SENTINEL | OT

GRANT NARRATIVE

SLCGP Grant Application Narrative: Cedar Ridge Regional Water Authority

DOCUMENT	State and Local Cybersecurity Grant Program Application Narrative
DATE	May 20, 2026
PREPARED BY	Sentinel OT (on behalf of CRRWA)
CLASSIFICATION	Confidential
REFERENCE	Report ID: pbcwud_cedar-ridge_sample_2026-05-12

Applicant Information

FIELD	DETAIL
Applicant	Cedar Ridge Regional Water Authority (CRRWA)
Type	Municipal water utility, community water system
Population served	Approximately 14,200
AWIA population tier	Small system (serving 3,301 to 49,999)
State	[State]
SAA	[State Administrative Agency]
NAICS	221310 (Water Supply and Irrigation Systems)

Executive Summary

Cedar Ridge Regional Water Authority operates a surface water treatment plant serving approximately 14,200 residents. A comprehensive external and internal vulnerability assessment conducted in April and May 2026 identified **seven Critical findings**, **five High findings**, and **four Medium findings** across the facility's operational technology infrastructure.

Three Critical vulnerabilities (CVSS 9.8) were confirmed on two internet-exposed Rockwell Automation CompactLogix controllers, including CVE-2021-22681, which is listed in the CISA Known Exploited Vulnerabilities (KEV) catalog with a federal remediation deadline that has already passed. The on-site assessment revealed additional Critical internal deficiencies: no network segmentation (flat OT network), an HMI workstation running end-of-life software with no endpoint protection, a historian database accessible with default vendor credentials, and no PLC program backups or change management controls.

CRRWA is requesting $115,020 in SLCGP funding to conduct a full remediation of its operational technology infrastructure. The project addresses all 16 findings across seven phases over approximately 95 calendar days.

The total project cost is $191,700 ($180,400 in professional services and $11,300 in hardware and software). CRRWA will provide the required 40% non-federal cost share of $76,680 from its capital improvement fund.

Problem Statement

Current Threat Landscape

Water and wastewater systems are designated critical infrastructure under Presidential Policy Directive 21 (PPD-21) and face an escalating threat environment. CISA, the FBI, and the EPA have issued multiple joint advisories since 2021 warning of nation-state and criminal targeting of water utility SCADA systems, including advisories addressing Iranian-affiliated actors (AA23-335A), Chinese state-sponsored Volt Typhoon campaigns (AA24-038A), and Russian hacktivists targeting HMI systems at water facilities (AA24-010A).

Small and medium water utilities face disproportionate risk due to limited cybersecurity staffing, legacy industrial control systems, and reliance on remote access configurations that were not designed with current threats in mind.

Cedar Ridge Specific Findings

A comprehensive vulnerability assessment combining passive external reconnaissance (April 14 to 15, 2026) and a five-day on-site assessment (May 5 to 9, 2026) identified the following findings at the Cedar Ridge Water Treatment Plant:

External Critical Findings (CVSS 9.8)

CVE	DESCRIPTION	CISA KEV
CVE-2021-22681	Rockwell Automation authentication bypass. Allows an unauthenticated attacker to connect to a CompactLogix controller and read, modify, or replace the running PLC program over CIP (port 44818).	Yes. Federal deadline passed.

CVE	DESCRIPTION	CISA KEV
CVE-2022-1161	Rockwell Automation controller program modification. Exploits the lack of runtime integrity verification to silently alter controller logic without detection by the engineering workstation.	No
CVE-2019-10952	Rockwell Automation web server buffer overflow. A crafted HTTP request to the controller's embedded web server can cause a denial-of-service condition or potentially allow remote code execution.	No

Internal Critical Findings

FINDING	DESCRIPTION
No network segmentation	All OT devices share a single flat 192.168.1.0/24 subnet with an unmanaged switch. No VLANs, firewalls, or access controls between devices.
HMI end-of-life OS	The HMI workstation runs Windows 10 Pro 21H2 (end of support June 2023) with no security updates since January 2025 and no endpoint protection.
Historian default credentials	The FactoryTalk Historian SE database is accessible with default vendor SA credentials from any device on the network.
No PLC backups or change management	No documented backup of either controller program exists. The most recent integrator backup is 22 months old. No change management procedure exists.

