SOLUTION OVERVIEW

Supporting NERC CIP Compliance

How Claroty supports the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Reliability Guidelines

With today's electric utilities continuing to modernize their operations and infrastructure for enhanced efficiency, reliability, and demand response, their information technology (IT) and operational technology (OT) networks are more connected than ever. Smart grid technologies, IIoT sensors, and other modern, internet-connected devices are now intertwined with the complex patchwork of previously air-gapped legacy OT equipment. At the same time, plant staff and third-parties alike are turning to remote (rather than onsite) access to carry out routine maintenance tasks, repairs, and audits at unmanned power generation units and other often-geographically isolated facilities. Although these technologies are undoubtedly bringing new efficiencies, improved safety, and greater sustainability — among a host of other benefits — they are also increasing exposure to complex cyber risks that are difficult for security teams to mitigate.

Mitigating these risks and further strengthening the resilience, safety, and integrity of the Bulk Electric System (BES) is what underpins the standards set forth by the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP). Claroty's OT security portfolio is purpose-built to support Responsible Entities (REs) in achieving and maintaining NERC CIP compliance. More specifically, Claroty provides REs the support to attest to the security of their cyber assets within the BES for generation and transmission safety and reliability.

Claroty Security Solutions

Unlike IT solutions, and those repurposed for OT, Claroty's portfolio is purpose-built for the unique security and operational needs of OT, as well as the broader cyber physical systems (CPS), processes and networks that underpin the BES. Claroty provides the choice of on-premises, cloud-based, and hybrid OT security solutions to address the breadth of security needed for these environments:

Vulnerability & Risk Management	Network Protection	Threat Detection	Asset Management	Change Management	Remote Access
Asset Visibility					
Flexible Deployment		**Role-specific UX**		**Integrated Ecosystem**	
Continuous Threat Detection (CTD): On-premises 		**xDome: SaaS-based platform** 		**Secure Remote Access: Reliable internal and third-party secure remote access** 	

© Copyright Claroty Ltd. All rights reserved

NERC CIP Guidelines

Claroty's portfolio of security solutions, noted above, supports NERC CIP compliance. The following table maps the latest NERC CIP requirements to the extent that specific Claroty product(s) enable compliance with them.

Guideline #	Claroty Support	Claroty Product
CIP-002-5.1a BES System Categorization	Claroty CTD and Claroty xDome can automatically identify all assets and identify configuration parameters about those assets (e.g. model number, firmware version, configuration, etc.). RE's can use this information to tag high, medium, and low impact BES systems.	CTD xDome
CIP-003-8* Security Management Controls	CTD and xDome can assist security programs to classify assets and support management of risk reduction capabilities. xDome Secure Access (xSA) can support remote access capabilities to reduce risk and mitigate access concerns, including but not limited to management of third-party contractors supporting OT environments.	CTD xDome
CIP-003-9 Security Management Controls	Claroty CTD and xDome provide deep visibility into all connected assets and vendor access points, including unmanaged and "shadow" connections. Specifically for CIP-003-9 compliance, xSA delivers secure, granular remote access with the mandatory capability to immediately detect and revoke active vendor sessions. Combined with OT-aware monitoring, Claroty identifies and alerts on malicious inbound/outbound communications in real-time, transforming policy requirements into automated, auditable, and enforceable security controls.	CTD xDome xDome Secure Access
CIP-005 Electronic Security Perimeter (ESP)	Claroty's solutions assist with the design and verification of these networks by identifying and mapping all assets communicating on control networks (Field Bus / Serial & IP Networks). This information is used to construct network diagrams identifying all external routable communication paths and access points. To monitor inbound and outbound access to the ESPs for the purpose of detecting malicious activity, Claroty's unique combination of signatures, purpose-built OT behavioral models, and proprietary anomaly detection capabilities assist RE's with this. CTD and xDome can immediately detect and provide actionable information on malicious activities. Most importantly, CTD and xDome can identify potentially malicious communications within OT protocols that may not be understood by traditional security tools, filling a potential gap in compliance.	CTD xDome

*Please note that this guideline has been superseded by CIP-003-9 which is slated to be released for use April 2026.

