SENTINEL | OT

AWIA COMPLIANCE

Cedar Ridge Regional Water Authority: Risk and Resilience Assessment, Cybersecurity Section

DOCUMENT	AWIA Section 2013 Risk and Resilience Assessment: Cybersecurity Component
DATE	July 10, 2026
PREPARED BY	Sentinel OT
CLASSIFICATION	Confidential
REFERENCE	Report ID: pbcwud_cedar-ridge_sample_2026-05-12

Purpose and Regulatory Context

America's Water Infrastructure Act (AWIA) of 2018, Section 2013, requires community water systems serving more than 3,300 people to conduct a Risk and Resilience Assessment (RRA) and to certify completion to the U.S. Environmental Protection Agency. The RRA must assess risks to the system from malevolent acts and natural hazards across all critical infrastructure components, including electronic, computer, and other automated systems.

This document constitutes the cybersecurity section of the Cedar Ridge Regional Water Authority (CRRWA) Risk and Resilience Assessment. It covers the mandatory AWIA assessment areas related to SCADA, industrial control systems, network infrastructure, and electronic security controls at the Cedar Ridge Water Treatment Plant.

This cybersecurity section is based on findings from a Comprehensive Vulnerability Assessment (Report ID: pbcwud_cedar-ridge_sample_2026-05-12) conducted by Sentinel OT in April and May 2026, and on the remediation work performed under the associated Project Scope (Phases 1 through 6, May through August 2026).

AWIA Mandatory Assessment Areas Addressed

AWIA REQUIREMENT (42 U.S.C. 1433)	COVERAGE IN THIS SECTION
Physical barriers	Not covered (see Physical Security section of full RRA)
Source water	Not covered (see Source Water section)
Pipes and constructed conveyances	Not covered (see Distribution section)
Electronic, computer, or other automated systems	**Fully covered**
Monitoring practices	**Covered** (electronic monitoring and logging)
Chemical handling and storage	Partially covered (control system integrity for chemical dosing)

AWIA REQUIREMENT (42 U.S.C. 1433)	COVERAGE IN THIS SECTION
Financial infrastructure	Not covered (see Financial section)
Operation and maintenance	**Covered** (change management, access controls, patch management)
Capital and operational needs	**Covered** (capital planning for controller replacement and OT monitoring)

Assessment Timeline

ACTIVITY	DATE
External passive reconnaissance	April 14 to 15, 2026
Phase 1 compensating controls applied	April 23 to 25, 2026
On-site internal assessment	May 5 to 9, 2026
Comprehensive Vulnerability Assessment Report delivered	May 12, 2026
Phase 3: Network architecture remediation	May 20 to July 5, 2026
Phase 4: Controller and endpoint remediation	June 1 to July 20, 2026
Phase 5: Access management, logging, and monitoring	July 1 to July 30, 2026
This RRA cybersecurity section completed	July 10, 2026
Full RRA certification target	August 15, 2026
ERP update due (within 6 months of RRA certification)	February 15, 2027

System Description

FIELD	DETAIL
System name	Cedar Ridge Regional Water Authority
PWSID	[State PWS ID]
System type	Community water system
Source	Surface water (Cedar Ridge Reservoir)
Treatment	Conventional surface water treatment
Design capacity	4.2 MGD
Average day demand	Approximately 2.8 MGD
Population served	Approximately 14,200
AWIA population tier	Small system (3,301 to 49,999)
Facilities	1 surface water treatment plant, distribution system, 1 booster station
Staffing	3 full-time operators, 1 contracted systems integrator (remote, on-call)

Automated Processes

The following water treatment processes are managed by programmable logic controllers at the Cedar Ridge Water Treatment Plant:

PROCESS	CONTROLLER	CONSEQUENCE OF UNAUTHORIZED MODIFICATION
Chlorine disinfection dosing	PLC-01	Over-dosing or under-dosing of chlorine. Under-dosing creates a public health risk from waterborne pathogens. Over-dosing can produce harmful disinfection byproducts and cause consumer complaints.

