as specifically to any cyber assets that control electronic access to the asset (e.g., firewalls protecting external access to the BES Cyber Systems).

Current NERC Efforts

- None

Gap Analysis

- Detection and prevention of unauthorized physical access of multiple individuals to initiate a coordinated attack against BES Cyber Asset(s) at multiple locations simultaneously. By not addressing local physical access, unauthorized use by multiple individuals of trusted electronic communication to BES Cyber Asset(s) at multiple locations may not be detected, logged, monitored, or controlled.

Chapter 4: Overall Analysis and Recommendations

In the previous chapter, each of the coordinated attack methods were analyzed for potential gaps in required protection within the CIP standards (accounting for current requirements and drafting efforts already underway). In reviewing each of those identified gaps across all the coordinated attack methods, they fall into five distinct control gaps:

- Lack of authentication of remote users
- Lack of protection of communications to and between low impact BCS across publicly accessible networks
- Lack of detection of malicious communications to/between low sites
- Undetected unauthorized physical access to lows
- Lack of procurement risk evaluation for lows

Each of these control gaps was analyzed to see where each appeared across all the attack methods as well as the team's recommended risk mitigation priority of each one. The attack method rating from **Chapter 2** is included in parentheses for reference.

Table 4.1: Attack Methods

Control Gap	Attack Method	Risk Mitigation Priority
Lack of authentication of remote users	Unauthorized Remote Access (High) Supply Chain Common Service Attack (Medium)	High
Rationale: The review identified potential high impact to the BES due to the absence of remote authentication controls. User authentication can mitigate coordinated attack methods via electronic means including some supply chain vendor access gaps, launching electronic attacks after unauthorized physical access, etc. Additionally, the cost to implement could be low, and the ease of compromise is high.		
Lack of protection of communications to and between low impact BCSs across publicly accessible networks	Supply Chain Common Service Attack (Medium) Denial of Service Attack (Low) Data Manipulation (Low)	Medium
Rationale: Theme of risks that may result in the ability to enable address spoofing, man in the middle, and denial of service attacks. High degree of risk mitigation potential for BES sites on the Internet with only firewall protection but no protection of operational traffic on the public network. However, the population of such sites is unknown so the overall risk to BES reliability is unknown.		
Lack of detection of malicious communications to/between low sites	Unauthorized Remote Access (High) Malicious Software (High) Supply Chain Common Service Attack (Medium) Unauthorized Internal Access by Single Actor (Medium)	High

Table 4.1: Attack Methods		
Control Gap	**Attack Method**	**Risk Mitigation Priority**
Rationale: Risk mitigation depends primarily on type of access and the protocols used to/between sites. If the access is only a single industrial protocol polling an RTU, there is a lower degree of mitigation possible. If access is granted to remotely manage BCS configuration at the site, there is a much higher degree of risk mitigation possible, so this is site and mode dependent.		
Undetected unauthorized physical access to lows	Unauthorized Internal Access by Single Actor (Medium) Unauthorized Internal Access by Multiple Actors (Low)	Low
Rationale: High cost with low probability/likelihood. This is more of a 'launch point' threat from an electronic perspective, i.e., physical access to one remote site should not equate to electronic access to many other sites. This is more effectively mitigated with network security controls such as authentication above.		
Lack of procurement risk evaluation for lows	Supply Chain Product Compromise (Medium)	Medium
Rationale: High cost for all lows. Should evaluate the effectiveness of risk mitigation for procurement of high and medium impact systems prior to expanding scope. Does not detect/prevent the spread of malware or the delivery of commands to perform a coordinated attack.		

In making recommendations for mitigating risks from these gap themes, the LICRT determined three categories of recommendations:

- **CIP Standards Revisions** – recommendations for a Standards Authorization Request (SAR) to address identified gaps with CIP Standard modifications.
- **Security Guidelines** – recommendations that NERC Security Guideline documents be developed to assist entities in identifying and mitigating identified gaps.
- **Risk Monitoring** – recommendations that call for NERC to monitor and/or gather more information to further gauge the risk from identified gaps.

For any recommendations in the *CIP Standards Revisions* category, there are various 'knobs' that can be turned within the standards themselves to tailor the requirements and their scope to the appropriate BES Cyber Systems:

- **Impact Rating Criteria** – The first is to modify the impact rating criteria in CIP-002, Attachment 1 to modify the impact rating BES Cyber Systems must receive based on an identifiable attribute of such systems. This is typically used for 'broad brush' scope changes, affecting an entire category of BES Cyber Systems. If an identifiable category of BES Cyber Systems is recognized as having a different impact level to the BES, the criteria can be modified accordingly to raise or lower the rating they receive in CIP-002.
- **Scope Modifiers**: Secondly, certain cyber security requirements often use scope modifiers to tailor applicability to subsets of an impact category with differing risk attributes. The most common is 'with External Routable Connectivity (ERC)'. A BES Cyber System may be categorized as a medium impact but have an elevated risk if it has ERC and is remotely accessible. Several such modifiers exist, such as: "at Control Centers", "with vendor remote access," and "with Dial-up Connectivity".

