# Meeting Relevant NERC CIP Cybersecurity Standards with a Simple and Secure OT User Access Platform

**XONA**™ has been third-party tested and complies fully with NERC-CIP Cybersecurity Standards 005-5, 007-6, 011-2 and 013-1. **XONA** utilizes protocol and system isolation, encrypted display, multi-factor authentication as well as session logging and recording of user access to support this compliance, securing against cybersecurity risks.

## CIP-005-5 ELECTRONIC SECURITY PERIMETERS – INTERACTIVE REMOTE ACCESS MANAGEMENT – PART 2.1, 2.2, 2.3

**The XONA platform supports requirements for controls over Interactive Remote Access to cyber assets through the following:**

- **XONA**'s Critical System Gateway (CSG) functions as an intermediate system to manage remote access that limits direct access to cyber assets (2.1)
- The CSG acts as an intermediate gateway with the capability of initiating & terminating encryption to limit direct access to cyber assets (2.2)
- **XONA** enforces authorized users based on Multi- Factor Authentication (MFA) for all interactive remote access sessions (2.3)
- **XONA** MFA controls utilize Yubico hardware tokens (Yubikeys) to enforce user access authentication at each system (2.3)
- **XONA** also provides user access data, including successful and failed log-in and log-off and start and end times for all sessions (2.3)

## CIP-007-6 SYSTEMS SECURITY MANAGEMENT – PORTS AND SERVICES -PART 1.1, SECURITY EVENT MONITORING -PART 4.1, 4.2, 4.3 AND SYSTEM ACCESS CONTROLS - PART 5.1

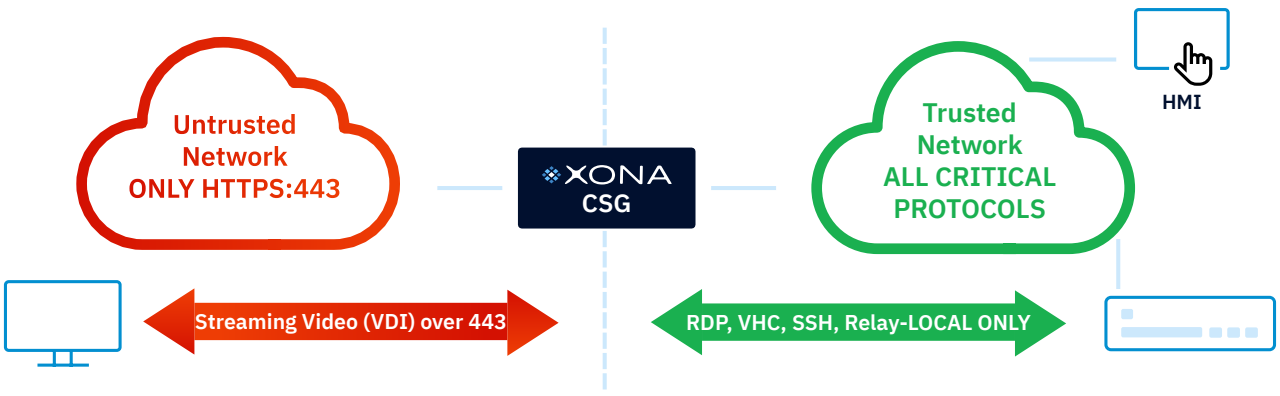
**The XONA platform supports requirements for controls over Systems Security Management to cyber assets through the following:**

- **XONA** combines strong MFA with granular authorizations to applications and cyber assets to ensure only authorized users have logical network access to ports on the CSG.; **XONA** utilizes standards-based encryption (SSL) and mutual TLS for client-to-CSG communication (1.1)
- **XONA** CSG provides session logging events of successful and failed log-in and log-off and start and end times for all sessions in support of Cyber Security incident investigations (4.1)
- **XONA** provides detailed user access and event logs that support detection of failed access attempts and login attempts for alert generation (4.2)
- **XONA** allows users to define event log retention, which can be maintained up to one year.;Users can set the CIP 90-day consecutive requirement or longer(4.3)
- **XONA**'s platform provides authentication for each separate cyber asset within an architecture, and through MFA, users are only given access to designated system or asset connections and are forbidden from traversing to any other cyber asset (5.1)