PROCESS	CONTROLLER	CONSEQUENCE OF UNAUTHORIZED MODIFICATION
Coagulant feed control	PLC-01	Improper coagulant dosing degrades turbidity removal in the sedimentation and filtration process. High turbidity in finished water violates the Surface Water Treatment Rule.
Clearwell level control	PLC-01	Loss of clearwell level control can cause overflow (wasted treated water) or low level conditions that compromise contact time for disinfection (CT violation).
Filtration backwash sequencing	PLC-02	Premature or skipped backwash cycles lead to filter breakthrough and elevated turbidity in finished water.
High-service pump control	PLC-02	Unauthorized pump manipulation can cause pressure transients in the distribution system, leading to main breaks or low-pressure conditions that create contamination intrusion risk.

Cybersecurity Threat Assessment

Threat Actors

The following threat actors are assessed as relevant to community water systems based on current CISA, FBI, and EPA intelligence:

THREAT ACTOR	MOTIVATION	LIKELIHOOD	RELEVANT ADVISORIES
Nation-state (China, Volt Typhoon)	Pre-positioning for future disruption of critical infrastructure	Medium	AA24-038A

THREAT ACTOR	MOTIVATION	LIKELIHOOD	RELEVANT ADVISORIES
Nation-state (Iran, IRGC-affiliated)	Targeting of water PLCs and HMIs, ideological motivation	Medium	AA23-335A
Hacktivists (pro-Russia, CyberAv3ngers)	Targeting of water utility HMI systems for propaganda	High	AA24-010A
Ransomware operators	Financial extortion, data theft	High	Multiple CISA alerts
Insider threat (disgruntled employee)	Sabotage, data theft	Low	N/A
Opportunistic attacker	Exploitation of internet-exposed ICS for any purpose	Very High	CISA CPG 2.F

Attack Scenarios

The following attack scenarios were evaluated during the risk assessment based on the facility's specific technology and exposure:

SCENARIO	ENTRY POINT	IMPACT	PRE-REMEDIATION LIKELIHOOD	POST-REMEDIATION LIKELIHOOD
Remote PLC logic modification via EtherNet/IP	Internet-exposed port 44818 (CVE-2021-22681)	Chemical dosing manipulation, loss of process control	Very High	Very Low (VPN + firewall + firmware upgrade)

SCENARIO	ENTRY POINT	IMPACT	PRE-REMEDIATION LIKELIHOOD	POST-REMEDIATION LIKELIHOOD
Stealth logic tampering (Evil PLC)	CVE-2022-1161 via authentication bypass	Silent process manipulation, undetectable by operator	High	Very Low (firmware upgrade + change detection + change management)
HMI workstation compromise via malware	USB media, browser exploit, or phishing (INT-2, INT-5)	Full controller access via Studio 5000, data exfiltration from historian	High	Low (OS upgrade, WDAC whitelisting, USB lockdown, segmentation)
Lateral movement from any compromised device	Flat network, no segmentation (INT-1)	Unrestricted access to all OT assets	High	Very Low (four-zone segmentation with industrial firewall)
Historian data tampering	Default SA credentials (INT-3)	Concealment of attack evidence, manipulation of compliance records	Medium	Very Low (credentials rotated, access restricted to historian VLAN)
Radio link interception/ injection	Unencrypted XetaWave link (INT-8)	Modbus command injection to booster station RTU	Low	Very Low (AES-256 encryption enabled)

OT Asset Inventory

The following asset inventory was validated during the on-site assessment (May 5 to 9, 2026).

Controllers

ASSET ID	DEVICE	IP ADDRESS	FIRMWARE	FUNCTION
PLC-01	Rockwell Automation CompactLogix 1769-L18ER/A	192.168.1.30	20.011 (pre-remediation)	Chlorine dosing, coagulant feed, clearwell level
PLC-02	Rockwell Automation CompactLogix 1769-L18ER/B	192.168.1.3	20.011 (pre-remediation)	Filtration backwash, high-service pumps

HMI and Engineering

ASSET ID	DEVICE	OS	SOFTWARE
HMI-01	Dell OptiPlex 7070	Windows 10 IoT Enterprise LTSC 2021 (post-remediation)	FactoryTalk View SE Client, Studio 5000 v20