Additional High and Medium Findings

- Shared operator credentials across all staff (no individual accountability)
- No logging or monitoring infrastructure in the OT environment
- USB ports enabled with no media controls on the HMI workstation
- XetaWave radio management interface exposed without authentication
- Radio telemetry link operating without encryption

- Default credentials and insecure services on the cellular gateway
- Server closet containing historian and network equipment is unlocked

These controllers manage chemical dosing, filtration backwash sequencing, and clearwell level control. The combination of internet-exposed controllers, unpatched internal systems, flat network architecture, and no change management controls means that unauthorized modification of water treatment processes is technically achievable with minimal skill and no physical presence.

Project Description

This project consists of seven phases executed over approximately 95 calendar days, with continuous monitoring beginning in month four. The project scope and statement of work (referenced as a companion document) provides detailed task-level descriptions for each phase.

Phase 1: Immediate Compensating Controls (Days 1 to 3)

Deploy access control lists and firewall rules on the existing Microhard BulletPlus cellular gateway to block all unauthorized inbound traffic to industrial control system ports. Rotate all credentials and disable insecure services. No plant downtime required.

This phase addresses the most urgent risk by eliminating direct internet accessibility of the PLCs within 72 hours of contract execution.

Phase 2: Comprehensive On-Site Assessment (Days 4 to 14)

Conduct a five-day on-site assessment of the complete OT network. Validate all external findings against physical infrastructure, map the full internal network architecture, perform controller integrity baselines, assess all endpoints (HMI, historian, radio), evaluate access management and logging posture, and conduct an AWIA-aligned risk and resilience assessment.

Phase 3: Network Architecture Remediation (Days 15 to 50)

Replace the current NAT/port-forwarding remote access model with a VPN-only architecture using certificate-based authentication. Deploy an industrial firewall (Fortinet FortiGate Rugged 60F or Cisco ISA 3000) between the cellular gateway and the OT network. Replace the unmanaged switch with a managed industrial Ethernet switch (Cisco IE-3300) supporting VLANs. Implement four-zone network segmentation per IEC 62443-3-3. Establish a secure remote access jump host with multi-factor authentication.

Phase 4: Controller and Endpoint Remediation (Days 35 to 75)

Upgrade PLC firmware to the latest supported version and enable CIP Security if supported. Rebuild the HMI workstation with a supported operating system (Windows 10 IoT Enterprise LTSC 2021), deploy application whitelisting, and disable USB mass storage. Harden the historian database by replacing default credentials with named service accounts. Enable AES-256 encryption on the XetaWave radio link. Install access control on the server closet.

Phase 5: Access Management, Logging, and Monitoring (Days 50 to 80)

Create individual named accounts for all operators and the systems integrator. Implement role-based access control and a password policy. Deploy a centralized syslog server with 90-day log retention. Configure log forwarding from the gateway, HMI, historian, and firewall. Establish a formal PLC change management procedure with golden image baselines. Conduct operator training on all new procedures.

Phase 6: Documentation and Compliance (Days 70 to 95)

Produce a complete documentation package including an AWIA-compliant Risk and Resilience Assessment, Emergency Response Plan update, standards compliance mapping (IEC 62443, NIST SP 800-82 Rev 3, CISA CPG 2.0), as-built network architecture document, and executive summary for the CRRWA Board of Directors. Conduct a closeout briefing with plant operations staff and the systems integrator.

Phase 7: Ongoing Monitoring (Month 4 onward)

Continuous passive monitoring of all CRRWA internet-facing assets, vulnerability alerting for deployed Rockwell Automation products, and quarterly posture reports. Annual review of compensating controls and risk acceptances. This phase is funded separately as an annual subscription ($9,600/year) and is not included in the SLCGP funding request.

Alignment to SLCGP Eligible Activities

SLCGP OBJECTIVE	PROJECT PHASE	DESCRIPTION
Objective 1: Governance and Planning	Phase 6	AWIA-compliant Risk and Resilience Assessment, Emergency Response Plan update, standards compliance mapping, as-built network documentation
Objective 2: Assessment and Evaluation	Phases 1 and 2	External reconnaissance validation, on-site comprehensive assessment, controller integrity baselines, internal vulnerability assessment
Objective 3: Mitigation	Phases 3, 4, and 5	Network segmentation, industrial firewall, VPN, controller firmware upgrades, HMI hardening, historian hardening, logging deployment, access controls
Objective 4: Workforce Development	Phase 5	Operator training on new access procedures, change management, USB media policy, syslog alert response, and escalation procedures

Alignment to NIST Cybersecurity Framework

CSF FUNCTION	PROJECT ACTIVITY
Identify (ID)	Asset inventory, network architecture mapping, vulnerability register, risk and resilience assessment
Protect (PR)	Network segmentation, VPN deployment, MFA, credential rotation, industrial firewall, firmware upgrades, application whitelisting, USB controls, radio encryption, historian hardening
Detect (DE)	Centralized syslog with alerting, controller change detection, continuous passive monitoring, quarterly posture reporting
Respond (RS)	Emergency Response Plan update, incident response capability assessment, escalation contacts
Recover (RC)	Controller golden image baselines, PLC backup procedures, change management documentation