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-005 **R2** **Parts 2.4 and 2.5** **Secure Remote Access**	1) xSA prevents a device that initiates a connection from directly accessing a protected asset. Remote access is securely proxied through xSA, ensuring that only the authorized user on the originating device has access. 2) xSA provides encryption between originating devices and the remote access server. Access to xSA is provided via HTTPS, an industry standard protocol for secure web access. 3) xSA supports 2-factor authentication. User accounts can be configured to require a one-time password (OTP) in addition to the required user password. xSA supports Google Authenticator and similar OTP systems. 4) xSA provides active monitoring of all sessions and the ability to disconnect any session at any time. 5) CTD and xDome supports SAML for the Identity provider (IdP) of choice for Multi-factor authentication (MFA)/IdP integrations.	CTD xDome xDome Secure Access
CIP-005 **R2** **Parts 2.4 and 2.5** **Supply chain access**	xSA provides active monitoring of all active vendor remote access sessions and the ability to disconnect any session at any time.	xDome Secure Access
CIP-005-7 **Electronic Security Perimeter**	CTD and xDome can automatically identify all perimeter communication in and out of the BES, and can identify critical communication and devices automatically. CTD and xDome can identify critical communication flows and devices automatically based on the classification engine. Based on their knowledge of “normal” traffic, CTD and xDome can thwart malicious inbound/outbound communications to assist in blocking an attempted exploit. xSA can control all access to and from BES systems, and create the appropriate audit logs for who accessed what system, and enforce approval requirements. As such, xSA can determine and disable active vendor remote access sessions if necessary.	CTD xDome xDome Secure Access

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-006-6 Physical Security of BES Cyber Systems	To support 1.10, CTD and xDome can automatically monitor all communication links in the environment, and can monitor the status of the communication links for communication failure or cyber attack, and alert appropriately. Both tools provide a straightforward way to demonstrate the existence of this monitoring and alerting.	CTD xDome
CIP-007-6 System Security Management **R1 Disable unnecessary logical network accessible ports**	In general for this requirement, both of Claroty's products, CTD and xDome, monitor for changes to BES systems, and provide audit trails. Both products can also detect and monitor for malicious code. In addition, as related to R4 and R5, xSA can enforce authentication and control remote access to OT systems. CTD and xDome monitor network communications and identify ports on which devices are communicating. This insight can be used to identify necessary ports for this requirement, or as an additional control to identify misconfigured devices or potential security incidents. For Claroty product roles within a NERC-CIP regulated network, and therefore in scope in their own right, by default xDome requires port 443 (HTTPS) to be open and accessible via the network and CTD requires port 22 (SSH) and port 443 (HTTPS).	CTD xDome xDome Secure Access
CIP-007-6 **R2 Patch management**	CTD and xDome can both assist by identifying specific hardware and firmware versions for devices on networks they monitor. This provides an inventory that can be used to establish and track patch sources. This inventory can also be used when evaluating specific patches for applicability to determine which specific devices may require the patch. Additionally, the products can automatically generate a comparison between the patch policy set by the organization and the actual list of installed patches on hosts, thereby identifying and reporting the list of missing patches per host. This acts as an additional control to ensure patches are installed. For Claroty product roles within a NERC-CIP regulated network, and therefore in scope in their own right, Claroty simplifies patch management compliance by providing all necessary patches, including security patches, for its software and the underlying operating system platform. These cover system functionality and operating system security. Patches for the underlying OS are tested by Claroty in-house prior to release to customers.	CTD xDome

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-007-6 **R3** **Malicious code prevention**	CTD and xDome security fabrics can monitor all network traffic within a protected network. With their advanced deep packet inspection (DPI) capabilities, built specifically for ICS networks and protocols, and their advanced machine learning algorithms, the products automatically whitelist legitimate baseline activities and alert on any changes or anomalies. These features provide a robust capability to detect malware activity occurring on the network. When Claroty products are in scope, as permitted by the standard, malicious code risks are addressed via product security hardening. Claroty has documented a full hardening procedure as part of the system deployment process. (Claroty hardening procedure guidelines are available upon request). Additionally, Claroty encrypts and signs all software updates and new software versions prior to being sent to customers.	CTD xDome
CIP-007-6 **R4** **Security event monitoring**	Many ICS devices have limited native logging, which CTD and xDome address by identifying security-relevant events through deep inspection of ICS network traffic. When a cyber asset cannot log a specific event, Claroty can detect it via DPI—including communication sessions, user logins/logouts, baseline configuration, firmware changes, command types, registers used, and response values. These events are captured across monitored assets and can be reviewed through management reports. The platforms can also be configured to capture and store network traffic to support post-incident investigations. Both CTD and xDome deliver real-time, actionable alerts on known and unknown threats, suspicious activity, logging failures, and risk-impacting changes—helping organizations protect ICS environments. For unsuccessful login attempts, they passively detect failed access across the network using DPI, and locally via WMI, SNMP, and log collection. Alerts can be triggered when defined thresholds for consecutive invalid attempts are exceeded, providing an important control—often the only one available for certain OT devices. When in scope, Claroty products provide strong logging capabilities and integrate seamlessly with modern SIEM platforms. They support standard protocols like syslog, enabling straightforward integration with enterprise environments. Claroty generates a broad set of security-relevant logs and alerts that exceed CIP requirements and support effective incident detection. Log formats are well-documented. Claroty also offers robust alerting across a wide range of detected security events, with notifications delivered directly via email.	CTD xDome