Servers

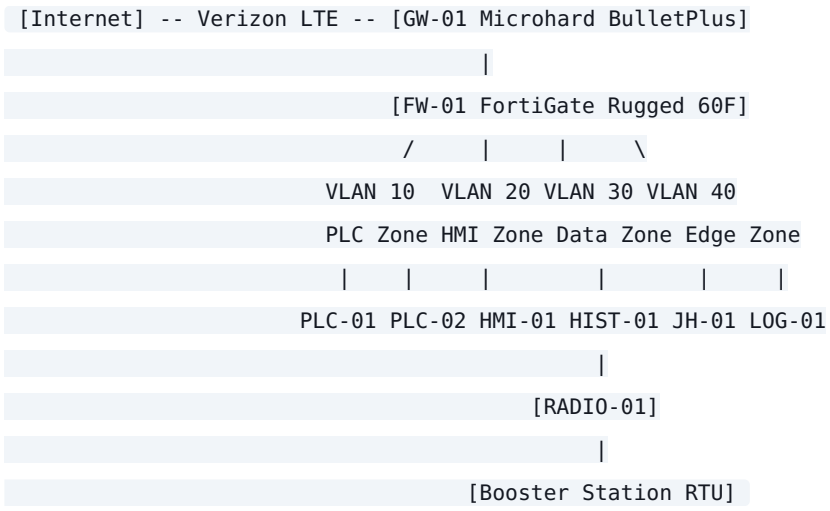
ASSET ID	DEVICE	OS	FUNCTION
HIST-01	Dell PowerEdge T340	Windows Server 2016 Standard	FactoryTalk Historian SE (SQL Server Express)

ASSET ID	DEVICE	OS	FUNCTION
LOG-01	Dell OptiPlex Micro (post-remediation)	Linux	Centralized syslog server (Wazuh)

Network Equipment

ASSET ID	DEVICE	FUNCTION
GW-01	Microhard BulletPlus	Cellular gateway (Verizon LTE), VPN termination
FW-01	Fortinet FortiGate Rugged 60F (post-remediation)	Industrial firewall, zone-based access control
SW-01	Cisco IE-3300-8T2S-E (post-remediation)	Managed switch, VLAN segmentation
RADIO-01	XetaWave XETA9-E	900 MHz point-to-point telemetry to booster station
JH-01	Dell OptiPlex Micro (post-remediation)	Secure remote access jump host with MFA

Network Architecture (Post-Remediation)



VLAN	ZONE	ASSETS	ACCESS RULES
10	Controller	PLC-01, PLC-02	Inbound: EtherNet/IP from VLAN 20 only. No internet access.
20	HMI/ Engineering	HMI-01	Inbound: from VLAN 40 (jump host) via RDP only. Outbound: EtherNet/IP to VLAN 10, SQL to VLAN 30.
30	Data	HIST-01, LOG-01, RADIO-01	Inbound: SQL from VLAN 20, syslog from all VLANs. No internet access.
40	Edge	GW-01, FW-01, JH-01	Inbound: VPN only. JH-01 outbound to VLAN 20 (RDP) only.

Vulnerability Assessment Summary

Findings Register

The following table summarizes all findings from the Comprehensive Vulnerability Assessment (May 12, 2026) and their current remediation status.

ID	FINDING	SEVERITY	PRE-REMEDIATION RISK	REMEDIATION ACTION	POST-REMEDIATION RISK	STATUS
EXT-1	CVE-2021-22681: Authentication bypass on EtherNet/IP (CISA KEV)	Critical	Critical	Phase 1 ACL, Phase 3 VPN + firewall, Phase 4 firmware upgrade	Low	Remediated

ID	FINDING	SEVERITY	PRE-REMEDIATION RISK	REMEDIATION ACTION	POST-REMEDIATION RISK	STATUS
EXT-2	CVE-2022-1161: Stealth logic modification	Critical	Critical	Phase 1 ACL, Phase 4 firmware + change detection, Phase 5 change management	Low	Remediated
EXT-3	CVE-2019-10952: Web server buffer overflow RCE	Critical	Critical	Phase 1 ACL, Phase 3 firewall, Phase 4 firmware upgrade	Low	Remediated
INT-1	No network segmentation (flat 192.168.1.0/24)	Critical	Critical	Phase 3 managed switch + firewall + four-zone VLANs	Low	Remediated
INT-2	HMI end-of-life OS, no endpoint protection	Critical	Critical	Phase 4 OS rebuild (Win10 IoT LTSC), WDAC whitelisting	Low	Remediated
INT-3	Historian default SA credentials	Critical	Critical	Phase 4 SA disabled, named service accounts, VLAN restriction	Low	Remediated