Alignment to CISA Cross-Sector Cybersecurity Performance Goals (CPGs)

CPG	PROJECT ACTIVITY
1.A: Mitigate Known Vulnerabilities	Remediation of CVE-2021-22681 (CISA KEV), CVE-2022-1161, CVE-2019-10952. HMI OS upgrade to supported version.
1.E: Default Credentials	Rotation of all default credentials on controllers, gateway, historian database, and radio equipment
2.A: Multi-Factor Authentication	MFA requirement for all remote access via secure jump host and VPN

CPG	PROJECT ACTIVITY
2.F: Network Segmentation	Four-zone segmentation (controller, HMI, historian, network edge) with industrial firewall and managed switch
5.A: Asset Inventory	Complete validated asset inventory of all OT infrastructure
5.B: Logging	Centralized syslog server with 90-day retention, log forwarding from all OT devices

Budget Justification

Professional Services

PHASE	DESCRIPTION	HOURS	RATE	COST	JUSTIFICATION
Phase 1	Compensating Controls	16	$300/hr	$4,800	Remote ACL configuration, credential rotation, service hardening on Microhard gateway.
Phase 2	On-Site Assessment	Blended	Blended	$52,000	5 days on-site (2 assessors) plus pre-assessment planning and post-assessment analysis. Includes travel, per diem, and specialized OT assessment tooling. Rate consistent with ICS/OT specialist market rates ($200 to $350/hr).

PHASE	DESCRIPTION	HOURS	RATE	COST	JUSTIFICATION
Phase 3	Network Architecture	140	$300/hr	$42,000	Firewall deployment, managed switch installation, VLAN configuration, VPN architecture, jump host setup, segmentation verification. Two on-site implementation trips with maintenance windows.
Phase 4	Controller and Endpoint	120	$300/hr	$36,000	Firmware upgrade coordination, HMI OS rebuild, application whitelisting, historian hardening, radio encryption, USB lockdown. Two on-site trips.
Phase 5	Access and Monitoring	80	$300/hr	$24,000	Individual account creation, RBAC, syslog server deployment, log forwarding, change management procedure, operator training.
Phase 6	Documentation	72	$300/hr	$21,600	AWIA RRA, ERP update, standards compliance mapping, as-built documentation, executive summary, closeout briefing.
	Professional Services Total			**$180,400**	

Hardware and Software

ITEM	ESTIMATED COST	JUSTIFICATION
Industrial firewall (Fortinet FortiGate Rugged 60F + 1-year FortiGuard subscription)	$3,400	Required for IEC 62443-compliant zone segmentation. List price $2,770 plus $630/yr subscription. Alternative: Cisco ISA 3000 (list $5,750).
Managed industrial switch (Cisco IE-3300-8T2S-E)	$2,350	Replaces unmanaged Stratix 2000. Required for VLAN segmentation. 8x GE copper + 2x GE SFP.
Secure jump host with MFA hardware	$1,350	Hardened workstation for authorized remote access. Includes 3x YubiKey 5 MFA tokens ($50 each).
Windows 10 IoT Enterprise LTSC 2021 license	$350	Supported OS for HMI workstation rebuild. 10-year support lifecycle.
Syslog/logging server	$1,400	Dedicated small form factor PC with 2 TB SSD. Software: Wazuh (open source, no license cost).
SFP modules, cabling, installation materials	$1,800	Cat6A cabling, SFP modules for managed switch, DIN rail adapters, patch panel, rack hardware.
Server closet access control	$650	Electronic keypad lock with audit trail for server closet containing historian and network equipment.
Hardware and Software Total	**$11,300**	

Total Project Budget

CATEGORY	AMOUNT
Professional services	$180,400
Hardware and software	$11,300
Total project cost	**$191,700**
Federal share (60%)	$115,020
Non-federal match (40%)	$76,680

CRRWA will provide the 40% non-federal cost share from its capital improvement fund. No in-kind match is included in this request.

Project Timeline

PHASE	START	END	DURATION
Phase 1: Compensating Controls	Day 1	Day 3	3 days
Phase 2: On-Site Assessment	Day 4	Day 14	11 days
Phase 3: Network Architecture	Day 15	Day 50	36 days
Phase 4: Controller and Endpoint	Day 35	Day 75	41 days
Phase 5: Access and Monitoring	Day 50	Day 80	31 days
Phase 6: Documentation	Day 70	Day 95	26 days

Phases 3 through 5 overlap where dependencies allow. Total project duration: approximately 95 calendar days from contract execution.

