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

XONATM has been third-party tested and complies fully with NERC-CIP Cybersecurity Standards 003-09, 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-003-09 – VENDOR ELECTRONIC REMOTE ACCESS SECURITY CONTROLS – PART 6.1, 6.2, 6.3

XONA supports requirements for documentation of vendor electronic remote access security controls through the following:

- **XONA** CSG employs a zero-trust model that includes both user authentication, handled locally or via third party identity providers, and authorization, done using a least privilege approach (6.1)

- **XONA** CSG allows admins to be notified of or view user activity, the monitoring of user sessions by two role types, the capture of data regarding activity and connection history, the use of time and date controls for user access and full session recording through RDP, SSH or VNC protocols (6.1)

- **XONA** CSG's Lockbox feature enables administrators to disable access for all users, on a user-by-user basis or for untrusted or trusted Ethernet ports (6.2)

- **XONA** CSG allows for user sessions to be immediately terminated, including the disabling of inbound/outbound ports; the Edit Connection feature can be used to disable communications protocols (6.2)

- **XONA** CSG, as a purpose-built appliance that protects the data stream between the user and the appliance and translates the OT protocols between the appliance and the OT/ ICS asset, does not allow any opportunity for malicious software to inject itself or have a need to integrate IDS/IPS technology (6.3)

- **XONA** CSG captures both data and video logs, and the information can be reviewed locally or via another security tool (6.3)

- **XONA** CSG integrates with a Moxa relay to provide physical alerting using external emergency lighting or sirens locally; alerting can also be achieve by integrating with other services that allow alerting (6.3)

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)
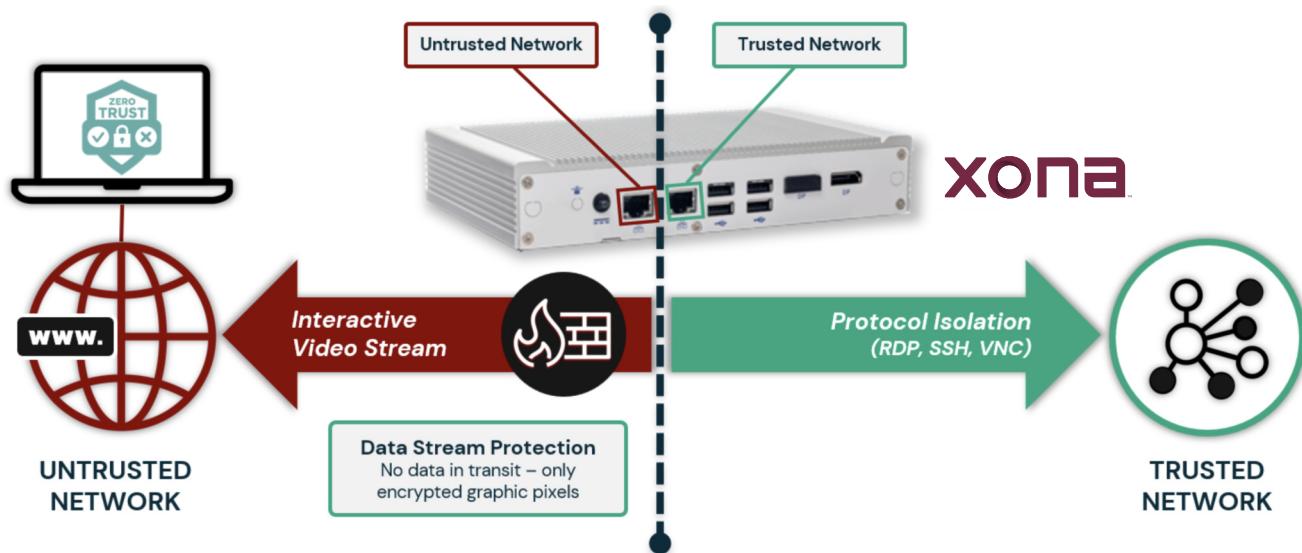
CIP-013-1 CYBER SECURITY – SUPPLY CHAIN RISK MANAGEMENT

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.
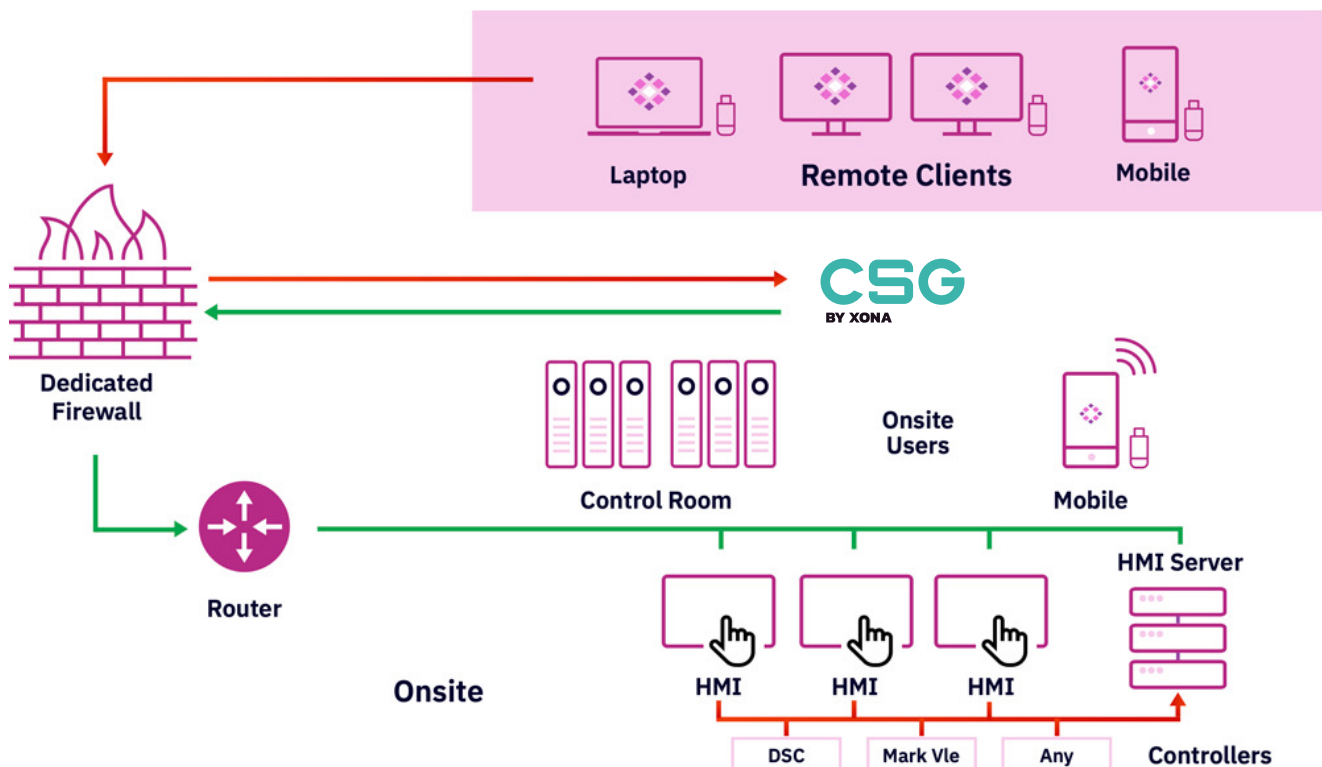
ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.