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-007-6 **R4** **Security event monitoring** (continued)	Claroty can alert when a monitoring interface goes down, supporting the requirement to alert on loss of logging under CIP-007 R4.2.2. Claroty is capable of retaining logs for the required 90-day interval. Additionally, since all logs can be sent to a SIEM, log retention can be centrally maintained for easy compliance. Log review requirements can be met in two ways. By taking advantage of Claroty's SIEM integration, log review can be performed on a single pane of glass by an entity's analyst team. Additionally, Claroty products themselves can generate reports that highlight specific events relevant to the operational environment. This allows staff to easily review security events, providing an appropriate level of expertise for this critical task.	CTD xDome
CIP-007-6 **R5** **Password guessing attacks**	As noted for R4, CTD and xDome can passively detect unsuccessful login attempts across the ICS network using DPI. Through WMI, SNMP, and log collection, they also identify local failed logins (including password guessing) at the asset level. Alerts are triggered when defined thresholds for consecutive invalid attempts are exceeded, providing an effective control for many devices—and in some cases, the only control available in ICS environments. For user authentication, Claroty supports both internal user databases and external Identity Providers (IdPs) via SAML 2.0 integration. When in scope, Claroty products meet the requirements of this guideline across key account and password controls: **User Authentication** – Claroty products contain a built-in capability to authenticate users against an internal user database or external Identity Provider (IdP) through SAML 2.0 integration. **Default Accounts** – Claroty products force users to change default passwords upon first log-in. **Password Controls** – Claroty products enable strong password controls that meet or exceed the requirements/guidelines. **Account Lockouts** – Claroty products support controls to deter password guessing attacks. The system will automatically disable user accounts after a configurable number of failed login attempts.	CTD xDome

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-008-06 Incident Reporting & Response planning	Both CTD and xDome assist with the identification of potential Cyber Security Incidents via their many capabilities for monitoring, analyzing, and reporting on network communications and system activity, including the generation of alerts for suspicious, unauthorized, or known malicious activity. CTD and xDome support response to incidents by quickly and easily reporting on communications and actions taken within systems they monitor, providing insights to investigators. Users can export information from both products for use in investigations. Both tools' outputs integrate with other tools, such as SIEMs, to support investigations. Both products can also support active response via integration with firewalls or Network Admission Control (NAC) technology. As a result, this functionality allows the Registered Entity to swiftly and effectively identify an incident, respond/act, and relay vital insight where needed.	CTD xDome
CIP-009-06 Recovery plans for BES Cyber Systems	Both CTD and xDome can identify the root cause of incidents that require a restoration process to occur, and will automatically preserve that data for later investigation. This will generate a record and alert on cyber incidents, to ensure the proper auditing capability.	CTD xDome
CIP-010-4* Configuration change management & vulnerability assessments	In addressing this guideline overall, both Claroty CTD and xDome can identify, establish and document a baseline of expected traffic, and generate alerts on changes against this baseline of activity. The products can do so by both active detection and passive monitoring. When Claroty products are in-scope, the products' software installation leverages the Linux update systems. Claroty provides all required packages and runs on a hardened, minimized Linux-based platform, making change management straightforward.	CTD xDome

*CIP-010-4 replaces CIP-010-3 as of October 2022.

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-010-4* **R1 Document baseline configurations**	Both CTD and xDome can identify and document baseline configurations using both passive monitoring and active detection. They establish and maintain configuration baselines for ICS assets, with historical data stored per asset to track and report on deviations from the authorized baseline. Reports can be generated to validate approved changes, routed to designated approvers, and documented within the organization's change control system, supporting auditor evidence requests during NERC CIP audits. As noted, Claroty also encrypts and digitally signs all software updates and new releases prior to delivery, providing strong security in support of R1, Part 1.6.	CTD xDome
CIP-010-4* **R2 Configuration monitoring and investigation of unauthorized changes**	Both CTD and xDome provide alerts when they detect that an asset has deviated from its documented, approved baseline. If unauthorized components are connected to the ICS network or unauthorized communications take place on the ICS network, both products create alerts for designated authorities.	CTD xDome
CIP-010-4* **R3 Vulnerability Assessments**	Through passive and active monitoring and detection techniques, CTD and xDome obtain detailed knowledge of the configuration of networks, the devices on those networks, and the communications between those devices. This provides a rich set of information from which to conduct vulnerability assessments. The products generate numerous insights from their analysis of network traffic. These are prioritized and made available via a number of standard reports. These insights identify potential vulnerabilities or weak spots in system design or defenses such as unpatched vulnerabilities, insecure protocols, and external communications.	CTD xDome

*CIP-010-4 replaces CIP-010-3 as of October 2022.