ID	FINDING	SEVERITY	PRE-REMEDIATION RISK	REMEDIATION ACTION	POST-REMEDIATION RISK	STATUS
INT-4	No PLC backups or change management	Critical	Critical	Phase 2 baseline, Phase 4 change detection, Phase 5 change management procedure	Low	Remediated
EXT-4	XetaWave radio UI exposed without auth	High	High	Phase 1 ACL, Phase 3 firewall (no external access to radio)	Low	Remediated
EXT-6	Cleartext FTP/ Telnet, default gateway credentials	High	High	Phase 1 services disabled, credentials rotated	Low	Remediated
INT-5	USB ports enabled, no media controls	High	High	Phase 4 USB mass storage disabled via Group Policy	Low	Remediated
INT-6	Shared operator credentials	High	High	Phase 5 individual accounts, RBAC, password policy, MFA for VPN	Low	Remediated

ID	FINDING	SEVERITY	PRE-REMEDIATION RISK	REMEDIATION ACTION	POST-REMEDIATION RISK	STATUS
INT-7	No OT logging or monitoring	High	High	Phase 5 Wazuh syslog server, log forwarding, 90-day retention, alerting	Medium	Partially remediated (see Residual Risk 2)
EXT-5	Open DNS resolver on gateway	Medium	Medium	Phase 1 restricted to internal interface	Low	Remediated
INT-8	Radio link unencrypted	Medium	Medium	Phase 4 AES-256 encryption on XetaWave	Low	Remediated
INT-9	Server closet unlocked	Medium	Medium	Phase 4 electronic keypad lock installed	Low	Remediated

Risk Reduction Summary

METRIC	PRE-REMEDIATION	POST-REMEDIATION
Critical findings	7	0
High findings	5	0
Medium findings	4	1 (INT-7 partially remediated)
Internet-exposed ICS devices	2	0

METRIC	PRE-REMEDIATION	POST-REMEDIATION
CISA KEV overdue	1	0
IEC 62443-3-3 SR compliance gaps	7 of 7 assessed	1 of 7 (SR 6.2 partial)

Cybersecurity Controls Assessment

This section evaluates the current state of cybersecurity controls against the AWIA-relevant requirements of IEC 62443-3-3, NIST SP 800-82 Rev 3, and CISA Cross-Sector Cybersecurity Performance Goals (CPG) 2.0.

IEC 62443-3-3 System Security Requirements

REQUIREMENT	DESCRIPTION	PRE-REMEDIATION	POST-REMEDIATION	EVIDENCE
SR 1.1	Human user identification and authentication	Non-compliant. Shared credentials, no individual accounts.	Compliant. Individual named accounts with role-based access. MFA on VPN.	User account registry, VPN configuration
SR 2.3	Use control for portable and mobile devices	Non-compliant. USB unrestricted.	Compliant. USB mass storage disabled. HID devices whitelisted.	Group Policy configuration
SR 3.1	Communication integrity	Non-compliant. No CIP Security. Radio unencrypted.	Partially compliant. Radio encrypted (AES-256). CIP Security enabled if firmware supports it, otherwise formal risk acceptance documented.	Radio configuration, firmware records or risk acceptance

REQUIREMENT	DESCRIPTION	PRE-REMEDIATION	POST-REMEDIATION	EVIDENCE
SR 3.4	Software and information integrity	Non-compliant. No backups, no change management.	Compliant. Golden image baselines, monthly comparison, written change procedure.	Change management procedure, baseline records
SR 5.1	Network segmentation	Non-compliant. Flat network.	Compliant. Four-zone VLAN architecture with industrial firewall.	Firewall rules, VLAN configuration, segmentation test results
SR 6.1	Audit log accessibility	Non-compliant. No logging.	Compliant. Centralized syslog (Wazuh), 90-day retention.	Syslog server configuration, retention policy
SR 6.2	Continuous monitoring	Non-compliant. No monitoring.	Partially compliant. Syslog-based monitoring and alerting deployed. Deep packet inspection (OT network monitoring sensor) not yet deployed.	Syslog alerting rules. See Residual Risk 2.