The project can begin within 30 days of grant award. Phase 1 (compensating controls) will be initiated within 72 hours of contract execution to address the immediate risk from CISA KEV-listed vulnerabilities.

Performance Metrics

METRIC	BASELINE (CURRENT)	TARGET (POST-PROJECT)	MEASUREMENT METHOD
Internet-exposed ICS devices	2 PLCs on public internet	0 devices exposed	Passive scan validation
Unpatched Critical CVEs	3 confirmed (CVSS 9.8)	0 unpatched Critical CVEs	Firmware version audit
CISA KEV compliance	1 overdue KEV (CVE-2021-22681)	0 overdue KEVs	KEV catalog cross-reference
Network segmentation	No segmentation (flat network)	Four-zone architecture per IEC 62443	Firewall rule audit and segmentation test
Multi-factor authentication	Not implemented	Required for all remote access	Access configuration audit
Individual user accounts	0 (shared credentials)	Named account for each user	Account registry review
Endpoint protection	None on HMI workstation	Application whitelisting (WDAC) deployed	Policy configuration audit
PLC change management	No backups, no procedure	Golden image baseline, monthly comparison, written change procedure	Backup verification and procedure review
Security logging	No logging infrastructure	Centralized syslog, 90-day retention, alerting	Log server audit

METRIC	BASELINE (CURRENT)	TARGET (POST-PROJECT)	MEASUREMENT METHOD
AWIA compliance documentation	Not current	Complete and current RRA and ERP	Document review

Sustainability Plan

Upon completion of Phases 1 through 6, CRRWA will maintain its improved cybersecurity posture through:

- **Continuous monitoring**: Sentinel OT will provide ongoing passive monitoring and vulnerability alerting as an annual subscription ($9,600/year), funded through CRRWA's operating budget.
- **Quarterly review**: Sentinel OT will deliver quarterly posture reports identifying any new exposures, advisories affecting deployed equipment, syslog alert summaries, or configuration drift.
- **Change management**: Phase 5 establishes a formal PLC change management procedure with golden image baselines, monthly program comparisons, and written change documentation. This procedure will be maintained by plant operations staff with integrator support.
- **Logging and monitoring**: The syslog infrastructure deployed in Phase 5 provides ongoing visibility into access events, configuration changes, and security alerts. Log retention is set to 90 days.
- **Capital planning**: If the 1769-L18ER platform does not support CIP Security, controller replacement will be included in the FY2027 capital budget with a cost estimate provided during Phase 4. A future capital request for a dedicated OT network monitoring sensor (estimated $25,000 to $50,000) is recommended to complement the syslog-based monitoring.

Organizational Capability

Sentinel OT (Cybersecurity Contractor)

Sentinel OT is a cybersecurity intelligence firm specializing in operational technology and industrial control system security for critical infrastructure operators. Sentinel OT's capabilities include:

- Passive reconnaissance and vulnerability intelligence for OT/ICS environments
- On-site assessment of SCADA, DCS, and PLC-based control systems
- Network architecture design per IEC 62443 zone and conduit models
- Endpoint hardening for OT workstations and servers
- Access management and logging infrastructure deployment
- Compliance documentation for AWIA, NIST SP 800-82, and CISA CPG frameworks
- Grant application support for SLCGP, DWSRF, and WIFIA-funded cybersecurity projects

CRRWA (Applicant)

Cedar Ridge Regional Water Authority operates one surface water treatment plant and a distribution system serving approximately 14,200 residents. CRRWA employs three full-time operators and contracts with a systems integrator for SCADA maintenance. CRRWA has not previously conducted a formal cybersecurity assessment of its OT infrastructure, which underscores the need for this engagement.

Supplementary Documentation

The following companion documents are available upon request:

1. **Comprehensive Vulnerability Assessment Report** (Report ID: pbcwud_cedar-ridge_sample_2026-05-12). Full external and internal assessment findings, validated asset inventory, controller integrity baseline, network architecture diagram, and complete vulnerability register with risk ratings.
2. **Project Scope and Statement of Work**. Task-level descriptions for all seven phases, itemized hardware and labor costs, acceptance criteria, assumptions, exclusions, and a findings-to-phase traceability matrix.

3. **CRRWA Cybersecurity Plan**. Alignment to the 16 required elements of the state cybersecurity plan (to be completed as part of the application process).

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