©Copyright Claroty. All rights reserved

Guideline #	Claroty Support	Claroty Product
CIP-010-4* **R3 Vulnerability Assessments** (continued)	The products can also generate a summarized Risk Assessment Report which provides a quick and easy overview of system security. With deep insights into the ICS environment, CTD and xDome enable users to proactively identify and fix configuration and other network hygiene issues that can leave the network vulnerable to attack. Leveraging proprietary intelligence, the products continuously monitor the network for new known vulnerabilities – providing precise CVE matching down to the firmware versions for industrial devices. Using precise asset inventory and a sanitized CVE database, these are the only solutions that present actual conclusive vulnerabilities. With other solutions that either fail to collect the full asset context (e.g. model and firmware) or fail to thoroughly sanitize their CVE databases, this can increase alert fatigue and result in precious resources spent chasing false alarms.	CTD xDome
CIP-010-4* **R4 Transient Cyber Assets and Removable Media**	Claroty products can identify transient assets connected to the network via a variety of different methods and alert on these to identify anomalous or malicious traffic.	CTD xDome
CIP-012-1** **Communications between Control Centers**	CTD and xDome can monitor traffic between control centers and specifically look for malicious or abnormal activity within that traffic.	CTD xDome
CIP-013-2 **Supply chain risk management**	CTD and xDome automatically identify vulnerabilities and show which assets are impacted by what vulnerabilities. Furthermore, both products make it easy to reference in real-time which assets have vendor disclosures.	CTD xDome
CIP-015-1 **Internal Network Security Monitoring**	CTD and xDome provide the continuous East-West visibility required to satisfy the risk-based data feed mandate (R1.1). By establishing an OT-aware behavioral baseline, the platforms detect and evaluate suspicious lateral movement or unauthorized activity inside the ESP in real-time (R1.2 and R1.3). Furthermore, Claroty ensures the forensic integrity of monitoring data through secure capture and immutable protection (R2 and R3), delivering the audit-ready evidence needed for both compliance reporting and rapid incident response.	CTD xDome Edge

**Modifications to this Guideline are underway. Please refer to NERC guidance for more information.

©Copyright Claroty. All rights reserved

Conclusion: Ease NERC CIP compliance and secure all electric services

At Claroty, we understand that Responsible Entities have a significant responsibility in securing their critical cyber assets. We also understand that all generation, transmission and distribution entities, from co-ops to municipalities and beyond, must secure the totality of their operational systems, devices and processes. Claroty provides security solutions to meet the breadth of security needed for these operational networks and processes.

The Claroty Difference

At Claroty, our goal is to provide electric utilities in the public and private sectors, regardless of size, with:

- **Flexibility** for how you deploy OT security: On-prem, cloud, or hybrid
- **Support across the OT security journey:** From asset visibility, asset management, vulnerability and risk insight, to the security of remote access across all accessing parties
- **Deep protocol support** with over 450 of the relevant protocols you need
- **Continuity** with the same solution and pricing across your environments - OT, building management, IoMT, and other IoT as your environment evolves
- **Broad and relevant integration** with the vendors you use, extending the value of your defenses, SOC & response, and IT network

Recognizing that securing the OT environments that underpin electric generation, transmission, and distribution is a complex endeavor, Claroty has tailored our cybersecurity portfolio to reflect three principles that help streamline this journey:

1. **Gain visibility into all cyber-physical systems in OT**
   Visibility is foundational to securing OT. Claroty helps utilities attain a full inventory of all OT, IoT, and other CPS across all grids, substations, transmission lines, and more.
2. **Integrate IT Tools with OT**
   Many devices and systems in these environments use proprietary protocols and legacy systems, incompatible with IT solutions. But that doesn't mean such solutions have no place in OT. Rather than require customers to expand their already-extensive tech stacks, Claroty integrates with them. As a result, customers can simply extend their IT tools and workflows to OT.
3. **Extend IT controls to OT**
   For those who lack some essential security controls and consistent governance, after providing visibility and integration with IT tools and workflows, Claroty helps extend existing IT controls to OT — unifying security governance and driving resilience across IT and OT, including the following use cases and governance controls:


Vulnerability Management


Network Segmentation


Endpoint Protection


Secure Remote Access


Threat Detection


Asset & Change Management

©Copyright Claroty. All rights reserved

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.

© Copyright Claroty Ltd. All rights reserved