NIST SP 800-82 Rev 3 Alignment

CONTROL AREA	PRE-REMEDIATION	POST-REMEDIATION
OT network architecture	No segmentation, no DMZ	Four-zone architecture with firewall, VPN-only remote access
Access control	Shared credentials, no MFA	Individual accounts, RBAC, MFA on VPN, application whitelisting
Patch management	HMI unpatched (3+ years), controllers at vulnerable firmware	HMI on supported LTSC with patch management, controllers upgraded

CONTROL AREA	PRE-REMEDIATION	POST-REMEDIATION
Audit and accountability	No logging	Centralized syslog, 90-day retention, alerting
Configuration management	No backups, no change control	Golden image baselines, monthly comparison, written change procedure
Incident response	No documented procedure	ERP update in progress (due within 6 months of RRA certification)

CISA CPG 2.0 Alignment

CPG	REQUIREMENT	PRE-REMEDIATION	POST-REMEDIATION
1.A	Mitigate known vulnerabilities	3 Critical CVEs unpatched, 1 KEV overdue	All CVEs remediated or compensating controls documented
1.E	Default credentials	Default credentials on gateway, historian, radio	All default credentials replaced
2.A	Multi-factor authentication	Not implemented	MFA required for all remote access
2.F	No exploitable services on the internet	2 PLCs, 9 services on public internet	Zero services on public internet
5.A	Asset inventory	No documented inventory	Complete validated asset inventory
5.B	Logging	No logging infrastructure	Centralized syslog with alerting

Residual Risks

The following residual risks remain after completion of all remediation phases. Each has been evaluated and either accepted with documented compensating controls or designated for future capital planning.

Residual Risk 1: CompactLogix 1769-L18ER CIP Security Limitation

Risk. If the 1769-L18ER platform does not support CIP Security at any available firmware version, EtherNet/IP sessions between the HMI and PLCs on the internal network will lack protocol-level authentication and integrity verification.

Compensating controls.

- Network segmentation (Phase 3) restricts EtherNet/IP traffic to VLAN 20 (HMI) to VLAN 10 (PLC) only. No other devices can initiate CIP connections.
- Individual accounts and RBAC (Phase 5) restrict who can access the HMI workstation.
- Application whitelisting (Phase 4) prevents unauthorized software from running on the HMI.
- Change detection and change management (Phases 4 and 5) enable detection of unauthorized program modifications.

Residual risk rating. Low (with compensating controls).

Capital plan. Controller replacement with CompactLogix 5380 (which supports CIP Security natively) is recommended for the FY2027 capital budget. Estimated cost: $8,000 to $12,000 per controller including migration services.

Residual Risk 2: No Deep Packet Inspection OT Monitoring

Risk. The Wazuh syslog deployment provides log-based monitoring and alerting, but does not perform deep packet inspection of industrial protocols (EtherNet/IP CIP, Modbus). Sophisticated attacks on the internal OT network that do not generate log events (for example, legitimate-looking CIP commands from a compromised HMI) may not be detected by syslog-based monitoring alone.

Compensating controls.

- Network segmentation limits the devices that can originate CIP traffic to the HMI workstation only.
- Application whitelisting restricts what software can run on the HMI.
- Change management and monthly golden image comparisons provide a detection mechanism for unauthorized PLC program modifications, albeit not in real time.

Residual risk rating. Medium.

Capital plan. Deployment of a passive OT network monitoring sensor (Nozomi Guardian, Claroty CTD, or Dragos Platform) is recommended for the FY2027 or FY2028 capital budget. Estimated cost: $25,000 to $50,000 for a single small-site sensor plus annual subscription. This investment would close the gap in IEC 62443-3-3 SR 6.2 (Continuous Monitoring).

Residual Risk 3: Historian Server Operating System

Risk. HIST-01 runs Windows Server 2016 Standard, which reaches end of extended support on January 12, 2027. After that date, no further security updates will be available.