## CIP-011-2 INFORMATION PROTECTION -INFORMATION PROTECTION - PART 1.2

**XONA supports requirements for controls for Information Protection for handling Cyber System Information as follows:**

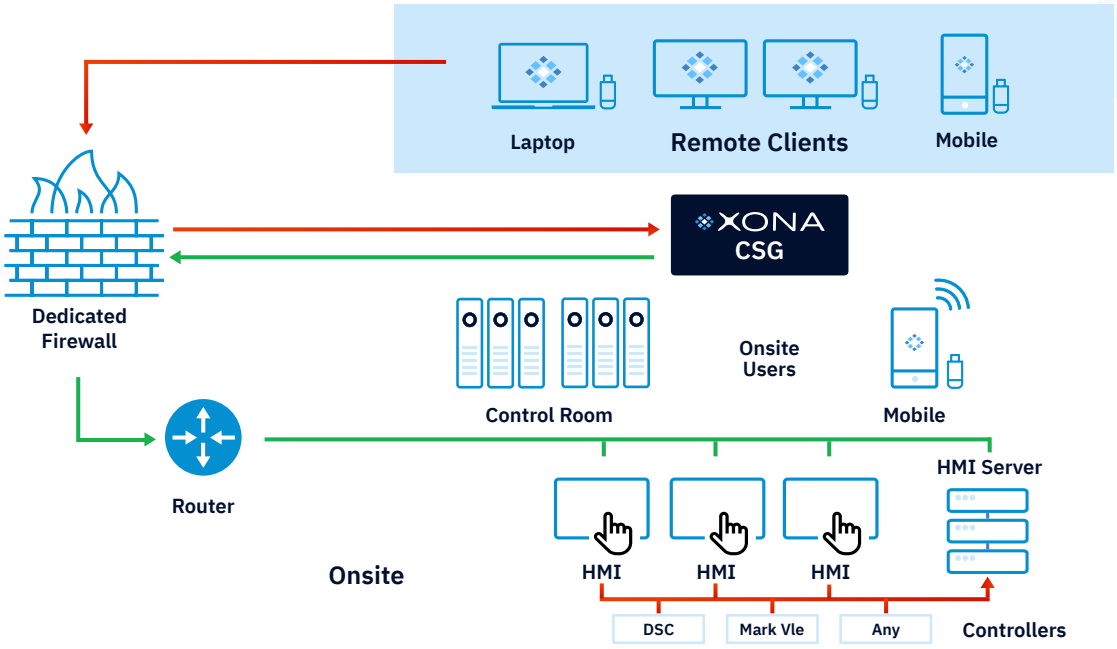
- **XONA** CSG employs encrypted browser-based thin client access to its critical system gateway using mutual transport layer security and ensures that Cyber System Information does not migrate to the endpoint.; **XONA** only remotes the pixels of the data, which supports the protecting and securing Cyber System Information (1.2) (5.1)



# CIP-013-1 CYBER SECURITY - SUPPLY CHAIN RISK MANAGEMENT

**The XONA platform supports requirements for Supply Chain Risk Management with the following procedures:**

- **XONA** has documented procedures to monitor and recognize new incidents that may affect software performance
- **XONA** procedures define the coordination of responses to new cyber security incidents
- **XONA** persistently performs in-house testing against new threats and ensures that 3rd party vendors are up to date
- **XONA** employs verification of software integrity and authenticity on all patches and new versions of software.




**XONA**'s user access platform includes Critical System Gateway (CSG) and Remote Operations Access Manager (ROAM) products. The CSG requires an encrypted channel for user access to critical infrastructure systems. ROAM manages the CSG and communicates over a secure, encrypted channel with a shared API key.

In the event of a malicious security event, one of the most important things that can be done is to review the activity that led up to it. Being able to review specific user actions and the applied security measures is essential to both piecing together a comprehensive after-action report and developing a more effective strategy for the future. This is why **XONA**'s platform provides logs of all successful and failed login attempts while also providing the option of screen recording any user session for both forensic and educational purposes.

Additionally, **XONA** adheres to the principle of least privilege by enforcing per system and user access in addition to multi-factor authentication. Users are given explicit access on a per system or asset connection. This means that users cannot traverse the network via their connection and gain access or affect anything outside of their allocated system or application connection.