SECURITY DIRECTIVE (SD) PIPELINE-2021-02C

TSA SD02C Compliance for Pipeline Owners/ Operators

+1 866-849-6629 | info@xonasystems.com

This Security Directive identifies actions required to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber intrusions affecting the nation's most critical gas and liquid pipelines.

The Cybersecurity Implementation Plan must provide the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the Owner/Operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.

The matrix below identifies each of the security controls in this directive that the XONA CSG solution either directly enforces or can be used to help assist.

III. CYBERSECURITY MEASURES

The XONA platform provides foundational requirements and additional security levels for Access Control to cyber assets through the following:

Security Controls	Description	XONA CSG
III.B.	**Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa. As applied to Critical Cyber Systems, these policies and controls must include:**	
III.B.	An identification and description of measures for securing and defending zone boundaries, that includes security controls	
III.B.2.a.	To prevent unauthorized communications between zones	**YES**
III.B.2.b.	To prohibit Operational Technology system services from traversing the Information Technology system, unless the content of the Operational Technology system is encrypted while in transit	**YES**

Security Controls	Description	XONA CSG
III.C.	**Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:**	
III.C.2.	Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to industrial control workstations in control rooms regulated under 49 CFR parts 192 or 195, the Owner/Operator shall specify what compensating controls are used to manage access	**YES**
III.C.3.	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply	**YES**
III.C.4.	Enforcement of standards that limit availability and use of shared accounts to those that are critical for operations, and then only if necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure	
III.C.4.a.	Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties	**YES**
III.C.4.b.	Individuals who no longer need access do not have knowledge of the password necessary to access the shared account	**YES**
III.C.5.	Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts	**ASSIST**
III.D.	**Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems.**	
III.D.2.b.	Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications	**ASSIST**

Security Controls	Description	XONA CSG
III.D.3.a.	Require continuous collection and analyzing of data for potential intrusions and anomalous behavior	YES
III.D.3.b.	Ensure data is maintained for sufficient periods to allow for effective investigation of cybersecurity incidents	YES
III.E.	**Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk-based methodology. These measures must include:**	
III.E.1.	A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.	ASSIST
IV.C.	**Documentation to Establish Compliance**	
IV.C.2.	TSA may request to inspect or copy the following documents to establish compliance with this Security Directive	
IV.C.2.e.i.	Data providing a “snapshot” of activity on and between Information and Operational Technology systems, such as Log files.	

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.

+1 866-849-6629 | info@xonasystems.com