Compensating controls.

- Network segmentation restricts historian access to VLAN 20 (HMI) and VLAN 30 (data) only. No internet access from the historian VLAN.
- Default credentials have been replaced with named service accounts.
- Security logging is forwarded to the centralized syslog server.

Residual risk rating. Medium (increases to High after January 2027 if not addressed).

Capital plan. Historian server OS upgrade or replacement should be planned for Q4 2026, prior to the end of support date. Options include upgrading to Windows Server 2022 (in-place or clean install) or migrating to a current-generation historian platform.

Recommendations for Next Assessment Cycle

The following items are recommended for inclusion in the next AWIA RRA cycle (due 5 years from initial certification):

1. **Deploy OT network monitoring sensor** (Residual Risk 2). Closes the IEC 62443-3-3 SR 6.2 gap and provides real-time visibility into CIP and Modbus traffic.
2. **Replace CompactLogix 1769-L18ER controllers** (Residual Risk 1). Migrate to CompactLogix 5380 with native CIP Security support.
3. **Upgrade historian server OS** (Residual Risk 3). Migrate to Windows Server 2022 or a current-generation historian platform before January 2027 end of support.
4. **Evaluate backup power for OT network equipment.** The industrial firewall, managed switch, and syslog server should be connected to UPS-protected circuits if not already.
5. **Expand cybersecurity training.** Consider annual cybersecurity awareness training for all plant operations staff, including phishing recognition and incident reporting.

6. **Assess booster station RTU security.** The XetaWave radio link is now encrypted, but the booster station RTU was out of scope for this assessment. Include it in the next cycle.

Certification Statement

This Risk and Resilience Assessment (cybersecurity section) has been prepared in accordance with the requirements of Section 2013 of America's Water Infrastructure Act of 2018 (42 U.S.C. 1433). The assessment covers all electronic, computer, and automated systems at the Cedar Ridge Water Treatment Plant.

The assessment was conducted by Sentinel OT using a combination of passive external reconnaissance, authorized on-site assessment, and post-remediation validation. All findings have been documented, remediated or mitigated, and residual risks have been formally evaluated with compensating controls or capital planning as described in this document.

Upon completion of the full RRA (incorporating physical security, source water, distribution, chemical handling, financial, and operational sections), the certifying official for Cedar Ridge Regional Water Authority should submit a signed certification to the U.S. EPA via the electronic certification portal at https://www.epa.gov/waterresilience.

FIELD	DETAIL
Certifying official	[Name and title]
Certification date	[Date]
RRA completion date	[Date]
ERP update due	Within 6 months of RRA certification
Next RRA recertification	Within 5 years of certification

References

DOCUMENT	DESCRIPTION
AWIA Section 2013 (42 U.S.C. 1433)	Statutory requirements for RRA and ERP
EPA Fact Sheet EPA-817-F-19-004	Risk and Resilience Assessment and Emergency Response Plan requirements
EPA Small System RRA Checklist	Optional guidance tool for small systems
IEC 62443-3-3:2013	System security requirements and security levels for IACS
NIST SP 800-82 Rev 3	Guide to Operational Technology Security
CISA CPG 2.0	Cross-Sector Cybersecurity Performance Goals
CISA Advisory AA23-335A	IRGC-affiliated cyber actors exploiting PLCs (November 2023)
CISA Advisory AA24-038A	PRC state-sponsored Volt Typhoon (February 2024)
CISA Advisory AA24-010A	Russian hacktivists targeting water HMI (January 2024)
Comprehensive Vulnerability Assessment Report	Report ID: pbcwud_cedar-ridge_sample_2026-05-12
Project Scope and Statement of Work	Sentinel OT, dated May 15, 2026

Sample document. Cedar Ridge Regional Water Authority is a fictional operator used to illustrate the format and depth of a Sentinel OT AWIA-compliant Risk and Resilience Assessment (cybersecurity section). No real utility, facility, or IP address is depicted. This document accompanies the sample Comprehensive Vulnerability Assessment Report, Project Scope, and Grant Narrative (Report ID: pbcwud_cedar-ridge_sample_2026-05-12).