- **Requirements:** Lastly, new or modified requirements can be created for the existing impact categories. This allows for the situation when a broad reclassification of impact levels is not necessary, but additional requirements are needed for an existing impact category.

Recommendations

After the analysis documented in this report, the LICRT arrived at the following overall conclusions regarding low impact BES Cyber Systems:

- Low impact BES Cyber Systems are truly low impact to BES reliability *individually* which 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 parts. A medium or high impact to the BES is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the *impact criteria* in CIP-002 for identifying and categorizing *individual* BES Cyber Systems at this time.
- *However*, there are risks to BES reliability from lows that could rise to medium or higher impact through aggregation of impact from a coordinated attack against many distributed low impact BES Cyber Systems. The team does see a need for additional recommendations on the existing low impact category to further mitigate the risk of coordinated attacks.

Those recommendations, sorted by category, are as follows:

CIP Standards 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 (e.g. combinations of usernames and passwords) 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 low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.

Security Guidelines

- Develop best practice guidance documents for protection of communications to and between low impact BES Cyber Systems across publicly accessible networks.
- Develop best practice guidance documents for procurement risk evaluation for low impact BES Cyber Systems.
- Develop best practice guidance documents for entities to voluntarily submit an E-ISAC report for unauthorized physical access attempts to low impact BES Cyber Systems.

Risk Monitoring

- Continuous monitoring of E-ISAC physical access attempt reports to low impact BES Cyber Systems to determine if the risk increases over time and should be addressed.

Appendix A: Low Impact Criteria Review Project and Team

Project Scope: Work with NERC staff to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact BES Cyber Systems and report on whether those criteria should be modified. Included is an analysis of risk to the BES from a coordinated attack involving low impact BES Cyber Systems.

Team Formation: Assemble a team of cybersecurity experts and compliance experts that represent a cross section of the industry to fairly represent the understanding of the potential threat and risk posed by a coordinated cyber-attack on low impact BES Cyber Systems.

The following are the members of the Low Impact Criteria Review Team that produced this report:

- NERC: Howard Gugel (Executive Sponsor), Lonnie Ratliff, Ryan Quint
- APPA: Carter Manucy
- CEA: Cameron Fisher, Henry Bosch
- EEI: Thad Ness, Jay Cribb
- FERC: Kal Ayoub, Michael Keane
- ISO/RTO Council: Tim Beach, Derek Drayer
- LPPC: Adam Gormley
- NRECA: Alice Ireland, Richard (Richie) Field

Appendix B: NERC Board Resolution

The NERC Board Resolution from which the Low Impact Criteria Review project and team was created:

> **WHEREAS,** the Board adopted proposed Reliability Standard CIP-002-6 on May 14, 2020, in which a new criterion was proposed to address the applicability of the CIP Reliability Standards to Control Centers owned by Transmission Owners performing the functional obligations of a Transmission Operator;
> **WHEREAS,** recent cybersecurity events and the evolving threat landscape warrant additional caution regarding any criteria that may permit more entities to categorize BES Cyber System as low impact and therefore subject to fewer requirements in the CIP Reliability Standards;
> **NOW, THEREFORE, BE IT RESOLVED**, that the Board hereby withdraws the proposed Reliability Standard CIP-002-6, as presented to the Board at this meeting.
> **FURTHER RESOLVED**, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolution.
> **FURTHER RESOLVED,** that NERC Staff, working with stakeholders, is directed to promptly conduct further study of the need to readdress the applicability of the CIP Reliability Standards to such Control Centers to safeguard reliability, for the purpose of recommending further action to the Board.
> **FURTHER RESOLVED,** that NERC Staff, working with stakeholders, recognizing the complexity of the undertaking, is directed to expeditiously complete its broader review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and report on whether those criteria should be modified.

Appendix C: CIP-002-5.1a BES Cyber System Categorization

This appendix contains 'Attachment 1' from the NERC CIP-002-5.1a standard that contains the complete impact rating criteria for BES Cyber Systems.

CIP-002-5.1a - Attachment 1
Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Table C.1: Aggregate Weighted Value Exceeding 3000

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

- **3.1.** Control Centers and backup Control Centers.
- **3.2.** Transmission stations and substations.
- **3.3.** Generation resources.
- **3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
- **3.5.** Special Protection Systems that support the reliable operation of the Bulk Electric System.
- **3.6.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.