FORMAL CASE STUDY

NERC CIP Low Impact Assessments Enable Compliant, Secure Utilities

An anonymized utility cybersecurity compliance case study

Customer Reference	A regional electric utility, referred to in this case study as “the Utility”.
Primary Need	Establish a practical path to NERC CIP low impact electronic access control compliance.
Operating Context	Bulk Electric System environments with low impact BES Cyber Systems and external routable communications.
Outcome	A repeatable assessment model that improves compliance posture, security visibility, and operational confidence.

Executive takeaway: Low impact BES Cyber Systems may not require discrete asset-by-asset identification, but responsible entities still need demonstrable cybersecurity controls. The most useful assessment begins with understanding application-level IP communication flows into, out of, and within each location.

Executive Summary

The Utility needed a practical, defensible approach for addressing NERC CIP low impact expectations without creating an unmanageable inventory exercise across thousands of field and operational technology assets. The regulatory language creates an important distinction. Low impact BES Cyber Systems are not required to be discretely identified in the same way as higher-rated systems, yet they remain subject to obligations for cybersecurity awareness, physical access control, electronic access control, and incident response. The challenge was to translate that distinction into an assessment method that could be executed consistently across operational locations.

This case study describes an anonymized engagement in which the Utility framed low impact compliance as a security control design problem rather than a documentation-only activity. The central insight was that effective electronic access controls depend on understanding protocol-based application flows. If a low impact location uses bi-directional routable protocol communication or dial-up connectivity to systems outside the asset, the entity must understand what communication is expected, what communication is unnecessary, and where access needs to be restricted or monitored. The assessment method therefore focused on identifying communication patterns, validating business and operational need, and defining control boundaries that could be supported by policy, architecture, and operational procedures.

Industry and Regulatory Context

The power sector faces a persistent cyber threat environment. Public sector guidance has repeatedly emphasized that utilities and other critical infrastructure operators are frequent targets for attempted intrusion, reconnaissance, credential attacks, and disruptive activity. In response, federal regulators and the electric reliability community have continued to strengthen critical infrastructure protection requirements for the Bulk Electric System. High and medium impact assets historically received the greatest compliance and security attention because of their direct risk profile, operational sensitivity, and more detailed control expectations. Low impact systems, however, represent a broad and distributed portion of the operating environment.

In early 2018, FERC approved a NERC CIP reliability standard that increased protection expectations for low impact Cyber Systems. The resulting compliance timeline placed low impact assessment work on near-term utility roadmaps. For many utilities, this created a strategic issue: how to improve control coverage without applying a high impact or medium impact framework in a way that would be disproportionate, costly, and difficult to sustain. The key was to respect the low impact categorization while still implementing practical controls that reduce cyber risk.

Customer Challenge

The Utility operated a broad set of field, substation, telecommunications, and supporting operational technology systems. Many of those systems were not categorized as high impact or medium impact and therefore defaulted to low impact. Individually listing every low impact BES Cyber System would have created a large administrative burden, and it would not necessarily have improved the organization's understanding of risk. The Utility needed an approach that would be compliant, scalable, and meaningful to operations.

The most important challenge was electronic access. Low impact environments often contain routable communication, vendor access paths, engineering workstations, serial-to-IP conversion, remote maintenance functions, and monitoring connections. These connections may be legitimate and necessary, but they can also create pathways that are difficult to defend if they are poorly documented or broadly permitted. The Utility's team therefore needed to move beyond a question of "what assets are present" and toward a question of "what communication is allowed, why it is needed, and how it is controlled."

Assessment Approach

The assessment began by interpreting low impact compliance obligations in practical operational terms. The team treated locations as control environments and mapped communications associated with those environments. For each location, the assessment considered external routable connections, internal routable communication, dial-up or equivalent remote connectivity, system-to-system exchanges, and any pathway that could enable access from

outside the immediate asset boundary. The intent was not to over-document every device. Instead, the assessment emphasized application flows, access methods, and control points.

The team established a repeatable workflow. First, available architecture diagrams, device lists, firewall rules, remote access records, and network information were collected. Second, expected communication flows were reviewed with operations, engineering, compliance, and cybersecurity stakeholders. Third, the team separated required operational communication from unnecessary or poorly understood communication. Fourth, control recommendations were developed to support electronic access management, monitoring, and incident response. Finally, findings were organized so they could be maintained as operating conditions changed.

This approach aligned the compliance task with security outcomes. By focusing on communications, the Utility could identify where segmentation, access control lists, firewall policy, jump-host controls, authentication requirements, monitoring, or procedural controls were most valuable. The result was a defensible assessment that supported both audit readiness and cyber risk reduction.

Key Findings

The assessment confirmed that low impact systems can be difficult to protect precisely because they are numerous, geographically dispersed, and operationally diverse. It also confirmed that many useful improvements do not require a burdensome asset-by-asset catalog. The most valuable information was the communication model: which protocols crossed a boundary, which systems initiated sessions, which connections were bi-directional, and which remote access methods could reach protected operational environments.

Several recurring patterns emerged. Some connections were clearly necessary for telemetry, event retrieval, engineering support, or operational monitoring. Other connections were historic, overly permissive, or insufficiently tied to a documented business need. In several cases, the assessment identified opportunities to narrow allowed traffic, remove unused access paths, strengthen authentication expectations, and improve evidence collection for compliance. The work also improved cross-functional alignment because compliance, operations, and cybersecurity stakeholders could discuss risk using a shared flow-based view of the environment.

Control Design Considerations

The assessment reinforced that electronic access control for low impact locations should be designed around the principle of necessary communication. Controls should allow required application flows and deny or restrict communications that do not support defined operational needs. A low impact program should also be maintainable. If the control model is too complex, it will degrade over time as projects, maintenance activities, and vendor support needs change.

A sustainable control design includes documented flow approval, defined ownership for changes, periodic review of access pathways, incident response alignment, and evidence that shows controls are operating as intended. Physical access and cybersecurity awareness remain important supporting elements, but they do not replace the need to understand routable and dial-up communication. The strongest programs connect people, process, and technology so that field changes and network changes do not silently create new exposure.

Results and Business Value

The Utility gained a structured, repeatable method for meeting low impact expectations while improving the security posture of operational environments. The flow-based assessment model reduced ambiguity by converting broad compliance language into concrete questions that engineers and operators could answer. It also created a practical bridge between regulatory obligation and operational reality.

The business value extended beyond audit preparation. The assessment improved visibility of operational communication, clarified ownership of access pathways, and highlighted areas where access could be reduced without impairing operations. It helped the Utility prioritize improvements based on risk and feasibility rather than attempting to treat all low impact assets the same. Most importantly, the approach created a foundation for ongoing maintenance. As new systems are added, retired, or modified, the Utility can evaluate whether associated communication flows remain necessary and properly controlled.

Lessons Learned

The engagement produced several lessons applicable to other utilities. First, low impact does not mean low priority. These systems may be less critical from a categorization standpoint, but they can still provide pathways into operational environments. Second, asset identification and control design are not the same activity. Even where discrete identification is not required, a utility must still know enough about communication patterns to establish effective controls. Third, operations input is essential. Engineers and field teams understand which connections are required, which are legacy, and which can be constrained. Fourth, the assessment output must be operationally maintainable. A document that cannot be updated during normal change processes will lose value quickly.

The most durable lesson is that compliance and security improve together when the assessment is anchored in application flow. Flow mapping creates a common language for policy, architecture, operations, and audit evidence. It also helps utilities avoid unnecessary complexity by focusing on the communication that actually matters.

Conclusion

NERC CIP low impact assessment work is most effective when it is framed as a practical control design effort. Low impact BES Cyber Systems may not require discrete identification, but entities still have an obligation to protect associated environments through appropriate cybersecurity awareness, physical access control, electronic access control, and incident response capabilities. For locations with bi-directional routable protocol communication or dial-up connectivity, the foundation of effective electronic access control is a clear understanding of application flow.

For the Utility, the assessment produced a defensible and scalable model that could be maintained over time. It supported compliance readiness, strengthened security visibility, and gave stakeholders a shared method for evaluating access risk. The broader implication for utilities is clear: start with communication flows, validate operational need, implement practical controls, and maintain the model through governance and change management. That approach enables compliant, secure utilities without imposing unnecessary complexity on already demanding operational environments.

Case Study Summary

Problem	The Utility needed a scalable way to address low impact compliance obligations without creating an excessive discrete asset inventory burden.
Method	The team assessed locations by mapping expected IP protocol-based application flows and reviewing external and internal access paths.
Controls Emphasized	Electronic access control, access path governance, flow approval, periodic review, monitoring alignment, and incident response readiness.
Security Benefit	Improved visibility into operational communication and reduced unnecessary or poorly understood access paths.
Compliance Benefit	A repeatable evidence model that supports low impact obligations while remaining maintainable for operations teams.